Stream:	Internet Engineering Task Force (IETF)
RFC:	9788
Updates:	8551
Category:	Standards Track
Published:	June 2025
ISSN:	2070-1721
Authors:	D. K. Gillmor	B. Hoeneisen	A. Melnikov
---	---	---	---
	American Civil Liberties Union	*pEp Project*	*Isode Ltd*

RFC 9788
Header Protection for Cryptographically Protected Email

Abstract

S/MIME version 3.1 introduced a mechanism to provide end-to-end cryptographic protection of email message headers. However, few implementations generate messages using this mechanism, and several legacy implementations have revealed rendering or security issues when handling such a message.

This document updates the S/MIME specification (RFC 8551) to offer a different mechanism that provides the same cryptographic protections but with fewer downsides when handled by legacy clients. Furthermore, it offers more explicit usability, privacy, and security guidance for clients when generating or handling email messages with cryptographic protection of message headers.

The Header Protection scheme defined here is also applicable to messages with PGP/MIME (Pretty Good Privacy with MIME) cryptographic protections.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9788.

Copyright Notice

Table of Contents

1. Introduction

Privacy and security issues regarding email Header Protection in S/MIME and PGP/MIME have been identified for some time. Most current implementations of cryptographically protected email protect only the Body of the message, which leaves significant room for attacks against otherwise-protected messages. For example, lack of Header Protection allows an attacker to substitute the message subject and/or author.

This document describes how to cryptographically protect message headers and provides guidance for the implementer of a Mail User Agent (MUA) that generates, interprets, and replies to such a message. It uses the term "Legacy MUA" to refer to an MUA that does not implement this specification. This document takes particular care to ensure that messages interact reasonably well with Legacy MUAs.

1.1. Update to RFC 8551

An older scheme for Header Protection was specified in S/MIME 3.1 [RFC8551], which involves wrapping a `message/rfc822` MIME object with a Cryptographic Envelope around the message to protect it. This document refers to that scheme as "RFC 8551 Header Protection", or "RFC8551HP". Substantial testing has shown that RFC8551HP does not interact well with some Legacy MUAs (see Section 1.1.1).

This specification supersedes RFC8551HP, effectively replacing the final two paragraphs of Section 3.1 of [RFC8551].

In this specification, all Header Fields gain end-to-end cryptographic integrity and authenticity by being copied directly into the Cryptographic Payload without using an intervening `message/rfc822` MIME object. In an encrypted message, some Header Fields can also be made confidential by removing or obscuring them from the Outer Header Section.

This specification also offers substantial security, privacy, and usability guidance for sending and receiving MUAs that was not considered in [RFC8551].

1.1.1. Problems with RFC 8551 Header Protection

Several Legacy MUAs have difficulty rendering a message that uses RFC8551HP. These problems can appear on signed-only messages, as well as signed-and-encrypted messages.

In some cases, some MUAs cannot render `message/rfc822` message subparts at all, which is in violation of baseline MIME requirements as defined in requirement 6 of Section 2 of [RFC2049]. A message using RFC8551HP is unreadable by any recipient using such an MUA.

In other cases, the user sees an attachment suggesting a forwarded email message that -- in fact -- contains the protected email message that should be rendered directly. In most of these cases, the user can click on the attachment to view the protected message.

However, viewing the protected message as an attachment in isolation may strip it of any security indications, leaving the user unable to assess the cryptographic properties of the message. Worse, for encrypted messages, interacting with the protected message in isolation may leak contents of the cleartext, for example, if the reply is not also encrypted.

Furthermore, RFC8551HP lacks any discussion of the following points, all of which are provided in this specification:

- Which Header Fields should be given end-to-end cryptographic integrity and authenticity protections (this specification mandates protection of all Header Fields that the sending MUA knows about).
- How to securely indicate the sender's intent to offer Header Protection and encryption, which lets a receiving MUA detect messages whose cryptographic properties may have been modified in transit (see Section 2.1.1).
- Which Header Fields should be given end-to-end cryptographic confidentiality protections in an encrypted message and how (see Section 3).
- How to securely indicate the sender's choices about which Header Fields were made confidential, which lets a receiving MUA reply or forward an encrypted message safely without accidentally leaking confidential material (see Section 2.2).

These stumbling blocks with Legacy MUAs, missing mechanisms, and missing guidance create a strong disincentive for existing MUAs to generate messages using RFC8551HP. Because few messages have been produced, there has been little incentive for those MUAs capable of upgrading to bother interpreting them better.

In contrast, the mechanisms defined here are safe to adopt and produce messages with very few problems for Legacy MUAs. And Section 4.10 provides useful guidance for rendering and replying to RFC8551HP messages.

1.2. Risks of Header Protection for Legacy MUA Recipients

Producing a signed-only message using this specification is risk free. Such a message will render in the same way on any Legacy MUA as a Legacy Signed Message (that is, a signed message without Header Protection). An MUA conformant to this specification that encounters such a message will be able to gain the benefits of end-to-end cryptographic integrity and authenticity for all Header Fields.

An encrypted message produced according to this specification that has some User-Facing Header Fields removed or obscured may not render as desired in a Legacy MUA. In particular, those Header Fields that were made confidential will not be visible to the user of a Legacy MUA. For example, if the `Subject` Header Field outside the Cryptographic Envelope is replaced with `[...]`, a Legacy MUA will render the `[...]` anywhere the `Subject` is normally seen. This is the only risk of producing an encrypted message according to this specification.

A workaround "Legacy Display" mechanism is provided in this specification (see Section 2.1.2). Legacy MUAs will render "Legacy Display Elements" to the user, albeit not in the same location that the Header Fields would normally be rendered.

Alternately, if the sender of an encrypted message is particularly concerned about the experience of a recipient using a Legacy MUA, and they are willing to accept leaking the User-Facing Header Fields, they can simply adopt the No Header Confidentiality Policy (see Section 3.2.3). A signed-and-encrypted message composed using the No Header Confidentiality Policy offers no usability risk for a reader using a Legacy MUA and retains end-to-end cryptographic integrity and authenticity properties for all Header Fields for any reader using a conformant MUA. Of course, such a message has the same (non-existent) confidentiality properties for all Header Fields as a Legacy Encrypted Message (that is, an encrypted message made without Header Protection).

1.3. Motivation

Ordinary Users generally do not understand the distinction between email message Body and Header Section. When an email message has cryptographic protections that cover the message Body but not the Header Fields, several attacks become possible.

For example, a Legacy Signed Message has a signature that covers the Body but not the Header Fields. An attacker can therefore modify the Header Fields (including Subject) without invalidating the signature. Since most readers consider a message Body in the context of the message's Subject, the meaning of the message itself could change drastically (under the attacker's control) while still retaining the same cryptographic indicators of integrity and authenticity.

In another example, a Legacy Encrypted Message has its Body effectively hidden from an adversary that snoops on the message. But if the Header Fields are not also encrypted, significant information about the message (such as the message Subject) will leak to the inspecting adversary.

However, if the sending and receiving MUAs ensure that cryptographic protections cover the message Header Section as well as the message Body, these attacks are defeated.

1.3.1. Backward Compatibility

If the sending MUA is unwilling to generate such a fully protected message due to the potential for rendering, usability, deliverability, or security issues, these defenses cannot be realized.

The sender cannot know what MUA (or MUAs) the recipient will use to handle the message. Thus, an outbound message format that is backward compatible with as many legacy implementations as possible is a more effective vehicle for providing the whole-message cryptographic protections described above.

This document aims for backward compatibility with Legacy MUAs to the extent possible. In some cases, like when a user-visible Header Field like the Subject is cryptographically hidden, a Legacy MUA will not be able to render or reply to the message exactly the same way as a conformant MUA would. But accommodations are described here that ensure a rough semantic equivalence for a Legacy MUA even in these cases.

1.3.2. Deliverability

A message with perfect cryptographic protections that cannot be delivered is less useful than a message with imperfect cryptographic protections that can be delivered. Senders want their messages to reach the intended recipients.

Given the current state of the Internet mail ecosystem, encrypted messages in particular cannot shield all of their Header Fields from visibility and still be guaranteed delivery to their intended recipient.

This document accounts for this concern by providing a mechanism (Section 3) that prioritizes initial deliverability (at the cost of some header leakage) while facilitating future message variants that shield more header metadata from casual inspection.

1.4. Other Protocols to Protect Email Header Fields

A separate pair of protocols also provides some cryptographic protection for the email message header integrity: DomainKeys Identified Mail (DKIM) [RFC6376], as used in combination with Domain-based Message Authentication, Reporting, and Conformance (DMARC) [RFC7489]. This pair of protocols provides a domain-based reputation mechanism that can be used to mitigate some forms of unsolicited email (spam).

However, the DKIM+DMARC suite provides cryptographic protection at a different scope, as it is usually applied by and evaluated by a mail transport agent (MTA). DKIM+DMARC typically provide MTA-to-MTA protection, whereas this specification provides MUA-to-MUA protection. This is because DKIM+DMARC are typically applied to messages by (and interpreted by) MTAs, whereas the mechanisms in this document are typically applied and interpreted by MUAs.

A receiving MUA that relies on DKIM+DMARC for sender authenticity should note Section 10.1.

Furthermore, the DKIM+DMARC suite only provides cryptographic integrity and authentication, not encryption. So cryptographic confidentiality is not available from that suite.

The DKIM+DMARC suite can be used on any message, including messages formed as defined in this document. There should be no conflict between DKIM+DMARC and the specification here.

Though not strictly email, similar protections have been in use on Usenet for the signing and verification of message Header Fields for years. See [PGPCONTROL] and [PGPVERIFY-FORMAT] for more details. Like DKIM, these Usenet control protections offer only integrity and authentication, not confidentiality.

1.5. Applicability to PGP/MIME

This document specifies end-to-end cryptographic protections for email messages in reference to S/MIME [RFC8551].

Comparable end-to-end cryptographic protections can also be provided by PGP/MIME [RFC3156].

The mechanisms in this document should be applicable in the PGP/MIME protections as well as S/MIME protections, but analysis and implementation in this document focuses on S/MIME.

To the extent that any divergence from the mechanism defined here is necessary for PGP/MIME, that divergence is out of scope for this document.

1.6. Requirements Language

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.7. Terms

The following terms are defined for the scope of this document:

S/MIME: Secure/Multipurpose Internet Mail Extensions (see [RFC8551])

PGP/MIME: Pretty Good Privacy with MIME (see [RFC3156])

Message: An email message consisting of Header Fields (collectively called "the Header Section of the message") optionally followed by a message Body; see [RFC5322].

Note: To avoid ambiguity, this document avoids using the terms "Header" or "Headers" in isolation, but instead always uses "Header Field" to refer to the individual field and "Header Section" to refer to the entire collection.

Header Field: A Header Field includes a field name, followed by a colon (":"), followed by a field Body (value), and is terminated by CRLF; see Section 2.2 of [RFC5322] for more details.

Header Section: The Header Section is a sequence of lines of characters with special syntax as defined in [RFC5322]. The Header Section of a message contains the Header Fields associated with the message itself. The Header Section of a MIME part (that is, a subpart of a message) typically contains Header Fields associated with that particular MIME part.

Outer Header Section: The unprotected Header Section that MTAs and MUAs unaware of Header Protection treat as the Header Section of the Message.

Body: The Body is the part of a message that follows the Header Section and is separated from the Header Section by an empty line (that is, a line with nothing preceding the CRLF); see [RFC5322]. It is the (bottom) section of a message containing the payload of a message. Typically, the Body consists of a (possibly multipart) MIME [RFC2045] construct.

Header Protection (HP): The cryptographic protection of email Header Sections (or parts of it) by means of signatures and/or encryption.

Legacy MUA: An MUA that does not understand Header Protection as defined in this document. A Legacy Non-Crypto MUA is incapable of doing any end-to-end cryptographic operations. A Legacy Crypto MUA is capable of doing cryptographic operations but does not understand or generate messages with Header Protection.

Legacy Signed Message: An email message that was signed by a Legacy MUA and therefore has no cryptographic authenticity or integrity protections on its Header Fields.

Legacy Encrypted Message: An email message that was signed and encrypted by a Legacy MUA and therefore has no cryptographic authenticity, integrity, or confidentiality protections on any of its Header Fields.

Header Confidentiality Policy (HCP): A functional specification of which Header Fields should be removed or obscured when composing an encrypted message with Header Protection. An HCP is considered more "conservative" when it removes or obscures fewer Header Fields. When it removes or obscures more Header Fields, it is more "ambitious". See Section 3.

Ordinary User: A user of an MUA who follows a simple and minimal experience, focused on sending and receiving emails. A user who opts into advanced configuration, expert mode, or the like is not an "Ordinary User".

Additionally, Cryptographic Layer, Cryptographic Payload, Cryptographic Envelope, Cryptographic Summary, Structural Header Fields, Non-Structural Header Fields, Main Body Part, User-Facing Header Fields, and MUA are all used as defined in [RFC9787].

The policies "Specification Required" and "IETF Review" that appear in this document when used to describe namespace allocation are to be interpreted as described in [RFC8126].

1.8. Document Scope

This document describes sensible, simple behavior for a program that generates an email message with standard end-to-end cryptographic protections, following the guidance in [RFC9787]. An implementation conformant to this document will produce messages that have cryptographic protection that covers the message's Header Fields as well as its Body.

1.8.1. In Scope

This document also describes sensible, simple behavior for a program that interprets such a message in a way that can take advantage of these protections covering the Header Fields as well as the Body.

The message generation guidance aims to minimize negative interactions with any Legacy receiving MUA while providing actionable cryptographic properties for modern receiving MUAs.

In particular, this document focuses on two standard types of cryptographic protection that cover the entire message:

- a cleartext message with a single signature and
- an encrypted message that contains a single cryptographic signature.

1.8.2. Out of Scope

The message composition guidance in this document (in Section 5.2) aims to provide minimal disruption for any Legacy MUA that receives such a message. However, by definition, a Legacy MUA does not implement any of the guidance here. Therefore, the document does not attempt to provide guidance for Legacy MUAs directly.

Furthermore, this document does not explicitly contemplate other variants of cryptographic message protections, including any of these:

- encrypted-only message (without a cryptographic signature; see Section 5.3 of [RFC9787])
- triple-wrapped message
- signed message with multiple signatures
- encrypted message with a cryptographic signature outside the encryption

All such messages are out of scope of this document.

1.9. Example

This section gives an overview by providing an example of how MIME messages with Header Protection look.

Consider the following MIME message:

```
A └─ application/pkcs7-mime; smime-type="enveloped-data"
  ↧(decrypts to)
B   └─ application/pkcs7-mime; smime-type="signed-data"
  ⇩(unwraps to)
C     └─┬ multipart/alternative; hp="cipher"
D       ├─ text/plain; hp-legacy-display="1"
E       └─ text/html; hp-legacy-display="1"
```

Observe that:

- Nodes A and B are collectively called the Cryptographic Envelope. Node C (including its subnodes D and E) is called the Cryptographic Payload [RFC9787].
- Node A contains the unprotected ("outer") Header Fields. Node C contains the protected ("inner") Header Fields.
- The presence of the `hp` attribute (see Section 2.1.1) on the `Content-Type` of node C allows the receiver to know that the sender applied Header Protection. Its value allows the receiver to distinguish whether the sender intended for the message to be confidential (`hp="cipher"`) or not (`hp="clear"`), since encryption may have been added in transit (see Section 10.2).

The "outer" Header Section on node A looks as follows:

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: [...]
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Type: application/pkcs7-mime; smime-type="enveloped-data"
MIME-Version: 1.0
```

The "inner" Header Section on node C looks as follows:

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: Handling the Jones contract
Keywords: Contract, Urgent
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Type: multipart/alternative; hp="cipher"
MIME-Version: 1.0
HP-Outer: Date: Wed, 11 Jan 2023 16:08:43 -0500
HP-Outer: From: Bob <bob@example.net>
HP-Outer: To: Alice <alice@example.net>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <20230111T210843Z.1234@lhp.example>
```

Observe that:

- Between node C and node A, some Header Fields are copied as is (`Date`, `From`, `To`, `Message-ID`), some are obscured (`Subject`), and some are removed (`Keywords`).
- The `HP-Outer` Header Fields (see Section 2.2) of node C contain a protected copy of the Header Fields in node A. The copy allows the receiver to recompute for which Header Fields the sender provided confidentiality by removing or obscuring them.
- The copying/removing/obscuring and the `HP-Outer` only apply to Non-Structural Header Fields, not to Structural Header Fields like `Content-Type` or `MIME-Version` (see Section 1.1 of [RFC9787]).

- If the sender intends no confidentiality and doesn't encrypt the message, it doesn't remove or obscure Header Fields. All Non-Structural Header Fields are copied as is. No `HP-Outer` Header Fields are present.

Node D looks as follows:

```
Content-Type: text/plain; charset="us-ascii"; hp-legacy-display="1";

Subject: Handling the Jones contract
Keywords: Contract, Urgent

Please review and approve or decline by Thursday, it's critical!

Thanks,
Bob

--
Bob Gonzalez
ACME, Inc.
```

Observe that:

- The sender adds the removed and obscured User-Facing Header Fields (see Section 1.1.2 of [RFC9787]) to the main Body (note the empty line after the Content-Type). This is called the Legacy Display Element. It allows a user with a Legacy MUA that doesn't implement this document to understand the message, since the Header Fields will be shown as part of the main Body.
- The `hp-legacy-display="1"` attribute (see Section 2.1.2) indicates that the sender added a Legacy Display Element. This allows receivers that implement this document to recognize the Legacy Display Element and distinguish it from user-added content. The receiver then hides the Legacy Display Element and doesn't display it to the user.
- `hp-legacy-display` is added to the node to which it applies, not on any outer nodes (e.g., not to node C).

For more examples, see Appendices D and E.

2. Internet Message Format Extensions

This section describes relevant, backward-compatible extensions to the Internet Message Format [RFC5322]. Subsequent sections offer concrete guidance for an MUA to make use of these mechanisms, including policy decisions and recommended pseudocode.

2.1. Content-Type Parameters

This document introduces two parameters for the `Content-Type` Header Field, which have distinct semantics and use cases.

2.1.1. Content-Type Parameter: hp

This specification defines a parameter for the `Content-Type` Header Field named `hp` (for Header Protection). This parameter is only relevant on the `Content-Type` Header Field at the root of the Cryptographic Payload. The presence of this parameter at the root of the Cryptographic Payload indicates that the sender intends for this message to have end-to-end cryptographic protections for the Header Fields.

The parameter's defined values describe the sender's cryptographic intent when producing the message:

hp Value	Authenticity	Integrity	Confidentiality	Description
`"clear"`	yes	yes	no	This message has been signed by the sender, with Header Protection.
`"cipher"`	yes	yes	yes	This message has been signed by the sender, with Header Protection, and is encrypted to the recipients.

Table 1: hp Parameter for Content-Type Header Field

A sending implementation **MUST NOT** produce a Cryptographic Payload with parameter `hp="cipher"` for an unencrypted message (that is, where none of the Cryptographic Layers in the Cryptographic Envelope of the message provide encryption). Likewise, if a sending implementation is sending an encrypted message with Header Protection, it **MUST** emit an `hp="cipher"` parameter, regardless of which Header Fields were made confidential.

Note that `hp="cipher"` indicates that the message itself has been encrypted by the sender to the recipients but makes no assertions about which Header Fields have been removed or obscured. This can be derived from the Cryptographic Payload itself (see Section 4.2).

A receiving implementation **MUST NOT** mistake the presence of an `hp="cipher"` parameter in the Cryptographic Payload for the actual presence of a Cryptographic Layer that provides encryption.

2.1.2. Content-Type Parameter: hp-legacy-display

This specification also defines an `hp-legacy-display` parameter for the `Content-Type` Header Field. The only defined value for this parameter is `1`.

This parameter is only relevant on a leaf MIME node of `Content-Type` `text/html` or `text/plain` within a well-formed message with end-to-end cryptographic protections. Its presence indicates that the MIME node it is attached to contains a decorative "Legacy Display Element". The Legacy Display Element itself is used for backward-compatible visibility of any removed or obscured User-Facing Header Field in a Legacy MUA.

Such a Legacy Display Element need not be rendered to the user of an MUA that implements this specification, because the MUA already knows the correct Header Field information and can render it to the user in the appropriate part of the MUA's user interface rather than in the Body of the message.

See Section 5.2.2 for how to insert a Legacy Display Element into a `text/plain` Main Body Part.
See Section 5.2.3 for how to insert a Legacy Display Element into a `text/html` Main Body Part.
See Section 4.5.3 for how to avoid rendering a Legacy Display Element.

2.2. HP-Outer Header Field

This document also specifies a new Header Field: `HP-Outer`.

This Header Field is used only in the Header Section of the Cryptographic Payload of an encrypted message. It is not relevant for signed-only messages. It documents, with the same cryptographic guarantees shared by the rest of the message, the sender's choices about Header Field confidentiality. It does so by embedding a copy within the Cryptographic Envelope of every Non-Structural Header Field that the sender put outside the Cryptographic Envelope. This Header Field enables the MUA receiving the encrypted message to reliably identify whether the sending MUA intended to make a Header Field confidential (see Section 11.3).

The `HP-Outer` Header Fields in a message's Cryptographic Payload are useful for ensuring that any confidential Header Field will not be automatically leaked in the clear if the user replies to or forwards the message. They may also be useful for an MUA that indicates the confidentiality status of any given Header Field to the user.

An implementation that composes encrypted email **MUST** include a copy of all Non-Structural Header Fields deliberately exposed to the outside of the Cryptographic Envelope using a series of `HP-Outer` Header Fields within the Cryptographic Payload. These `HP-Outer` MIME Header Fields should only ever appear directly within the Header Section of the Cryptographic Payload of a Cryptographic Envelope offering confidentiality. They **MUST** be ignored for the purposes of evaluating the message's Header Protection if they appear in other places.

Each instance of `HP-Outer` contains a Non-Structural Header Field name and the value that this Header Field was set to within the outer (unprotected) Header Section. The `HP-Outer` Header Field can appear multiple times in the Header Section of a Cryptographic Payload.

If a Non-Structural Header Field named `Z` is present in Header Section of the Cryptographic Payload but doesn't appear in an `HP-Outer` Header Field value at all, then the sender is effectively asserting that every instance of `Z` was made confidential by removal from the Outer Header Section. Specifically, it means that no Header Field `Z` was included on the outside of the message's Cryptographic Envelope by the sender at the time the message was injected into the mail system.

See Section 5.2 for how to insert `HP-Outer` Header Fields into an encrypted message. See Section 4.3 for how to determine the end-to-end confidentiality of a given Header Field from an encrypted message with Header Protection using `HP-Outer`. See Section 6.1 for how an MUA can safely reply to (or forward) an encrypted message without leaking confidential Header Fields by default.

2.2.1. HP-Outer Header Field Definition

The syntax of this Header Field is defined using the following ABNF [RFC5234], where `field-name`, `WSP`, `VCHAR`, and `FWS` are defined in [RFC5322]:

```
hp-outer      =   "HP-Outer:" [FWS] field-name ": "
                     hp-outer-value CRLF

hp-outer-value  =   (*([FWS] VCHAR) *WSP)
```

Note that `hp-outer-value` is the same as `unstructured` from Section 3.2.5 of [RFC5322] but without the obsolete `obs-unstruct` option.

3. Header Confidentiality Policy

An MUA composing an encrypted message according to this specification may make any given Header Field confidential by removing it from the Header Section outside the Cryptographic Envelope or by obscuring it by rewriting it to a different value in that Outer Header Section. The composing MUA faces a choice for any new message: Which Header Fields should be made confidential, and how?

This section defines the "Header Confidentiality Policy" (or HCP) as a well-defined abstraction to encourage MUA developers to consider, document, and share reasonable policies across the community. It establishes a registry of known HCPs, defines a small number of simple HCPs in that registry, and makes a recommendation for a reasonable default.

Note that such a policy is only needed when the end-to-end protections include encryption (confidentiality). No comparable policy is needed for other end-to-end cryptographic protections (integrity and authenticity), as they are simply uniformly applied so that all Header Fields known by the sender have these protections.

This asymmetry is a consequence of complexities in existing message delivery systems, some of which may reject, drop, or delay messages where all Header Fields are removed from the top-level MIME object.

Note that no representation of the HCP itself ever appears "on the wire". However, the consumer of the encrypted message can see the decisions that were made by the sender's HCP via the `HP-Outer` Header Fields (see Section 2.2).

3.1. HCP Definition

In this document, we represent that HCP as a function `hcp`:

- `hcp(name, val_in) -> val_out`: This function takes a Non-Structural Header Field identified by `name` with the initial value `val_in` as arguments and returns a replacement Header Field value `val_out`. If `val_out` is the special value `null`, it means that the Header Field in question should be removed from the set of Header Fields visible outside the Cryptographic Envelope.

In the pseudocode descriptions of various choices of HCP in this document, any comparison with the `name` input is done case-insensitively. This is appropriate for Header Field names, as described in [RFC5322].

Note that `hcp` is only applied to Non-Structural Header Fields. When composing a message, Structural Header Fields are dealt with separately, as described in Section 5.2.

As an example, an MUA that obscures the `Subject` Header Field by replacing it with the literal string "`[...]`", hides all `Cc`'ed recipients, and does not offer confidentiality to any other Header Fields would be represented as (in pseudocode):

```
hcp_example_hide_cc(name, val_in) → val_out:
    if lower(name) is 'subject':
        return '[...]'
    else if lower(name) is 'cc':
        return null
    else:
        return val_in
```

For alignment with common practice as well as the ABNF in Section 2.2.1 for `HP-Outer`, `val_out` **MUST** be one of the following:

- identical to `val_in`,
- the special value `null` (meaning that the Header Field will be removed from the outside of the message), or
- a sequence of whitespace (that is, space or tab) and printable 7-bit clean ASCII characters (of course, non-ASCII text can be encoded as ASCII using the `encoded-word` construct from [RFC2047])

The HCP can compute `val_out` using any technique describable in pseudocode, such as copying a fixed string or invocations of other pseudocode functions. If it alters the value, it **MUST NOT** include control or NUL characters in `val_out`. `val_out` **SHOULD** match the expected ABNF for the Header Field identified by `name`.

3.1.1. HCP Avoids Changing addr-spec of From Header Field

The `From` Header Field should also be treated specially by the HCP to enable defense against possible email address spoofing (see Section 10.1). In particular, for `hcp("From", val_in)`, the `addr-spec` of `val_in` and the `addr-spec` of `val_out` **SHOULD** match according to Section 4.4.5, unless the sending MUA has additional knowledge coordinated with the receiving MUA about more subtle `addr-spec` equivalence or certificate validity.

3.2. Initial Registered HCPs

This document formally defines three Header Confidentiality Policies with known and reasonably well-understood characteristics as a way to compare and contrast different possible behavioral choices for a composing MUA. These definitions are not meant to preclude the creation of other HCPs.

The purpose of the registry of HCPs is to facilitate HCP evolution and interoperability discussion among MUA developers and MTA operators.

(The example hypothetical HCP, `hcp_example_hide_cc`, described in Section 3.1 above is deliberately not formally registered, as it has not been evaluated in practice.)

3.2.1. Baseline Header Confidentiality Policy

The most conservative recommended HCP only provides confidentiality for Informational Fields, as defined in Section 3.6.5 of [RFC5322]. These fields are "only human-readable content" and thus their content should not be relevant to transport agents. Since most Internet messages today do have a `Subject` Header Field, and some filtering engines might object to a message without a `Subject`, this policy is conservative and merely obscures that Header Field by replacing it with a fixed string `[...]`. By contrast, `Comments` and `Keywords` Header Fields are comparatively rare, so these fields are removed entirely from the Outer Header Section.

```
hcp_baseline(name, val_in) → val_out:
    if lower(name) is 'subject':
        return '[...]'
    else if lower(name) is in ['comments', 'keywords']:
        return null
    else:
        return val_in
```

`hcp_baseline` is the recommended default HCP for a new implementation, as it provides meaningful confidentiality protections and is unlikely to cause deliverability or usability problems.

3.2.2. Shy Header Confidentiality Policy

Alternately, a slightly more ambitious (and therefore more privacy-preserving) HCP might avoid leaking human-interpretable data that MTAs generally don't care about. The additional protected data isn't related to message routing or transport but might reveal sensitive information about the sender or their relationship to the recipients. This "shy" HCP builds on `hcp_baseline` but also:

- avoids revealing the `display-name` of each identified email address and
- avoids leaking the sender's locally configured time zone in the `Date` Header Field.

```
hcp_shy(name, val_in) → val_out:
   if lower(name) is 'from':
      if val_in is an RFC 5322 mailbox:
         return the RFC 5322 addr-spec part of val_in
   if lower(name) in ['to', 'cc']:
      if val_in is an RFC 5322 mailbox-list:
         let val_out be an empty mailbox-list
         for each mailbox in val_in:
            append the RFC 5322 addr-spec part of mailbox to val_out
         return val_out
   if lower(name) is 'date':
      if val_in is an RFC 5322 date-time:
          return the UTC form of val_in
   else if lower(name) is 'subject':
      return '[...]'
   else if lower(name) is in ['comments', 'keywords']:
      return null
   return val_in
```

`hcp_shy` requires more sophisticated parsing and Header Field manipulation and is not recommended as a default HCP for new implementations.

3.2.3. No Header Confidentiality Policy

Legacy MUAs can be conceptualized as offering a "No Header Confidentiality" Policy, which offers no confidentiality protection to any Header Field:

```
hcp_no_confidentiality(name, val_in) → val_out:
    return val_in
```

A conformant MUA that is not modified by local policy or configuration **MUST NOT** use `hcp_no_confidentiality` by default.

3.3. Default Header Confidentiality Policy

An MUA **MUST** have a default HCP that offers confidentiality for the `Subject` Header Field at least. Local policy and configuration may alter this default, but the MUA **SHOULD NOT** require the user to select an HCP.

`hcp_baseline` provides confidentiality for the `Subject` Header Field by replacing it with the literal string "`[...]`". It also provides confidentiality for the other less common Informational Header Fields (`Comments` and `Keywords`) by removing them entirely from the Outer Header Section. This is a sensible default because most users treat the Informational Fields of a message (particularly the Subject) the same way that they treat the Body, and they are surprised to find that the Subject of an encrypted message is visible.

3.4. HCP Evolution

This document does not mandate any particular HCP, though it offers guidance for MUA implementers in selecting one in Section 3.3. Future documents may recommend or mandate such a policy for an MUA with specific needs. Such a recommendation might be motivated by descriptions of metadata-derived attacks, stem from research about message deliverability, or describe new signaling mechanisms, but these topics are out of scope for this document.

3.4.1. Offering More Ambitious Header Confidentiality

An MUA **MAY** offer even more ambitious confidentiality for Header Fields of an encrypted message than defined in Section 3.2.2. For example, it might implement an HCP that removes the `To` and `Cc` Header Fields entirely, relying on the SMTP envelope to ensure proper routing. Or it might remove `References` and `In-Reply-To` so that message threading is not visible to any MTA. Any more ambitious choice might result in deliverability, rendering, or usability issues for the relevant messages, so testing and documentation will be valuable to get this right.

The authors of this document hope that implementers with deployment experience will document their chosen HCP and the rationale behind their choice.

3.4.2. Expert Guidance for Registering Header Confidentiality Policies

There is no formal syntax specified for the HCP, but any attempt to specify an HCP for inclusion in the registry needs to provide:

- a stable reference document clearly indicating the distinct name for the proposed HCP,
- pseudocode that other implementers can clearly and unambiguously interpret,
- a clear explanation of why this HCP is different from all other registered HCPs, and
- any relevant considerations related to deployment of the HCP (for example, known or expected deliverability, rendering, or privacy challenges and possible mitigations).

When the proposed HCP produces any non-`null` output for a given Header Field name, `val_out` **SHOULD** match the expected ABNF for that Header Field. If the proposed HCP does not match the expected ABNF for that Header Field, the documentation should explicitly identify the relevant circumstances and provide a justification for the deviation.

An entry should not be marked as "Recommended" unless it has been shown to offer confidentiality or privacy improvements over the status quo and have minimal or mitigable negative impact on messages to which it is applied, considering factors such as message deliverability and security. Only one entry in the table (`hcp_baseline`) is initially marked as "Recommended". In the future, more than one entry may be marked as "Recommended".

4. Receiving Guidance

An MUA that receives a cryptographically protected email will render it for the user.

The receiving MUA will render the message Body, render a selected subset of Header Fields, and (as described in Section 3 of [RFC9787]) provide a summary of the cryptographic properties of the message.

Most MUAs only render a subset of Header Fields by default. For example, most MUAs render the `From`, `To`, `Cc`, `Date`, and `Subject` Header Fields to the user, but few render `Message-Id` or `Received`.

An MUA that knows how to handle a message with Header Protection makes the following four changes to its behavior when rendering a message:

- If the MUA detects that an incoming message has protected Header Fields:
  - For a Header Field that is present in the protected Header Section, the MUA **SHOULD** render the protected value and ignore any unprotected counterparts that may be present (with a special exception for the `From` Header Field (see Section 4.4)).
  - For a Header Field that is present only in the Outer Header Section, the MUA **SHOULD NOT** render that value. If it does render the value, the MUA **SHOULD** indicate that the rendered value is `unprotected`. For an exception to this, see Section 7 for a discussion of some specific Header Fields that are known to be added in transit and therefore are not expected to have end-to-end cryptographic protections.
- The MUA **SHOULD** include information in the message's Cryptographic Summary to indicate the types of protection that applied to each rendered Header Field (if any).
- If any Legacy Display Elements are present in the Body of the message, it does not render them.
- When replying to a message with confidential Header Fields, the replying MUA avoids leaking any Header Fields that were confidential in the original into the cleartext of the reply. It does this even if its own HCP would not have treated those Header Fields as confidential. See Section 6 for more details.

Note that an MUA that handles a message with Header Protection does *not* need to render any new Header Fields that it did not render before.

4.1. Identifying That a Message Has Header Protection

An incoming message can be identified as having Header Protection using the following test:

- The Cryptographic Payload has parameter `hp` set to `"clear"` or `"cipher"`. See Section 4.5 for rendering guidance.

When consuming a message, an MUA **MUST** ignore the `hp` parameter to `Content-Type` when it encounters it anywhere other than the root of the message's Cryptographic Payload.

4.2. Extracting Protected and Unprotected ("Outer") Header Fields

When a message is encrypted and uses Header Protection, an MUA extracts a list of protected Header Fields (names and values), as well as a list of Header Fields that were added by the original message sender in unprotected form to the outside of the message's Cryptographic Envelope.

The following algorithm takes reference message `refmsg` as input, which is encrypted with Header Protection as described in this document (that is, the Cryptographic Envelope includes a Cryptographic Layer that provides encryption, and the `hp` parameter for the `Content-Type` Header Field of the Cryptographic Payload is `cipher`). It produces as output a pair of lists of `(h, v)` Header Fields.

4.2.1. HeaderSetsFromMessage

Method signature:

```
HeaderSetsFromMessage(refmsg) -> (refouter, refprotected)
```

Procedure:

1. Let `refheaders` be the list of `(h, v)` protected Header Fields found in the root of the Cryptographic Payload.
2. Let `refouter` be an empty list of Header Field names and values.
3. Let `refprotected` be an empty list of Header Field names and values.
4. For each `(h, v)` in `refheaders`:
   i. If `h` is `HP-Outer`:
      a. Split `v` into `(h1, v1)` on the first colon (:), followed by any amount of whitespace.
      b. Append `(h1, v1)` to `refouter`.
   ii. Else:
      a. Append `(h, v)` to `refprotected`.
5. Return `refouter`, `refprotected`.

Note that this algorithm is independent of the unprotected Header Fields. It derives its output only from the normal Header Fields and the `HP-Outer` Header Fields, both contained inside the Cryptographic Payload.

4.3. Updating the Cryptographic Summary

Regardless of whether a cryptographically protected message has protected Header Fields, the Cryptographic Summary of the message should be modified to indicate what protections the Header Fields have. This field-by-field status is complex and isn't necessarily intended to be presented in full to the user. Rather, it represents the state of the message internally within the MUA and may be used to influence behavior like replying to the message (see Section 6.1).

Each Header Field individually has exactly one of the following protection states:

- `unprotected` (has no Header Protection)
- `signed-only` (bound into the same validated signature as the enclosing message, but also visible in transit)
- `encrypted-only` (only appears within the Cryptographic Payload; the corresponding external Header Field was either removed or obscured)
- `signed-and-encrypted` (same as encrypted-only, but additionally is under a validated signature)

If the message does not have Header Protection (as determined by Section 4.1), then all of the Header Fields are by definition `unprotected`.

If the message has Header Protection, an MUA **SHOULD** use the following algorithm to compute the protection state of a protected Header Field `(h,v)` (that is, an element of `refprotected` from Section 4.2):

4.3.1. HeaderFieldProtection

Method signature:

```
HeaderFieldProtection(msg, h, v) -> protection_state
```

Procedure:

1. Let `ct` be the `Content-Type` of the root of the Cryptographic Payload of `msg`.
2. Compute (`refouter`, `refprotected`) from HeaderSetsFromMessage(`msg`).
3. If `(h, v)` is not in `refprotected`:
   i. Abort, `v` is not a valid value for Header Field `h`.
4. Let `is_sig_valid` be `false`.
5. If the message is signed:
   i. Let `is_sig_valid` be the result of validating the signature.
6. If the message is encrypted, and if `ct` has a parameter `hp="cipher"`, and if `(h,v)` is not in `refouter`:
   i. Return `signed-and-encrypted` if `is_sig_valid`, otherwise return `encrypted-only`.
7. Return `signed-only` if `is_sig_valid`, otherwise return `unprotected`.

Note that:

- This algorithm is independent of the unprotected Header Fields. It derives the protection state only from `(h,v)` and the set of `HP-Outer` Header Fields, both of which are inside the Cryptographic Envelope.

- If the signature fails validation, the MUA lowers the affected state to `unprotected` or `encrypted-only` without any additional warning to the user, as specified by Section 3.1 of [RFC9787].
- Data from `signed-and-encrypted` and `encrypted-only` Header Fields may still not be fully private (see Section 11.2).
- Encryption may have been added in transit to an originally signed-only message. Thus, only consider Header Fields to be confidential if the sender indicates it with the `hp="cipher"` parameter.
- The protection state of a Header Field may be weaker than that of the message Body. For example, a message Body can be `signed-and-encrypted`, but a Header Field that is copied unmodified to the Outer Header Section is `signed-only`.

If the message has Header Protection, Header Fields that are not in `refprotected` (e.g., because they were added in transit) are `unprotected`.

Rendering the cryptographic status of each Header Field is likely to be complex and messy -- users may not understand it. It is beyond the scope of this document to suggest any specific graphical affordances or user experience. Future work should include examples of successful rendering of this information.

4.4. Handling Mismatch of From Header Fields

End-to-end (MUA-to-MUA) Header Protection is good for authenticity, integrity, and confidentiality, but it potentially introduces new issues when an MUA depends on its MTA to authenticate parts of the Header Section. The latter is typically the case in modern email systems.

In particular, when an MUA depends on its MTA to ensure that the email address in the (unprotected) `From` Header Field is authentic, but the MUA renders the email address of the protected `From` Header Field that differs from the address visible to the MTA, this could create a risk of sender address spoofing (see Section 10.1). This potential risk applies to signed-only messages as well as signed-and-encrypted messages.

4.4.1. Definitions

4.4.1.1. From Header Field Mismatch

"`From` Header Field Mismatch" is defined as follows:

The `addr-spec` of the inner `From` Header Field doesn't match the `addr-spec` of the outer `From` Header Field (see Section 4.4.5).

Note: The unprotected `From` Header Field used in this comparison is the actual outer Header Field (as seen by the MTA), not the value indicated by any potential inner `HP-Outer`.

4.4.1.2. No Valid and Correctly Bound Signature

"No Valid and Correctly Bound Signature" is defined as follows:

There is no valid signature made by a certificate for which the MUA has a valid binding to the protected `From` address. This includes:

- the message has no signature
- the message has a broken signature
- the message has a valid signature, but the receiving MUA does not see any valid binding between the signing certificate and the `addr-spec` of the inner `From` Header Field

Note: There are many possible ways that an MUA could choose to validate a certificate-to-address binding. For example, the MUA could ensure the certificate is issued by one of a set of trusted certification authorities, it could rely on the user to do a manual out-of-band comparison, it could rely on a DNSSEC signal ([RFC7929] or [RFC8162]), and so on. It is beyond the scope of this document to describe all possible ways an MUA might validate the certificate-to-address binding or to choose among them.

4.4.2. Warning for From Header Field Mismatch

To mitigate the above described risk of sender address spoofing, an MUA **SHOULD** warn the user whenever both of the following conditions are met:

- `From` Header Field Mismatch (as defined in Section 4.4.1.1) and
- No Valid and Correctly Bound Signature (as defined in Section 4.4.1.2)

This warning should be comparable to the MUA's warning about messages that are likely spam or phishing, and it **SHOULD** show both of the non-matching `From` Header Fields.

4.4.3. From Header Field Rendering

Furthermore, a receiving MUA that depends on its MTA to authenticate the unprotected (outer) `From` Header Field **SHOULD** render the outer `From` Header Field (as an exception to the guidance in the beginning of Section 4) if both of the following conditions are met:

- `From` Header Field Mismatch (as defined in Section 4.4.1.1) and
- No Valid and Correctly Bound Signature (as defined in Section 4.4.1.2)

An MUA **MAY** apply a local preference to render a different display name (e.g., from an address book).

See Section 10.1.1 for a detailed explanation of this rendering guidance.

4.4.4. Handling the Protected From Header Field When Responding

When responding to a message, an MUA has different ways to populate the recipients of the new message. Depending on whether it is a Reply, a Reply All, or a Forward, an MUA may populate the composer view using a combination of the referenced message's `From`, `To`, `Cc`, `Reply-To`, or `Mail-Followup-To` Header Fields or any other signals.

When responding to a message with Header Protection, an MUA **MUST** only use the protected Header Fields when populating the recipients of the new message.

This avoids compromise of message confidentiality when a machine-in-the-middle (MITM) attacker modifies the unprotected `From` address of an encrypted message, attempting to learn the contents through a misdirected reply. Note that with the rendering guidance above, a MITM attacker can cause the unprotected `From` Header Field to be displayed. Thus, when responding, the populated `To` address may differ from the rendered `From` address. However, this change in addresses should not cause more user confusion than the address change caused by a `Reply-To` in a Legacy Message does.

4.4.5. Matching addr-specs

When generating (Section 3.1.1) or consuming (Section 4.4) a protected `From` Header Field, the MUA considers the equivalence of two different `addr-spec` values.

First, the MUA **MUST** check whether the `domain` part of an `addr-spec` being compared contains a U-label [RFC5890]. If it does, it **MUST** be converted to the A-label form as described in [RFC5891]. We call a domain converted in this way (or the original domain if it didn't contain any U-label) "the ASCII version of the `domain` part". Second, the MUA **MUST** compare the ASCII version of the `domain` part of the two `addr-specs` by standard DNS comparison: Assume ASCII text and compare alphabetic characters case-insensitively, as described in Section 3.1 of [RFC1035]. If the `domain` parts match, then the two `local-parts` are matched against each other. The simplest and most common comparison for the `local-part` is also an ASCII-based, case-insensitive match. If the MUA has special knowledge about the `domain` and, when composing, it can reasonably expect the receiving MUAs to have the same information, it **MAY** match the `local-part` using a more sophisticated and inclusive matching algorithm.

It is beyond the scope of this document to recommend a more sophisticated and inclusive matching algorithm.

4.5. Rendering a Message with Header Protection

When the Cryptographic Payload's `Content-Type` has the parameter `hp` set to `"clear"` or `"cipher"`, the values of the protected Header Fields are drawn from the Header Fields of the Cryptographic Payload, and the Body that is rendered is the Cryptographic Payload itself.

4.5.1. Example Signed-Only Message

Consider a message with this structure, where the MUA is able to validate the cryptographic signature:

```
A └─ application/pkcs7-mime; smime-type="signed-data"
  ⇩ (unwraps to)
B   └─┬ multipart/alternative [Cryptographic Payload + Rendered Body]
C     ├── text/plain
D     └── text/html
```

The message Body should be rendered the same way as this message:

```
B └─ multipart/alternative
C   ├─ text/plain
D   └─ text/html
```

The MUA should render Header Fields taken from part `B`.

Its Cryptographic Summary should indicate that the message was signed and all rendered Header Fields were included in the signature.

Because this message is signed-only, none of its parts will have a Legacy Display Element.

The MUA should ignore Header Fields from part `A` for the purposes of rendering.

4.5.2. Example Signed-and-Encrypted Message

Consider a message with this structure, where the MUA is able to validate the cryptographic signature:

```
E └─ application/pkcs7-mime; smime-type="enveloped-data"
  ↧(decrypts to)
F   └─ application/pkcs7-mime; smime-type="signed-data"
   ⇩(unwraps to)
G    └─ multipart/alternative [Cryptographic Payload + Rendered Body]
H     ├─ text/plain
I     └─ text/html
```

The message Body should be rendered the same way as this message:

```
G └─ multipart/alternative
H   ├─ text/plain
I   └─ text/html
```

It should render Header Fields taken from part `G`.

Its Cryptographic Summary should indicate that the message is `signed-and-encrypted`.

When rendering the Cryptographic Status of a Header Field and when composing a reply, each Header Field found in `G` should be considered against all `HP-Outer` Header Fields found in `G`. If an `HP-Outer` Header Field that matches both the name and value is found, the Header Field's Cryptographic Status is just `signed-only`, even though the message itself is `signed-and-encrypted`. If no matching `HP-Outer` Header Field is found, the Header Field's Cryptographic Status is `signed-and-encrypted`, like the rest of the message.

If any of the User-Facing Header Fields are removed or obscured, the composer of this message may have placed Legacy Display Elements in parts H and I.

The MUA should ignore Header Fields from part `E` for the purposes of rendering.

4.5.3. Do Not Render Legacy Display Elements

As described in Section 2.1.2, a message with cryptographic confidentiality protection **MAY** include Legacy Display Elements for backward compatibility with Legacy MUAs. These Legacy Display Elements are strictly decorative and unambiguously identifiable and will be discarded by compliant implementations.

The receiving MUA **MUST** completely avoid rendering the identified Legacy Display Elements to the user, since it is aware of Header Protection and can render the actual protected Header Fields.

If a `text/html` or `text/plain` part within the Cryptographic Envelope is identified as containing Legacy Display Elements, those elements **MUST** be hidden when rendering and **MUST** be dropped when generating a draft reply or inline forwarded message. Whenever a Message or MIME subtree is exported, downloaded, or otherwise further processed, if there is no need to retain a valid cryptographic signature, the implementer **MAY** drop the Legacy Display Elements.

4.5.3.1. Identifying a Part with Legacy Display Elements

A receiving MUA acting on a message that contains an encrypting Cryptographic Layer identifies a MIME subpart within the Cryptographic Payload as containing Legacy Display Elements based on the Content-Type of the subpart. The subpart's Content-Type:

- contains a parameter `hp-legacy-display` with value set to `1` and
- is either `text/html` (see Section 4.5.3.3) or `text/plain` (see Section 4.5.3.2).

Note that the term "subpart" above is used in the general sense: If the Cryptographic Payload is a single part, that part itself may contain a Legacy Display Element if it is marked with the `hp-legacy-display="1"` parameter.

4.5.3.2. Omitting Legacy Display Elements from text/plain

If a `text/plain` part within the Cryptographic Payload has the Content-Type parameter `hp-legacy-display="1"`, it should be processed before rendering in the following fashion:

- Discard the leading lines of the content of the MIME part up to and including the first entirely blank line.

Note that implementing this strategy is dependent on the charset used by the MIME part.

See Appendix E.1 for an example.

4.5.3.3. Omitting Legacy Display Elements from text/html

If a `text/html` part within the Cryptographic Payload has the Content-Type parameter `hp-legacy-display="1"`, it should be processed before rendering in the following fashion:

- If any element of the HTML `<body>` is a `<div>` with `class` attribute `header-protection-legacy-display`, that entire element should be omitted.

This cleanup could be done, for example, as a custom rule in the MUA's HTML sanitizer, if one exists. Another implementation strategy for an HTML-capable MUA would be to add an entry to the [CSS] style sheet for such a part:

```
body div.header-protection-legacy-display { display: none; }
```

4.6. Implicitly Rendered Header Fields

While the `From`, `To`, `Cc`, `Subject`, and `Date` Header Fields are often explicitly rendered to the user, some Header Fields do affect message display without being explicitly rendered.

For example, the `Message-Id`, `References`, and `In-Reply-To` Header Fields may collectively be used to place a message in a "thread" or series of messages.

In another example, Section 6.2 notes that the value of the `Reply-To` Header Field can influence the draft reply message. So while the user may never see the `Reply-To` Header Field directly, it is implicitly "rendered" when the user interacts with the message by replying to it.

An MUA that depends on any implicitly rendered Header Field in a message with Header Protection **MUST** use the value from the protected Header Field and **SHOULD NOT** use any value found outside the cryptographic protection unless it is known to be a Header Field added in transit, as specified in Section 7.

4.7. Handling Undecryptable Messages

An MUA might receive an apparently encrypted message that it cannot currently decrypt. For example, when an MUA does not have regular access to the secret key material needed for decryption, it cannot know the cryptographically protected Header Fields or even whether the message has any cryptographically protected Header Fields.

Such an undecrypted message will be rendered by the MUA as a message without any Header Protection. This means that the message summary may well change how it is rendered when the user is finally able to supply the secret key.

For example, the rendering of the `Subject` Header Field in a mailbox summary might change from `[...]` to the real message subject when the message is decrypted. Or the message's placement in a message thread might change if, say, `References` or `In-Reply-To` have been removed or obscured (see Section 4.6).

Additionally, if the MUA does not retain access to the decrypting secret key, and it drops the decrypted form of a message, the message's rendering may revert to the encrypted form. For example, if an MUA follows this behavior, the `Subject` Header Field in a mailbox summary might change from the real message subject back to `[...]`. Or the message might be displayed outside of its current thread if the MUA loses access to a removed `References` or `In-Reply-To` Header Field.

These behaviors are likely to surprise the user. However, an MUA has several possible ways of reducing or avoiding all of these surprises, including:

- Ensuring that the MUA always has access to decryption-capable secret key material.
- Rendering undecrypted messages in a special quarantine view until the decryption-capable secret key material is available.

To reduce or avoid the surprises associated with a decrypted message with removed or obscured Header Fields becoming undecryptable, the MUA could also:

- Securely cache metadata from a decrypted message's protected Header Fields so that its rendering doesn't change after the first decryption.
- Securely store the session key associated with a decrypted message so that attempts to read the message when the long-term secret key is unavailable can proceed using only the session key itself. For example, see the discussion about stashing session keys in Section 9.1 of [RFC9787].

4.8. Guidance for Automated Message Handling

Some automated systems have a control channel that is operated by email. For example, an incoming email message could subscribe someone to a mailing list, initiate the purchase of a specific product, approve another message for redistribution, or adjust the state of some shared object.

To the extent that such a system depends on end-to-end cryptographic guarantees about the email control message, Header Protection as defined in this document should improve the system's security. This section provides some specific guidance for systems that use email messages as a control channel that want to benefit from these security improvements.

4.8.1. Only Interpret Protected Header Fields

Consider the situation where an email-based control channel depends on the message's cryptographic signature and the action taken depends on some Header Field of the message.

In this case, the automated system **MUST** rely on information from the Header Field that is protected by the mechanism defined in this document. It **MUST NOT** rely on any Header Field found outside the Cryptographic Payload.

For example, consider an administrative interface for a mailing list manager that only accepts control messages that are signed by one of its administrators. When an inbound message for the list arrives, it is queued (waiting for administrative approval) and the system generates and listens for two distinct email addresses related to the queued message -- one that approves the message and one that rejects it. If an administrator sends a signed control message to the approval address, the mailing list verifies that the protected `To` Header Field of the signed control message contains the approval address before approving the queued message for redistribution. If the protected `To` Header Field does not contain that address, or there is no protected `To` Header Field, then the mailing list logs or reports the error and does not act on that control message.

4.8.2. Ignore Legacy Display Elements

Consider the situation where an email-based control channel expects to receive an end-to-end encrypted message -- for example, where the control messages need confidentiality guarantees -- and where the action taken depends on the contents of some MIME part within the message Body.

In this case, the automated system that decrypts the incoming messages and scans the relevant MIME part **MUST** identify when the MIME part contains a Legacy Display Element (see Section 4.5.3.1), and it **MUST** parse the relevant MIME part with the Legacy Display Element removed.

For example, consider an administrative interface of a confidential issue tracking software. An authorized user can confidentially adjust the status of a tracked issue by a specially formatted first line of the message Body (for example, `severity #183 serious`). When the user's MUA encrypts a plaintext control message to this issue tracker, depending on the MUA's HCP and its choice of `legacy` value, it may add a Legacy Display Element. If it does so, then the first line of the message Body will contain a decorative copy of the confidential `Subject` Header Field. The issue tracking software decrypts the incoming control message, identifies that there is a Legacy Display Element in the part (see Section 4.5.3.1), strips the lines comprising the Legacy Display Element (including the first blank line), and only then parses the remaining top line to look for the expected special formatting.

4.9. Affordances for Debugging and Troubleshooting

Note that advanced users of an MUA may need access to the original message, for example, to troubleshoot problems with the rendering MUA itself or problems with the SMTP transport path taken by the message.

An MUA that applies these rendering guidelines **SHOULD** ensure that the full original source of the message as it was received remains available to such a user for debugging and troubleshooting.

If a troubleshooting scenario demands information about the cryptographically protected values of Header Fields, and the message is encrypted, the debugging interface **SHOULD** also provide a "source" view of the Cryptographic Payload itself, alongside the full original source of the message as received.

4.10. Handling RFC8551HP Messages (Backward Compatibility)

Section 1.1.1 describes some drawbacks to the Header Protection scheme defined in [RFC8551], referred to here as RFC8551HP. An MUA **MUST NOT** generate an RFC8551HP message. However, for backward compatibility, an MUA **MAY** try to render or respond to such a message as though the message has standard Header Protection.

The following two sections contain guidance for identifying, rendering, and replying to RFC8551HP messages. Corresponding test vectors are provided in Appendices C.2.5, C.2.6, and C.3.17.

4.10.1. Identifying an RFC8551HP Message

An RFC8551HP message can be identified by its MIME structure, given that all of the following conditions are met:

- It has a well-formed Cryptographic Envelope consisting of at least one Cryptographic Layer as the outermost MIME object.
- The Cryptographic Payload is a single `message/rfc822` object.
- The message that constitutes the Cryptographic Payload does not itself have a well-formed Cryptographic Envelope; that is, its outermost MIME object is not a Cryptographic Layer.
- No `Content-Type` parameter of `hp=` is set on either the Cryptographic Payload or its immediate MIME child.

Here is the MIME structure of an example signed-and-encrypted RFC8551HP message:

```
A └─ application/pkcs7-mime; smime-type="enveloped-data"
  ↧ (decrypts to)
B   └─ application/pkcs7-mime; smime-type="signed-data"
  ⇩ (unwraps to)
C     └─ message/rfc822 [Cryptographic Payload]
D       └─ multipart/alternative [Rendered Body]
E         ├─ text/plain
F         └─ text/html
```

This meets the definition of an RFC8551HP message because:

- Cryptographic Layers `A` and `B` form the Cryptographic Envelope.
- The Cryptographic Payload, rooted in part `C`, has `Content-Type: message/rfc822`.
- Part `D` (the MIME root of the message at `C`) is itself not a Cryptographic Layer.
- Neither part `C` nor part `D` have any `hp` parameters set on their `Content-Type`.

4.10.2. Rendering or Responding to an RFC8551HP Message

When an MUA has precisely identified a message as an RFC8551HP message, the MUA **MAY** render or respond to that message as though it were a message with Header Protection as defined in this document by making the following adjustments:

- Rather than rendering the message Body as the Cryptographic Payload itself (part `C` in the example above), render the RFC8551HP message's Body as the MIME subtree that is the Cryptographic Payload's immediate child (part `D`).
- Make a comparable modification to HeaderSetsFromMessage (Section 4.2.1) and HeaderFieldProtection (Section 4.3.1): Both algorithms currently look for the protected Header Fields on the Cryptographic Payload (part `C`), but they should instead look at the Cryptographic Payload's immediate child (part `D`).

- If the Cryptographic Envelope is signed-only, behave as though there is an `hp="clear"` parameter for the Cryptographic Payload; if the Envelope contains encryption, behave as though there is an `hp="cipher"` parameter. That is, infer the sender's cryptographic intent from the structure of the message.
- If the Cryptographic Envelope contains encryption, further modify HeaderSetsFromMessage to derive `refouter` from the actual outer message Header Fields (those found in part `A` in the example above) rather than looking for `HP-Outer` Header Fields with the other protected Header Fields. That is, infer Header Field confidentiality based on the unprotected Header Fields.

The inferences in the above modifications are not based on any strong end-to-end guarantees. An intervening MTA may tamper with the message's Outer Header Section or wrap the message in an encryption layer to undetectably change the recipient's understanding of the confidentiality of the message's Header Fields or the message Body itself.

4.11. Rendering Other Schemes

Other MUAs may have generated different structures of messages that aim to offer end-to-end cryptographic protections that include Header Protection. This document is not normative for those schemes, and it is **NOT RECOMMENDED** to generate these other schemes, as they can either have structural flaws or simply render poorly on Legacy MUAs. A conformant MUA **MAY** attempt to infer Header Protection when rendering an existing message that appears to use some other scheme not documented here. Pointers to some known other schemes can be found in Appendix F.

5. Sending Guidance

This section describes the process an MUA should use to apply cryptographic protection to an email message with Header Protection.

When composing a message with end-to-end cryptographic protections, an MUA **SHOULD** apply Header Protection.

When generating such a message, an MUA **MUST** add the `hp` parameter (see Section 2.1.1) only to the `Content-Type` Header Field at the root of the message's Cryptographic Payload. The value of the parameter **MUST** indicate whether the Cryptographic Envelope contains a layer that provides encryption.

5.1. Composing a Cryptographically Protected Message Without Header Protection

For contrast, we first consider the typical message composition process of a Legacy Crypto MUA, which does not provide any Header Protection.

This process is described in Section 5.1 of [RFC9787]. We replicate it here for reference. The inputs to the algorithm are:

- `origbody`: The unprotected message Body as a well-formed MIME tree (possibly just a single MIME leaf part). As a well-formed MIME tree, `origbody` already has Structural Header Fields (`Content-*`) present.
- `origheaders`: The intended Non-Structural Header Fields for the message, represented here as a list of `(h,v)` pairs, where `h` is a Header Field name and `v` is the associated value. Note that these are Header Fields that the MUA intends to be visible to the recipient of the message. In particular, if the MUA uses the `Bcc` Header Field during composition but plans to omit it from the message (see Section 3.6.3 of [RFC5322]), it will not be in `origheaders`.
- `crypto`: The series of cryptographic protections to apply (for example, "sign with the secret key corresponding to X.509 certificate X, then encrypt to X.509 certificates X and Y"). This is a routine that accepts a MIME tree as input (the Cryptographic Payload), wraps the input in the appropriate Cryptographic Envelope, and returns the resultant MIME tree as output.

The algorithm returns a MIME object that is ready to be injected into the mail system.

5.1.1. ComposeNoHeaderProtection

Method signature:

```
ComposeNoHeaderProtection(origbody, origheaders, crypto) -> mime_message
```

Procedure:

1. Apply `crypto` to MIME part `origbody`, producing MIME tree `output`.
2. For each Header Field name and value `(h,v)` in `origheaders`:
   i. Add Header Field `h` to `output` with value `v`.
3. Return `output`.

5.2. Composing a Message with Header Protection

To compose a message using Header Protection, the composing MUA uses the following inputs:

- all the inputs described in Section 5.1
- `hcp`: an HCP, as defined in Section 3
- `respond`: if the new message is a response to another message (e.g., "Reply", "Reply All", "Forward", etc.), the MUA function corresponding to the user's action (see Section 6.1), otherwise `null`
- `refmsg`: if the new message is a response to another message, the message being responded to, otherwise `null`
- `legacy`: a boolean value, indicating whether any recipient of the message is believed to have a Legacy MUA. If all recipients are known to implement this document, `legacy` should be set to `false`. (How an MUA determines the value of `legacy` is out of scope for this document; an initial implementation can simply set it to `true`.)

To enable visibility of User-Facing but now removed/obscured Header Fields for decryption-capable Legacy MUAs, the Header Fields are included as a decorative Legacy Display Element in specially marked parts of the message (see Section 2.1.2). This document recommends two mechanisms for such a decorative adjustment: one for a `text/html` Main Body Part of the email message and one for a `text/plain` Main Body Part. This document does not recommend adding a Legacy Display Element to any other part.

Please see Section 7.1 of [RFC9787] for guidance on identifying the parts of a message that are a Main Body Part.

5.2.1. Compose

Method signature:

```
Compose(origbody, origheaders, crypto, hcp, respond, refmsg, legacy) ->
mime_message
```

Procedure:

1. Let `newbody` be a copy of `origbody`.
2. If `crypto` contains encryption and `legacy` is `true`:
   i. Create `ldlist`, an empty list of `(header, value)` pairs.
   ii. For each Header Field name and value `(h,v)` in `origheaders`:
      a. If `h` is User-Facing (see Section 1.1.2 of [RFC9787]):
         I. If `hcp(h,v)` is not `v`:
            A. Add `(h,v)` to `ldlist`.
   iii. If `ldlist` is not empty:
      a. Identify each leaf MIME part of `newbody` that represents a "Main Body Part" of the message.
      b. For each "Main Body Part" `bodypart` of type `text/plain` or `text/html`:
         I. Adjust `bodypart` by inserting a Legacy Display Element Header Field list `ldlist` into its content and adding a `Content-Type` parameter `hp-legacy-display` with value `1` (see Section 5.2.2 for `text/plain` and Section 5.2.3 for `text/html`).
3. For each Header Field name and value `(h,v)` in `origheaders`:
   i. Add Header Field `h` to MIME part `newbody` with value `v`.
4. If `crypto` does not contain encryption:
   i. Set the `hp` parameter on the `Content-Type` of MIME part `newbody` to `clear`.
   ii. Let `newheaders` be a copy of `origheaders`.
5. Else (if `crypto` contains encryption):
   i. Set the `hp` parameter on the `Content-Type` of MIME part `newbody` to `cipher`.

ii. If `refmsg` is not `null`, `respond` is not `null`, and `refmsg` itself is encrypted with Header Protection:

a. Let `response_hcp` be a single-use HCP derived from `respond` and `refmsg` (see Section 6.1).

iii. Else (if this is not a response to an encrypted, header-protected message):

a. Set `response_hcp` to `hcp_no_confidentiality`.

iv. Create a new empty list of Header Field names and values `newheaders`.

v. For each Header Field name and value `(h, v)` in `origheaders`:

a. Let `newval` be `hcp(h, v)`.

b. If `newval` is `v`:

I. Let `newval` be `response_hcp(h, v)`.

c. If `newval` is not `null`:

I. Add `(h, newval)` to `newheaders`.

vi. For each Header Field name and value `(h, v)` in `newheaders`:

a. Let string `record` be the concatenation of `h`, a literal `": "` (ASCII colon (0x3A) followed by ASCII space (0x20)), and `v`.

b. Add Header Field `"HP-Outer"` to MIME part `newbody` with value `record`.

6. Apply `crypto` to MIME part `newbody`, producing MIME tree `output`.

7. For each Header Field name and value `(h, v)` in `newheaders`:

i. Add Header Field `h` to `output` with value `v`.

8. Return `output`.

Note that both new parameters (`hcp` and `legacy`) are effectively ignored if `crypto` does not contain encryption. This is by design, because they are irrelevant for signed-only cryptographic protections.

5.2.2. Adding a Legacy Display Element to a text/plain Part

For a list of obscured and removed User-Facing Header Fields represented as `(header, value)` pairs, concatenate them as a set of lines, with one newline at the end of each pair. Add an additional trailing newline after the resultant text, and prepend the entire list to the content of the `text/plain` part.

The MUA **MUST** also add a `Content-Type` parameter of `hp-legacy-display` with value `1` to the MIME part to indicate that a Legacy Display Element was added.

For example, if the list of obscured Header Fields was `[("Cc", "alice@example.net"), ("Subject", "Thursday's meeting")]`, then a `text/plain` Main Body Part that originally looked like this:

```
Content-Type: text/plain; charset=UTF-8

I think we should skip the meeting.
```

would become:

```
Content-Type: text/plain; charset=UTF-8; hp-legacy-display=1

Subject: Thursday's meeting
Cc: alice@example.net

I think we should skip the meeting.
```

Note that the Legacy Display Element (the lines beginning with `Subject:` and `Cc:`) is part of the content of the MIME part in question.

This example assumes that the Main Body Part in question is not the root of the Cryptographic Payload. For instance, it could be a leaf of a `multipart/alternative` Cryptographic Payload. This is why no additional Header Fields have been injected into the MIME part in this example.

5.2.3. Adding a Legacy Display Element to a text/html Part

Adding a Legacy Display Element to a `text/html` part is similar to how it is added to a `text/plain` part (see Section 5.2.2). Instead of adding the obscured or removed User-Facing Header Fields to a block of text delimited by a blank line, the composing MUA injects them in an HTML `<div>` element annotated with a `class` attribute of `header-protection-legacy-display`.

The content and formatting of this decorative `<div>` have no strict requirements, but they **MUST** represent all the obscured and removed User-Facing Header Fields in a readable fashion. A simple approach is to assemble the text in the same way as Section 5.2.2, wrap it in a verbatim `<pre>` element, and put that element in the annotated `<div>`.

The annotated `<div>` should be placed as close to the start of the `<body>` as possible, where it will be visible when viewed with a standard HTML renderer.

The MUA **MUST** also add a `Content-Type` parameter of `hp-legacy-display` with value `1` to the MIME part to indicate that a Legacy Display Element was added.

For example, if the list of obscured Header Fields was `[("Cc", "alice@example.net"), ("Subject", "Thursday's meeting")]`, then a `text/html` Main Body Part that originally looked like this:

```
Content-Type: text/html; charset=UTF-8

<html><head><title></title></head><body>
<p>I think we should skip the meeting.</p>
</body></html>
```

would become:

```
Content-Type: text/html; charset=UTF-8; hp-legacy-display=1

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>Subject: Thursday's meeting
Cc: alice@example.net</pre></div>
<p>I think we should skip the meeting.</p>
</body></html>
```

This example assumes that the Main Body Part in question is not the root of the Cryptographic Payload. For instance, it could be a leaf of a `multipart/alternative` Cryptographic Payload. This is why no additional Header Fields have been injected into the MIME part in this example.

5.2.3.1. Step-by-Step Example for Inserting a Legacy Display Element into text/html

A composing MUA **MAY** insert the Legacy Display Element anywhere reasonable within the message as long as it prioritizes visibility for the reader using a Legacy MUA that is capable of decryption. This decision may take into account special message-specific HTML formatting expectations if the MUA is aware of them. However, some MUAs may not have any special insight into the user's preferred HTML formatting and still want to insert a Legacy Display Element. This section offers a non-normative, simple, and minimal step-by-step approach for a composing MUA that has no other information or preferences to fall back on.

The process below assumes that the MUA already has the full HTML object that it intends to send, including all of the text supplied by the user.

1. Assemble the text exactly as specified for `text/plain` (see Section 5.2.2).
2. Wrap that text in a verbatim `<pre>` element.
3. Wrap that `<pre>` element in a `<div>` element annotated with the class `header-protection-legacy-display`.
4. Find the `<body>` element of the full HTML object.
5. Insert the `<div>` element as the first child of the `<body>` element.

5.2.4. Only Add a Legacy Display Element to Main Body Parts

Some messages may contain a `text/plain` or `text/html` subpart that is *not* a Main Body Part. For example, an email message might contain an attached text file or a downloaded web page. Attached documents need to be preserved as intended in the transmission, without modification.

The composing MUA **MUST NOT** add a Legacy Display Element to any part of the message that is not a Main Body Part. In particular, if a part is annotated with `Content-Disposition: attachment`, or if it does not descend via the first child of any of its `multipart/mixed` or `multipart/related` ancestors, it is not a Main Body Part and **MUST NOT** be modified.

See Section 7.1 of [RFC9787] for more guidance about common ways to distinguish Main Body Parts from other MIME parts in a message.

5.2.5. Do Not Add a Legacy Display Element to Other Content-Types

The purpose of injecting a Legacy Display Element into each Main Body Part is to enable rendering of otherwise obscured Header Fields in Legacy MUAs that are capable of message decryption but don't know how to follow the rest of the guidance in this document.

The authors are unaware of any Legacy MUA that would render any MIME part type other than `text/plain` and `text/html` as the Main Body. A generating MUA **SHOULD NOT** add a Legacy Display Element to any MIME part with any other `Content-Type`.

6. Replying and Forwarding Guidance

An MUA might create a new message in response to another message, thus acting both as a receiving MUA and as a sending MUA. For example, the user of an MUA viewing any given message might take an action like "Reply", "Reply All", "Forward", or some comparable action to start the composition of a new message. The new message created this way effectively references the original message that was viewed at the time.

For encrypted messages, special guidance applies, because information can leak in at least two ways: leaking previously confidential Header Fields and leaking the entire message by sending the reply or forward to the wrong party.

6.1. Avoid Leaking Encrypted Header Fields in Replies and Forwards

As noted in Section 5.4 of [RFC9787], an MUA in this position **MUST NOT** leak previously encrypted content in the clear in a follow-up message. The same is true for protected Header Fields.

Values from any Header Field that was identified as either `encrypted-only` or `signed-and-encrypted` based on the steps outlined above **MUST NOT** be placed in cleartext output when generating a message.

In particular, if `Subject` was encrypted, and it is copied into the draft encrypted reply, the replying MUA **MUST** obscure the unprotected (cleartext) `Subject` Header Field.

When crafting the Header Fields for a reply or forwarded message, the composing MUA **SHOULD** make use of the `HP-Outer` Header Fields from within the Cryptographic Envelope of the reference message to ensure that Header Fields derived from the reference message do not leak in the reply.

On a high level, this can be achieved as follows: Consider a Header Field in a reply message that is generated by derivation from a Header Field in the reference message. For example, the `To` Header Field is typically derived from the reference message's `Reply-To` or `From` Header Fields. When generating the outer copy of the Header Field, the composing MUA first applies its own HCP. If the Header Field's value is changed by the HCP, then it is applied to the Outer Header Section. If the Header Field's value is unchanged, the composing MUA re-generates the Header Field using the Header Fields that had been on the outside of the original message at sending

time. These can be inferred from the `HP-Outer` Header Fields located within the Cryptographic Payload of the referenced message. If that value is itself different than the protected value, then it is applied to the Outer Header Section. If the value is the same as the protected value, then it is simply copied to the Outer Header Section directly. Whether it was changed or not, it is noted in the protected Header Section using `HP-Outer`, as described in Section 2.2.1.

See Appendix D.2 for a simple worked example of this process.

Below we describe a supporting algorithm to handle this. It produces a list of Header Fields that should be obscured or removed in the new message even if the sender's choice of HCP wouldn't normally remove or obscure the Header Field in question. This is effectively a single-use HCP. The normal sending guidance in Section 5.2 applies this single-use HCP to implement the high-level guidance above.

6.1.1. ReferenceHCP

The algorithm takes two inputs:

- A single referenced message `refmsg`
- A built-in MUA `respond` function associated with the user's action. The `respond` function takes a list of Header Fields from a referenced message as input and generates a list of initial candidate message Header Field names and values that are used to populate the message composition interface. Something like this function already exists in most MUAs, though it may differ across responsive actions. For example, the `respond` function that implements "Reply All" is likely to be a different from the `respond` function that implements "Reply".

As an output, it produces an ephemeral single-use HCP, specific to this kind of response to this specific message.

Method signature:

```
ReferenceHCP(refmsg, respond) -> ephemeral_hcp
```

Procedure:

1. If `refmsg` is not encrypted with Header Protection:
   i. Return `hcp_no_confidentiality` (there is no header confidentiality in the reference message that needs protection).
2. Extract `refouter`, `refprotected` from `refmsg` as described in Section 4.2.
3. Let `genprotected` be a list of `(h,v)` pairs generated by `respond(refprotected)`.
4. Let `genouter` be a list of `(h,v)` pairs generated by `respond(refouter)`.
5. For each `(h,v)` in `genprotected`:
   i. If `(h,v)` is in `genouter`:
      a. Remove `(h,v)` from both `genprotected` and `genouter` (this Header Field does not need additional confidentiality).

6. Let `confmap` be a mapping from a Header Field name and value `(h,v)` to either a string or the special value `null` (this mapping is initially empty).
7. For each `(h,v)` remaining in `genprotected`:
   i. Set `result` to the special value `null`.
   ii. For each `(h1,v1)` in `genouter`:
      a. If `h1` is `h`:
         I. Set `result` to `v1`.
   iii. Insert `(h,v) -> result` into `confmap`.
8. Return a new HCP from `confmap` that tests whether the `(name,val_in)` tuple is in `confmap`; if so, return `confmap[(name,val_in)]`; otherwise, return `val_in`.

Note that the key idea here is to reuse the MUA's existing `respond` function. The algorithm simulates how the MUA would pre-populate a reply to two messages whose Header Fields have the values `refouter` and `refprotected`, respectively (independent of any cryptographic protections). Then, it uses the difference to derive a one-time HCP. This HCP takes into account both the referenced message's sender's preferences and the derivations that can happen to Header Field values when responding. Note that while some of these derivations are straightforward (e.g., `In-Reply-To` is usually derived from `Message-ID`), others are non-trivial. For example, the `From` address may be derived from `To`, `Cc`, or the MUA's local address preference (especially when the MUA received the referenced message via `Bcc`). Similarly, `To` may be derived from `To`, `From`, and/or `Cc` Header Fields depending on the MUA implementation and depending on whether the user clicked "Reply", "Reply All", "Forward", or any other action that generates a response to a message. Reusing the MUA's existing `respond` function incorporates these nuances without requiring any extra configuration choices or additional maintenance burden.

6.2. Avoid Misdirected Replies

When replying to a message, the composing MUA typically decides who to send the reply to based on:

- the `Reply-To`, `Mail-Followup-To`, or `From` Header Fields
- optionally, the other `To` or `Cc` Header Fields (if the user chose to "Reply All")

When a message has Header Protection, the replying MUA **MUST** populate the destination fields of the draft message using the protected Header Fields and ignore any unprotected Header Fields.

This mitigates against an attack where Mallory gets a copy of an encrypted message from Alice to Bob and then replays the message to Bob with an additional `Cc` to Mallory's own email address in the message's outer (unprotected) Header Section.

If Bob knows Mallory's certificate already, and he replies to such a message without following the guidance in this section, it's likely that his MUA will encrypt the cleartext of the message directly to Mallory.

7. Unprotected Header Fields Added in Transit

Some Header Fields are legitimately added in transit and could not have been known to the sender at message composition time.

The most common of these Header Fields are `Received` and `DKIM-Signature`, neither of which are typically rendered, either explicitly or implicitly.

If a receiving MUA has specific knowledge about a given Header Field, including that:

- the Header Field would not have been known to the original sender and
- the Header Field might be rendered explicitly or implicitly,

then the MUA **MAY** decide to operate on the value of that Header Field from the Outer Header Section, even though the message has Header Protection.

The MUA **MAY** prefer to verify that the Header Fields in question have additional transit-derived cryptographic protections before rendering or acting on them. For example, the MUA could verify whether these Header Fields are covered by an appropriate and valid `ARC-Authentication-Results` (see [RFC8617]) or `DKIM-Signature` (see [RFC6376]) Header Field.

Specific examples of Header Fields that are meaningful to the user and are commonly added by MTAs appear below.

7.1. Mailing List Header Fields: List-* and Archived-At

If the message arrives through a mailing list, the list manager itself may inject Header Fields (most have a `List-` prefix) in the message:

- `List-Archive`
- `List-Subscribe`
- `List-Unsubscribe`
- `List-Id`
- `List-Help`
- `List-Post`
- `Archived-At`

For some MUAs, these Header Fields are implicitly rendered by providing buttons for actions like "Subscribe", "View Archived Version", "Reply List", "List Info", etc.

An MUA that receives a message with Header Protection that contains these Header Fields in the Outer Header Section and that has reason to believe the message is coming through a mailing list **MAY** decide to render them to the user (explicitly or implicitly) even though they are not protected.

8. Email Ecosystem Evolution

The email ecosystem is the set of client-side and server-side software and policies that are used in the creation, transmission, storage, rendering, and indexing of email over the Internet.

This document is intended to offer tooling needed to improve the state of the email ecosystem in a way that can be deployed without significant disruption. Some elements of this specification are present for transitional purposes but would not exist if the system were designed from scratch.

This section describes these transitional mechanisms, as well as some suggestions for how they might eventually be phased out.

8.1. Dropping Legacy Display Elements

Any decorative Legacy Display Element added to an encrypted message that uses Header Protection is present strictly for enabling Header Field visibility (most importantly, the Subject Header Field) when the message is viewed with a decryption-capable Legacy MUA.

Eventually, the hope is that most decryption-capable MUAs will conform to this specification and there will be no need for injection of Legacy Display Elements in the message Body. A survey of widely used decryption-capable MUAs might be able to establish when most of them do support this specification.

At that point, a composing MUA could set the `legacy` parameter defined in Section 5.2 to `false` by default or could even hard-code it to `false`, yielding a much simpler message construction set.

Until that point, an end user might want to signal that their receiving MUAs are conformant to this document so that a peer composing a message to them can set `legacy` to `false`. A signal indicating capability of handling messages with Header Protection might be placed in the user's cryptographic certificate or in outbound messages.

This document does not attempt to define the syntax or semantics of such a signal.

8.2. More Ambitious Default HCP

This document defines a few different forms of HCP. An MUA implementing an HCP for the first time **SHOULD** deploy `hcp_baseline` as recommended in Section 3.3. This HCP offers the most commonly expected protection (obscuring the Subject Header Field) without risking deliverability or rendering issues.

The HCPs proposed in this document are relatively conservative and still leak a significant amount of metadata for encrypted messages. This is largely done to ensure deliverability (see Section 1.3.2) and usability, as messages without some critical Header Fields are more likely to not reach their intended recipient.

In the future, some mail transport systems may accept and deliver messages with even less publicly visible metadata. Many MTA operators today would ask for additional guarantees about such a message to limit the risks associated with abusive or spam mail.

This specification offers the HCP formalism itself as a way for MUA developers and MTA operators to describe their expectations around message deliverability. MUA developers can propose a more ambitious default HCP and ask MTA operators (or simply test) whether their MTAs would be likely to deliver or reject encrypted mail with that HCP applied. Proponents of a more ambitious HCP should explicitly document the HCP and name it clearly and unambiguously to facilitate this kind of interoperability discussion.

Reaching widespread consensus around a more ambitious global default HCP is a challenging problem of coordinating many different actors. A piecemeal approach might be more feasible, where some signaling mechanism allows a message recipient, MTA operator, or third-party clearinghouse to announce what kinds of HCPs are likely to be deliverable for a given recipient. In such a situation, the default HCP for an MUA might involve consulting the signaled acceptable HCPs for all recipients and combining them (along with a default for when no signal is present) in some way.

If such a signal were to reach widespread use, it could also be used to guide reasonable statistical default HCP choices for recipients with no signal.

This document does not attempt to define the syntax or semantics of such a signal.

8.3. Deprecation of Messages Without Header Protection

At some point, when the majority of MUA clients that can generate cryptographically protected messages can do so with Header Protection, it should be possible to deprecate any cryptographically protected message that does not have Header Protection.

For example, as noted in Section 9.1, it's possible for an MUA to render a `signed-only` message that has no Header Protection the same as an `unprotected` message. And a `signed-and-encrypted` message without Header Protection could likewise be marked as not fully protected.

These stricter rules could be adopted immediately for all messages. Or an MUA developer could roll them out immediately for any new message but still treat an old message (based on the Date Header Field and cryptographic signature timestamp) more leniently.

A decision like this by any popular receiving MUA could drive adoption of this standard for sending MUAs.

9. Usability Considerations

This section describes concerns for MUAs that are interested in easy adoption of Header Protection by normal users.

While they are not protocol-level artifacts, these concerns motivate the protocol features described in this document.

See also the usability commentary in Section 2 of [RFC9787].

9.1. Mixed Protections Within a Message Are Hard to Understand

When rendering a message to the user, the ideal circumstance is to present a single cryptographic status for any given message. However, when message Header Fields are present, some message Header Fields do not have the same cryptographic protections as the main message.

Representing such a mixed set of protection statuses is very difficult to do in a way that an Ordinary User can understand. There are at least three scenarios that are likely to be common and poorly understood:

- A signed message with no Header Protection.
- A signed-and-encrypted message with no Header Protection.
- A signed-and-encrypted message with Header Protection as defined in this document, where some User-Facing Header Fields have confidentiality but some do not.

An MUA should have a reasonable strategy for clearly communicating each of these scenarios to the user. For example, an MUA operating in an environment where it expects most cryptographically protected messages to have Header Protection could use the following rendering strategy:

- When rendering a message with a `signed-only` cryptographic status but no Header Protection, an MUA may decline to indicate a positive security status overall and only indicate the cryptographic status to a user in a message properties or diagnostic view. That is, the message may appear identical to an unsigned message except if a user verifies the properties through a menu option.
- When rendering a message with a `signed-and-encrypted` or `encrypted-only` cryptographic status but no Header Protection, overlay a warning flag on the typical cryptographic status indicator. That is, if a typical `signed-and-encrypted` message displays a lock icon, display a lock icon with a warning sign (e.g., an exclamation point in a triangle) overlaid. For example, see the graphics in [chrome-indicators].
- When rendering a message with a `signed-and-encrypted` or `encrypted-only` cryptographic status with Header Protection but where the Subject Header Field has not been removed or obscured, place a warning sign on the Subject line.

Other simple rendering strategies could also be reasonable.

9.2. Users Should Not Have to Choose a Header Confidentiality Policy

This document defines the abstraction of an HCP object for the sake of communication between implementers and deployments.

Most email users are unlikely to understand the trade-offs between different policies. In particular, the potential negative side effects (e.g., poor deliverability) may not be easily attributable by a normal user to a particular HCP.

Therefore, MUA implementers should be conservative in their choice of default HCP and should not require the Ordinary User to make an incomprehensible choice that could cause unfixable, undiagnosable problems. The safest option is for the MUA developer to select a known, stable HCP (this document recommends `hcp_baseline` in Section 3.3) on the user's behalf. An MUA should not expose the Ordinary User to a configuration option where they are expected to manually select (let alone define) an HCP.

10. Security Considerations

Header Protection improves the security of cryptographically protected email messages. Following the guidance in this document improves security for users by more directly aligning the underlying messages with user expectations about confidentiality, authenticity, and integrity.

Nevertheless, helping the user distinguish between cryptographic protections of various messages remains a security challenge for MUAs. This is exacerbated by the fact that many existing messages with cryptographic protections do not employ Header Protection. MUAs encountering these messages (e.g., in an archive) will need to handle older forms (without Header Protection) for quite some time, possibly forever.

The security considerations from Section 6 of [RFC8551] continue to apply for any MUA that offers S/MIME cryptographic protections, as well as Section 3 of [RFC5083] (Authenticated-Enveloped-Data in Cryptographic Message Syntax (CMS)) and Section 14 of [RFC5652] (CMS more broadly). Likewise, the security considerations from Section 8 of [RFC3156] continue to apply for any MUA that offers PGP/MIME cryptographic protections, as well as Section 13 of [RFC9580] (OpenPGP itself). In addition, these underlying security considerations are now also applicable to the contents of the message Header Section, not just the message Body.

10.1. From Address Spoofing

If the `From` Header Field were treated like any other protected Header Field by the receiving MUA, this scheme would enable sender address spoofing.

To prevent sender spoofing, many receiving MUAs implicitly rely on their receiving MTA to inspect the Outer Header Section and verify that the `From` Header Field is authentic. If a receiving MUA displays a `From` address that doesn't match the `From` address that the receiving and/or sending MTAs filtered on, the MUA may be vulnerable to spoofing.

Consider a malicious MUA that sets the following Header Fields on an encrypted message with Header Protection:

- Outer: `From: <alice@example.com>`
- Inner: `HP-Outer: From: <alice@example.com>`
- Inner: `From: <bob@example.org>`

During sending, the MTA of `example.com` validates that the sending MUA is authorized to send from `alice@example.com`. Since the message is encrypted, the sending and receiving MTAs cannot see the protected Header Fields. A naive receiving MUA might follow the algorithms in this document without special consideration for the `From` Header Field. Such an MUA might display the email as coming from `bob@example.org` to the user, resulting in a spoofed address.

This problem applies both between domains and within a domain.

This problem always applies to signed-and-encrypted messages. This problem also applies to signed-only messages because MTAs typically do not look at the protected Header Fields when confirming `From` address authenticity.

Sender address spoofing is relevant for two distinct security properties:

- Sender authenticity: relevant for rendering the message (which address to show the user?)
- Message confidentiality: relevant when replying to a message (a reply to the wrong address can leak the message contents)

10.1.1. From Rendering Reasoning

Section 4.4.3 provides guidance for rendering the `From` Header Field. It recommends a receiving MUA that depends on its MTA to authenticate the unprotected (outer) `From` Header Field to render the outer `From` Header Field if both of the following conditions are met:

- `From` Header Field Mismatch (as defined in Section 4.4.1.1) and
- No Valid and Correctly Bound Signature (as defined in Section 4.4.1.2)

Note: The second condition effectively means that the inner (expected to be protected) `From` Header Field appears to have insufficient protection.

This may seem surprising since it causes the MUA to render a mix of both protected and unprotected values. This section provides an argument as to why this guidance makes sense.

We proceed by case distinction:

- Case 1: Malicious sending MUA.
  - Attack situation: The sending MUA puts a different inner `From` Header Field to spoof the sender address.
  - In this case, it is "better" to fall back and render the outer `From` Header Field because this is what the receiving MTA can validate. Otherwise, this document would introduce a new way for senders to spoof the `From` address of the message.

- This does not preclude a future document from updating this document to specify a protocol for legitimate sender address hiding.

- Case 2: Malicious sending/transiting/receiving MTA (or anyone meddling between MTAs).
  - Attack situation: An on-path attacker changes the outer `From` Header Field (possibly with other meddling to break the signature; see below). Their goal is to get the receiving MUA to show a different `From` address than the sending MUA intended (breaking MUA-to-MUA sender authenticity).
  - Case 2.a: The sending MUA submitted an unsigned or encrypted-only message to the email system. In this case, there can be no sender authenticity anyway.
  - Case 2.b: The sending MUA submitted a signed-only message to the email system.
    - Case 2.b.i: The attacker removes or breaks the signature. In this case, the attacker can also modify the inner `From` Header Field to their liking.
    - Case 2.b.ii: The signature is valid, but the receiving MUA does not see any valid binding between the signing certificate and the `addr-spec` of the inner `From` Header Field. In this case, there can be no sender authenticity anyways (the certificate could have been generated by the on-path attacker). This case is indistinguishable from a malicious sending MUA; hence, it is "better" to fall back to the outer `From` Header Field that the MTA can validate. Note that once the binding is validated (e.g., after an out-of-band comparison), the rendering may change from showing the outer `From` address (and a warning) to showing the inner, now validated `From` address. In some cases, the binding may be instantly validated even for previously unseen certificates (e.g., if the certificate is issued by a trusted certification authority).
  - Case 2.c: The sending MUA submitted a signed-and-encrypted message to the email system.
    - Case 2.c.i: The attacker removes or breaks the signature. Note that the signature is inside the ciphertext (see Section 5.2 of [RFC9787]). Thus, assuming the encryption is non-malleable, any on-path attacker cannot break the signature while ensuring that the message still decrypts successfully.
    - Case 2.c.ii: The signature is valid, but the receiving MUA does not see any valid binding between the signing certificate and the `addr-spec` of the inner `From` Header Field. See case 2.b.ii.

As the case distinction shows, the outer `From` Header Field is either the preferred fallback (in particular, to avoid introducing a new spoofing channel) or just as good (because just as modifiable) as the inner `From` Header Field.

Rendering the outer `From` Header Field does carry the risk of a "temporary downgrade attack" in cases 2.b.ii and 2.c.ii, where a malicious MTA keeps the signature intact but modifies the outer `From` Header Field. The MUA can resolve this temporary downgrade by validating the certificate-to-`addr-spec` binding. If the MUA never does this validation, the entire message could be fake.

If there were a signaling channel where the MTA can tell the MUA whether it authenticated the `From` Header Field, an MUA could use this in its rendering decision. In the absence of such a signal, and when end-to-end authenticity is unavailable, this document prefers to fall back to the

outer `From` Header Field. This default is based on the assumption that most MTAs apply some filtering based on the outer `From` Header Field (whether the MTA can authenticate it or not). Rendering the unprotected outer `From` Header Field (instead of the protected inner one) in case of a mismatch retains this ability for MTAs.

If the MUA decides not to rely on the MTA to authenticate the outer `From` Header Field, it may prefer the inner `From` Header Field.

10.2. Avoid Cryptographic Summary Confusion from the hp Parameter

When parsing a message, the recipient MUA infers the message's Cryptographic Status from the Cryptographic Layers, as described in Section 4.6 of [RFC9787].

The Cryptographic Layers that make up the Cryptographic Envelope describe an ordered list of cryptographic properties as present in the message after it has been delivered. By contrast, the `hp` parameter to the `Content-Type` Header Field contains a simpler indication: whether the sender originally tried to encrypt the message or not. In particular, for a message with Header Protection, the Cryptographic Payload should have a `hp` parameter of `cipher` if the message is encrypted (in addition to signed) and `clear` if no encryption is present (that is, the message is `signed-only`).

As noted in Section 2.1.1, the receiving implementation should not inflate its estimation of the confidentiality of the message or its Header Fields based on the sender's intent if it can see that the message was not actually encrypted. A signed-only message that happens to have an `hp` parameter of `cipher` is still signed-only.

Conversely, since the encrypting Cryptographic Layer is typically outside the signature layer (see Section 5.2 of [RFC9787]), an originally signed-only message could have been wrapped in an encryption layer by an intervening party before receipt to appear encrypted.

If a message appears to be wrapped in an encryption layer, and the `hp` parameter is present but is not set to `cipher`, then it is likely that the encryption layer was not added by the original sender. For such a message, the lack of any `HP-Outer` Header Field in the Header Section of the Cryptographic Payload **MUST NOT** be used to infer that all Header Fields were removed from the message by the original sender. In such a case, the receiving MUA **SHOULD** treat every Header Field as though it was not confidential.

10.3. Caution About Composing with Legacy Display Elements

When composing a message, it's possible for a Legacy Display Element to contain risky data that could trigger errors in a rendering client.

For example, if the value for a Header Field to be included in a Legacy Display Element within a given Body part contains folding whitespace, it should be "unfolded" before generating the Legacy Display Element: All contiguous folding whitespace should be replaced with a single space character. Likewise, if the Header Field value was originally encoded per [RFC2047], it should be decoded first to a standard string and re-encoded using the charset appropriate to the target part.

When including a Legacy Display Element in a `text/plain` part (see Section 5.2.2), if the decoded Subject Header Field contains a pair of newlines (e.g., if it is broken across multiple lines by encoded newlines), any newline **MUST** be stripped from the Legacy Display Element. If the pair of newlines is not stripped, a receiving MUA that follows the guidance in Section 4.5.3.2 might leave the later part of the Legacy Display Element in the rendered message.

When including a Legacy Display Element in a `text/html` part (see Section 5.2.3), any material in the Header Field values should be explicitly HTML escaped to avoid being rendered as part of the HTML. At a minimum, the characters `<`, `>`, and `&` should be escaped to `<`, `>`, and `&`, respectively (for example, see [HTML-ESCAPES]). If unescaped characters from removed or obscured Header Field values end up in the Legacy Display Element, a receiving MUA that follows the guidance in Section 4.5.3.3 might fail to identify the boundaries of the Legacy Display Element, cutting out more than it should or leaving remnants visible. And a Legacy MUA parsing such a message might misrender the entire HTML stream, depending on the content of the removed or obscured Header Field values.

The Legacy Display Element is a decorative addition solely to enable visibility of obscured or removed Header Fields in decryption-capable Legacy MUAs. When it is produced, it should be generated minimally and strictly, as described above, to avoid damaging the rest of the message.

10.4. Plaintext Attacks

An encrypted email message using S/MIME or PGP/MIME tends to have some amount of predictable plaintext. For example, the standard MIME Header Fields of the Cryptographic Payload of a message are often a predictable sequence of bytes, even without Header Protection, when they only include the Structural Header Fields `MIME-Version` and `Content-Type`. This is a potential risk for known-plaintext attacks.

Including protected Header Fields as defined in this document increases the amount of known plaintext. Since some of those Header Fields in a reply will be derived from the message being replied to, this also creates a potential risk for chosen-plaintext attacks, in addition to known-plaintext attacks.

Modern message encryption mechanisms are expected to be secure against both known-plaintext attacks and chosen-plaintext attacks. An MUA composing an encrypted message should ensure that it is using such a mechanism, regardless of whether it does Header Protection.

11. Privacy Considerations

11.1. Leaks When Replying

The encrypted Header Fields of a message may accidentally leak when replying to the message. See the guidance in Section 6.

11.2. Encrypted Header Fields Are Not Always Private

For encrypted messages, depending on the sender's HCP, some Header Fields may appear both within the Cryptographic Envelope and on the outside of the message (e.g., `Date` might exist identically in both places). Section 4.3 identifies such a Header Field as `signed-only`. These Header Fields are clearly *not* private at all, despite a copy being inside the Cryptographic Envelope.

A Header Field whose name and value are not matched verbatim by any `HP-Outer` Header Field from the same part will have an `encrypted-only` or `signed-and-encrypted` status. But even Header Fields with these stronger levels of cryptographic confidentiality protection might not be as private as the user would like.

See the examples below.

This concern is true for any encrypted data, including the Body of the message, not just the Header Fields: If the sender isn't careful, the message contents or session keys can leak in many ways that are beyond the scope of this document. The message recipient has no way in principle to tell whether the apparent confidentiality of any given piece of encrypted content has been broken via channels that they cannot perceive. Additionally, an active intermediary aware of the recipient's public key can always encrypt a cleartext message in transit to give the recipient a false sense of security.

11.2.1. Encrypted Header Fields Can Leak Unwanted Information to the Recipient

For encrypted messages, even with an ambitious HCP that successfully obscures most Header Fields from all transport agents, Header Fields will be ultimately visible to all intended recipients. This can be especially problematic for Header Fields that are not User-Facing; the sender may not expect such Header Fields to be injected by their MUA. Consider the three following examples:

- The MUA may inject a `User-Agent` Header Field that describes itself to every recipient, even though the sender may not want the recipient to know the exact version of their OS, hardware platform, or MUA.
- The MUA may have an idiosyncratic way of generating a `Message-ID` Header Field, which could embed the choice of MUA, time zone, hostname, or other subtle information to a knowledgeable recipient.
- The MUA may erroneously include a `Bcc` Header Field in the `origheaders` of a copy of a message sent to the named recipient, defeating the purpose of using `Bcc` instead of `Cc` (see Section 11.4 for more details about risks related to `Bcc`).

Clearly, no end-to-end cryptographic protection of any Header Field as defined in this document will hide such a sensitive field from the intended recipient. Instead, the composing MUA **MUST** populate the `origheaders` list for any outbound message with only information the recipient should have access to. This is true for messages without any cryptographic protection as well, of course, and it is even worse there: Such a leak is exposed to the transport agents as well as the

recipient. An encrypted message with Header Protection and a more ambitious HCP avoids these leaks that expose information to the transport agents, but it cannot defend against such a leak to the recipient.

11.2.2. Encrypted Header Fields Can Be Inferred from External or Internal Metadata

For example, if the `To` and `Cc` Header Fields are removed from the Outer Header Section, the values in those fields might still be inferred with high probability by an adversary who looks at the message either in transit or at rest. For example, if the message is found in a mailbox, or being delivered to a mailbox, and the mailbox is known to be associated with the email address `bob@example.org`, it's likely that Bob was in either `To` or `Cc`. Furthermore, encrypted message ciphertext may hint at the recipients: For S/MIME messages, the `RecipientInfo`, and for PGP/MIME messages, the key ID in the Public Key Encrypted Session Key (PKESK) packets will all hint at a specific set of recipients. Additionally, an MTA that handles the message may add a `Received` Header Field (or some other custom Header Field) that leaks some information about the nature of the delivery.

11.2.3. Encrypted Header Fields May Not Be Fully Masked by HCP

In another example, if the HCP modifies the `Date` Header Field to mask out high-resolution timestamps (e.g., rounding to the most recent hour), some information about the date of delivery will still be attached to the email. At the very least, the low-resolution, global version of the date will be present on the message. Additionally, Header Fields like `Received` that are added during message delivery might include higher-resolution timestamps. And if the message lands in a mailbox that is ordered by time of receipt, even its placement in the mailbox and the unobscured `Date` Header Fields of the surrounding messages could leak this information.

Some Header Fields like `From` may be impossible to fully obscure, as many modern message delivery systems depend on at least domain information in the `From` Header Field for determining whether a message is coming from a domain with "good reputation" (that is, from a domain that is not known for leaking spam). So even if an ambitious HCP opts to remove the human-readable part from any `From` Header Field and to standardize/genericize the local part of the `From` address, the domain will still leak.

11.3. A Naive Recipient May Overestimate the Cryptographic Status of a Header Field in an Encrypted Message

When an encrypted (or signed-and-encrypted) message is in transit, an active intermediary can strip or tamper with any Header Field that appears outside the Cryptographic Envelope. A receiving MUA that naively infers cryptographic status from differences between the external Header Fields and those found in the Cryptographic Envelope could be tricked into overestimating the protections afforded to some Header Fields.

For example, if the original sender's HCP passes through the `Cc` Header Field unchanged, a cleanly delivered message would indicate that the `Cc` Header Field has a cryptographic status of `signed`. But if an intermediary attacker simply removes the Header Field from the Outer Header Section before forwarding the message, then the naive recipient might believe that the field has a cryptographic status of `signed-and-encrypted`.

This document offers protection against such an attack by way of the `HP-Outer` Header Fields that can be found on the Cryptographic Payload. If a Header Field appears to have been obscured by inspection of the outer message but an `HP-Outer` Header Field matches it exactly, then the receiving MUA can indicate to the user that the Header Field in question may not have been confidential.

In such a case, a cautious MUA may render the Header Field in question as `signed` (because the sender did not hide it) but still treat it as `signed-and-encrypted` during reply to avoid accidental leakage of the cleartext value in the reply message, as described in Section 6.1.

11.4. Privacy and Deliverability Risks with Bcc and Encrypted Messages

As noted in Section 9.3 of [RFC9787], handling `Bcc` when generating an encrypted email message can be particularly tricky. With Header Protection, there is an additional wrinkle. When an encrypted email message with Header Protection has a `Bcc`'ed recipient, and the composing MUA explicitly includes the `Bcc`'ed recipient's address in their copy of the message (see the "second method" in Section 3.6.3 of [RFC5322]), that `Bcc` Header Field will always be visible to the `Bcc`'ed recipient.

In this scenario, though, the composing MUA has one additional choice: whether or not to hide the `Bcc` Header Field from intervening message transport agents by returning `null` when the HCP is invoked for `Bcc`. If the composing MUA's rationale for including an explicit `Bcc` in the copy of the message sent to the `Bcc` recipient is to ensure deliverability via a message transport agent that inspects message Header Fields, then stripping the `Bcc` field during encryption may cause the intervening transport agent to drop the message entirely. This is why `Bcc` is not explicitly stripped in `hcp_baseline`.

On the other hand, if deliverability to a `Bcc`'ed recipient is not a concern, the most privacy-preserving option is to simply omit the `Bcc` Header Field from the protected Header Section in the first place. An MUA that is capable of receiving and processing such a message can infer that since their user's address was not mentioned in any `To` or `Cc` Header Field, they were likely a `Bcc` recipient.

Please also see Section 9.3 of [RFC9787] for more discussion about `Bcc` and encrypted messages.

12. IANA Considerations

This document registers an email Header Field, describes parameters for the `Content-Type` Header Field, and establishes a registry for Header Confidentiality Policies to facilitate HCP evolution.

12.1. Registration of the HP-Outer Header Field

IANA has registered the following Header Field in the "Permanent Message Header Field Names" registry within the "Message Headers" registry group <https://www.iana.org/assignments/message-headers> in accordance with [RFC3864].

Header Field Name	Protocol	Status	Reference
HP-Outer	mail	standard	Section 2.2.1 of RFC 9788

Table 2: Addition to the Permanent Message Header Field Names Registry

Note that the Template and Trace columns are empty and therefore not included in the table.

The Author/Change Controller (Section 4.5 of [RFC3864]) for this entry is the IETF.

12.2. Reference Update for the Content-Type Header Field

This document defines the Content-Type parameters known as hp (in Section 2.1.1) and hp-legacy-display (in Section 2.1.2). Consequently, IANA has added this document as a reference for Content-Type in the "Permanent Message Header Field Names" registry as shown below.

Header Field Name	Protocol	Reference
Content-Type	MIME	[RFC4021] and RFC 9788

Table 3: Permanent Message Header Field Names Registry

Note that the Template and Trace columns are empty and therefore not included in the table.

12.3. New Mail Header Confidentiality Policies Registry

IANA has created a new registry titled "Mail Header Confidentiality Policies" within the "MAIL Parameters" registry group <https://www.iana.org/assignments/mail-parameters/> with the following content:

Header Confidentiality Policy Name	Description	Recommended	Reference
hcp_no_confidentiality	No header confidentiality	N	Section 3.2.3 of RFC 9788
hcp_baseline	Confidentiality for Informational Header Fields: Subject Header Field is obscured, Keywords and Comments are removed	Y	Section 3.2.1 of RFC 9788
hcp_shy	Obscure Subject, remove Keywords and Comments, remove the time zone from Date, and obscure display-names	N	Section 3.2.2 of RFC 9788

Table 4: Mail Header Confidentiality Policies Registry

Note that `hcp_example_hide_cc` is offered as an example in Section 3 but is not formally registered by this document.

The following textual note has been added to this registry:

> Adding an entry to this registry with an `N` in the "Recommended" column follows the registration policy of Specification Required. Adding an entry to this registry with a `Y` in the "Recommended" column or changing the "Recommended" column in an existing entry (from `N` to `Y` or vice versa) requires IETF Review.

Note that during IETF Review, the designated expert must be consulted. Guidance for the designated expert can be found in Section 3.4.2.

Additionally, this textual note has been added to the registry:

> The Header Confidentiality Policy Name never appears on the wire. This registry merely tracks stable references to implementable descriptions of distinct policies. Any addition to this registry should be governed by guidance in Section 3.4.2 of RFC 9788.

13. References

13.1. Normative References

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <https://www.rfc-editor.org/info/rfc2045>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, DOI 10.17487/RFC3864, September 2004, <https://www.rfc-editor.org/info/rfc3864>.

[RFC5083] Housley, R., "Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type", RFC 5083, DOI 10.17487/RFC5083, November 2007, <https://www.rfc-editor.org/info/rfc5083>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8551] Schaad, J., Ramsdell, B., and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", RFC 8551, DOI 10.17487/RFC8551, April 2019, <https://www.rfc-editor.org/info/rfc8551>.

[RFC9580] Wouters, P., Ed., Huigens, D., Winter, J., and Y. Niibe, "OpenPGP", RFC 9580, DOI 10.17487/RFC9580, July 2024, <https://www.rfc-editor.org/info/rfc9580>.

[RFC9787] Gillmor, D. K., Ed., Hoeneisen, B., Ed., and A. Melnikov, Ed., "Guidance on End-to-End Email Security", RFC 9787, DOI 10.17487/RFC9787, June 2025, <https://www.rfc-editor.org/info/rfc9787>.

13.2. Informative References

[chrome-indicators] Schechter, E., "Evolving Chrome's security indicators", Chromium Blog, May 2018, <https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html>.

[CSS] Bos, B., Ed., "Cascading Style Sheets Level 2 Revision 2 (CSS 2.2) Specification", W3C First Public Working Draft, 12 April 2016, <https://www.w3.org/TR/2016/WD-CSS22-20160412/>. Latest version available at <https://www.w3.org/TR/CSS22/>.

[HTML-ESCAPES] W3C, "Using character escapes in markup and CSS", 12 August 2010, <https://www.w3.org/International/questions/qa-escapes#use>.

[PEP-EMAIL] Marques, H. and B. Hoeneisen, "pretty Easy privacy (pEp): Email Formats and Protocols", Work in Progress, Internet-Draft, draft-pep-email-03, 22 May 2025, <https://datatracker.ietf.org/doc/html/draft-pep-email-03>.

[PEP-GENERAL] Birk, V., Marques, H., and B. Hoeneisen, "pretty Easy privacy (pEp): Privacy by Default", Work in Progress, Internet-Draft, draft-pep-general-03, 22 May 2025, <https://datatracker.ietf.org/doc/html/draft-pep-general-03>.

[PGPCONTROL] UUNET Technologies, Inc., "Authentication of Usenet Group Changes", 27 October 2016, <https://ftp.isc.org/pub/pgpcontrol/>.

[PGPVERIFY-FORMAT] Lawrence, D. C., "Signing Control Messages, Verifying Control Messages", <https://www.eyrie.org/~eagle/usefor/other/pgpverify>.

[PROTECTED-HEADERS] Einarsson, B. R., juga, and D. K. Gillmor, "(Deprecated) Protected E-mail Headers", Work in Progress, Internet-Draft, draft-autocrypt-lamps-protected-headers-03, 16 April 2025, <https://datatracker.ietf.org/doc/html/draft-autocrypt-lamps-protected-headers-03>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2047] Moore, K., "MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text", RFC 2047, DOI 10.17487/RFC2047, November 1996, <https://www.rfc-editor.org/info/rfc2047>.

[RFC2049] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples", RFC 2049, DOI 10.17487/RFC2049, November 1996, <https://www.rfc-editor.org/info/rfc2049>.

[RFC3156] Elkins, M., Del Torto, D., Levien, R., and T. Roessler, "MIME Security with OpenPGP", RFC 3156, DOI 10.17487/RFC3156, August 2001, <https://www.rfc-editor.org/info/rfc3156>.

[RFC3851] Ramsdell, B., Ed., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, DOI 10.17487/RFC3851, July 2004, <https://www.rfc-editor.org/info/rfc3851>.

[RFC4021] Klyne, G. and J. Palme, "Registration of Mail and MIME Header Fields", RFC 4021, DOI 10.17487/RFC4021, March 2005, <https://www.rfc-editor.org/info/rfc4021>.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, DOI 10.17487/RFC5751, January 2010, <https://www.rfc-editor.org/info/rfc5751>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <https://www.rfc-editor.org/info/rfc5890>.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <https://www.rfc-editor.org/info/rfc5891>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

[RFC7929] Wouters, P., "DNS-Based Authentication of Named Entities (DANE) Bindings for OpenPGP", RFC 7929, DOI 10.17487/RFC7929, August 2016, <https://www.rfc-editor.org/info/rfc7929>.

[RFC8162] Hoffman, P. and J. Schlyter, "Using Secure DNS to Associate Certificates with Domain Names for S/MIME", RFC 8162, DOI 10.17487/RFC8162, May 2017, <https://www.rfc-editor.org/info/rfc8162>.

[RFC8617] Andersen, K., Long, B., Ed., Blank, S., Ed., and M. Kucherawy, Ed., "The Authenticated Received Chain (ARC) Protocol", RFC 8617, DOI 10.17487/RFC8617, July 2019, <https://www.rfc-editor.org/info/rfc8617>.

[RFC9216] Gillmor, D. K., Ed., "S/MIME Example Keys and Certificates", RFC 9216, DOI 10.17487/RFC9216, April 2022, <https://www.rfc-editor.org/info/rfc9216>.

Appendix A. Table of Pseudocode Listings

This document contains guidance with pseudocode descriptions. Each algorithm is listed here for easy reference.

Method Name	Description	Reference
HeaderSetsFromMessage	Derive "outer" and "protected" sets of Header Fields from a given message	Section 4.2.1
HeaderFieldProtection	Calculate cryptographic protections for a Header Field in a given message	Section 4.3.1
ReferenceHCP	Produce an ephemeral HCP to use when responding to a given message	Section 6.1.1
ComposeNoHeaderProtection	Legacy Message composition with end-to-end cryptographic protections (but no Header Protection)	Section 5.1.1
Compose	Compose a message with end-to-end cryptographic protections including Header Protection	Section 5.2.1

Table 5: Table of Pseudocode Listings

Appendix B. Possible Problems with Legacy MUAs

When an email message with end-to-end cryptographic protection is received by an MUA, the user might experience many different possible problematic interactions. A message with Header Protection may introduce new forms of user experience failure.

In this section, the authors enumerate different kinds of failures we have observed when reviewing, rendering, and replying to messages with different forms of Header Protection in different Legacy MUAs. Different Legacy MUAs demonstrate different subsets of these problems.

A conformant MUA would not exhibit any of these problems. An implementer updating their Legacy MUA to be compliant with this specification should consider these concerns and try to avoid them.

Recall that "protected" refers to the "inner" values, e.g., the real `Subject`, and "unprotected" refers to the "outer" values, e.g., the replacement `Subject`.

B.1. Problems Viewing Messages in a List View

- Unprotected `Subject`, `Date`, `From`, and `To` Header Fields are visible (instead of being replaced by protected values)
- Threading is not visible

B.2. Problems When Rendering a Message

- Unprotected `Subject` is visible
- Protected `Subject` (on its own) is visible in the Body
- Protected `Subject`, `Date`, `From`, and `To` Header Fields are visible in the Body
- User interaction needed to view the whole message
- User interaction needed to view the message Body
- User interaction needed to view the protected `Subject`
- Impossible to view the protected `Subject`
- Nuisance alarms during user interaction
- Impossible to view the message Body
- Appears as a forwarded message
- Appears as an attachment
- Security indicators not visible
- Security indicators do not identify the protection status of Header Fields
- User has multiple different methods to reply (e.g., reply to outer, reply to inner)
- User sees English "Subject:" in Body despite message itself being in non-English
- Security indicators do not identify the protection status of Header Fields
- Header Fields in the Body render with local Header Field names (e.g., showing "Betreff" instead of "Subject") and dates (TZ, locale)

B.3. Problems When Replying to a Message

Note that the use case here is:

- User views a message, to the point where they can read it

- User then replies to the message, and they are shown a message composition window, which has some UI elements
- If the MUA has multiple different methods to reply to a message, each way may need to be evaluated separately

This section also uses the shorthand UI:x to mean "the UI element that the user can edit that they think of as x".

- Unprotected `Subject` is in UI:subject (instead of the protected `Subject`)
- Protected `Subject` is quoted in UI:body (from Legacy Display Element)
- Protected `Subject` leaks when the reply is serialized into MIME
- Protected `Subject` is not anywhere in UI
- Message Body is *not* visible/quoted in UI:body
- User cannot reply while viewing protected message
- Reply is not encrypted by default (but is for legacy signed-and-encrypted messages without Header Protection)
- Unprotected `From` or `Reply-To` Header Field is in UI:To (instead of the protected `From` or `Reply-To` Header Field)
- User's locale (lang, TZ) leaks in quoted Body
- Header Fields not protected (and in particular, `Subject` is not obscured) by default

Appendix C. Test Vectors

This section contains sample messages using the specification defined above. Each sample contains a MIME object, a textual and diagrammatic view of its structure, and examples of how an MUA might render it.

The cryptographic protections used in this document use the S/MIME standard, and keying material and certificates come from [RFC9216].

These messages should be accessible to any IMAP client at `imap://bob@header-protection.cmrg.net/` (any password should authenticate to this read-only IMAP mailbox).

Copies of these test vectors can also be downloaded separately at <https://header-protection.cmrg.net>.

If any of the messages downloaded differ from those offered here, this document is the canonical source.

C.1. Baseline Messages

These messages offer no Header Protection at all and can be used as a baseline. They are provided in this document as a counterexample. An MUA implementer can use these Messages to verify that the reported Cryptographic Summary of the Message indicates no Header Protection.

C.1.1. No Cryptographic Protections over a Simple Message

This message uses no cryptographic protection at all. Its Body is a text/plain message.

It has the following structure:

```
└─ text/plain 152 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit
Subject: no-crypto
Message-ID: <no-crypto@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:00:02 -0500
User-Agent: Sample MUA Version 1.0

This is the
no-crypto
message.

This message uses no cryptographic protection at all.  Its Body
is a text/plain message.

--
Alice
alice@smime.example
```

C.1.2. S/MIME Signed-Only signedData over a Simple Message, No Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a text/plain message. It uses no Header Protection.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 3856 bytes
⇩ (unwraps to)
 └─ text/plain 206 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
Subject: smime-one-part
Message-ID: <smime-one-part@example>
```

```
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:01:02 -0500
User-Agent: Sample MUA Version 1.0

MIILGQYJKoZIhvcNAQcCoIILCjCCCwYCAQExDTALBglghkgBZQMEAgEwggFCBgkq
hkiG9w0BBwGgggEzBIIBL01JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6
IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04Ig0KQ29udGVudC1UcmFuc2Zlci1F
bmNvZGluZzogN2JpdA0KDQpUaGlzIGlzIHRoZQ0Kc21pbWUtb25lLXBhcnQNCm1l
c3NhZ2UuDQoNClRoaXMgaXMgYSBzaWduZWQtb25seSBTL01JTUUgbWVzc2FnZSB2
aWEgUEtDUyM3IHNpZ25lZERhdGEuICBUaGUNCnBheWxvYWQgaXMgYSB0ZXh0L3Bs
YWluIG1lc3NhZ2UuIEl0IHVzZXMgbm8gSGVhZGVyIFByb3RlY3Rpb24uDQoNCi0t
IA0KQWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUNCqCCB6YwggPPMIICt6ADAgEC
AhMPLSW9ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMg
UlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIw
NTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnelN41KImVaTC3D
9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs
165ernT9O5NLFflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZu
TtMc1zy++MxQlqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCqlLqhBwDH
dZ5qDTII2PVX1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy
6SCf58duq/AOEksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/
BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VA
c21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMC
BSAwHQYDVR0OBBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEw
jnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCBSXignLEynBak
DKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9Ii6zyBZVjdao
x644DsiLOQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz53PYDBh4zE4Na
r2inC0D+VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eDOdu+F2MVtl
uLihne0Bp1GUTkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb744gqoeuD9YSHjKK
49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzlEc2tUpAr4vR
hZjVD6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpqp1zANBgkqhkiG
9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8G
A1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAg
Fw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVU
RjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTk
fCv4TfA/pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY63PQWl+DI
Ls7GxVwXurhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TC
NO12DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtws1q7
ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTM
SiPR+peCrhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90njlsJLOwID
AQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATAB
MB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYB
BQUHAwQwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDT
IGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0B
AQ0FAAOCAQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3Bj
JOd64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIj
So27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahiXRn/C9
cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgkLD59fk4P
GHnYxs1FhdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+u
CDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJcOvT4as6a
qdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkq
hkiG9w0BCQUxDxcNMjEwMjIwMTUwMTAyWjAvBgkqhkiG9w0BCQQxIgQg+APzZJl4
```

```
pcksifU3FOYwAUqexbFmtbnUdg8eCFIklg8wDQYJKoZIhvcNAQEBBQAEggEARlZH
lulQA7h4AzGUznSRv1TB3w2u4oXQBgxTTaUFXvezPsEacndc16K4ESz8IpjsLEqC
lhFU6haOKz3OZnab6A8sCqozqAoCpJI35L3D0XwlqucqRDMQoNDZf1AZw1/2rvhl
BA4+YVc1vNjwbFF7T8bz6ttkXBdseesPV8zy01tsPVBSEr9A8QtVGTPw/BLEV/sV
d6QtbPMCqdVDjRAa5onUPyZvXkt+Qkt5Wcqxfwbotg/u7ecLhqnK0rC2SZkGDjtZ
a6BuLu88DxA9T90G+L3hhL5VPdEdkdRCounTb9McyGWWmnK0PYind/sKBATP5ouF
jj3rLaMfllxGB0xn3A==
```

C.1.2.1. S/MIME Signed-Only signedData over a Simple Message, No Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit

This is the
smime-one-part
message.

This is a signed-only S/MIME message via PKCS#7 signedData.  The
payload is a text/plain message. It uses no Header Protection.

--
Alice
alice@smime.example
```

C.1.3. S/MIME Signed-Only multipart/signed over a Simple Message, No Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a text/plain message. It uses no Header Protection.

It has the following structure:

```
└─┬ multipart/signed 4187 bytes
  ├── text/plain 224 bytes
  └── application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
 protocol="application/pkcs7-signature"; boundary="e19";
 micalg="sha-256"
Subject: smime-multipart
Message-ID: <smime-multipart@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:02:02 -0500
User-Agent: Sample MUA Version 1.0
```

```
--e19
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit

This is the
smime-multipart
message.

This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed).  The payload is a text/plain
message. It uses no Header Protection.

--
Alice
alice@smime.example

--e19
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
dHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
acKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOa
Gdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXC
N5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj
8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4F
zkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8
A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQs
qm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
a4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3
SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgE
ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOH
```

```
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp
7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNTAyMDJa
MC8GCSqGSIb3DQEJBDEiBCAokSzA71kmvoyy0h+lrO2jw3pvGhvgRnv/zTDC9IxD
UzANBgkqhkiG9w0BAQEFAASCAQBWL6C/VCYFv6ZiQR6JYBbLWiQJyAmNFrRhAbfi
w5bPndhDbJNSv3DXoUfCKd87pvD5Qr1PsH4WXDZ/IY95h3dD7k6oIIFXhPBTYYW7
Np+vrVtS0sDklr03+ebMBY6J0rEtNf5ZXCkQULTmvwmmuKcg4S+5piNqhTnnE0en
IvICii8NgjP3VVPZmNpFmxwmztGWd04omYHbY4JY9C7yvuQ6SNEQm47bxnSIS5yH
sowWnDYqs2cMDLxZ7zy0cEyOpSy8oDfVde4TyOifqMT3VzSmlttdG1uDNE90ek3t
xJn9E+hE02sw0Mv1lLjNdRXviRsaMw33DxGbtoUSo2mOkpYb

--e19--
```

C.1.4. S/MIME Signed-and-Encrypted over a Simple Message, No Header Protection

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses no Header Protection.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 6720 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 3960 bytes
 ⇩(unwraps to)
  └─ text/plain 241 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: smime-signed-enc
Message-ID: <smime-signed-enc@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:03:02 -0500
User-Agent: Sample MUA Version 1.0

MIITXAYJKoZIhvcNAQcDoIITTTCCE0kCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAFxh1OX2qKJrCxk4NBNVX/kprtR6yjMWM/1n
tepVdA0A/uf69sMzbyZhd8wFl1eapv05Xp6+1DuOZfqYgkbCJwD+ZtSL4MB7EBPM
ytxB42LTEC9f8Z/80L96/+nnDotKHxFSVZPXfmi+FKLLDlddH7bswV3GH/nozzYl
4wjesm/nvakHEv2CNJ2mh5XHq0gqNPDx5/2OmxaU+x0biLPcGNzFob39ok+1rTbN
/9fIGDLKr1ENzQXW0vixcyAS/RBlHw6WGby51EvV7FObcdxsXkTI+vvHTcTGbPhi
54ShTTEocIj7mrXzHodVEy0pysuYCl2hOkqre9HSspAqw7s+/3wwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
```

```
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAbrhe4bg9I4GbmhF5qnO5kJXw
JTfpgB3iK+K+bIxH/gsZbLAOx2UR2OHESrW2dqojynuxZ+QE571NXQN7X7THoOaB
mhUPuBRPycw/orR2GR0KCYx4taATw9o2fK3KssO+IAnNP1OM7yUsgABZHT6BfvtC
qH7ZPBJaj73A9AyrxTNPtJJHwueE3X5CPTODViasPRZrqiGB/WO/siuApdk0MPik
tp29bVqzQuD1tpDFb+aQyfggEnqGQn1ReZYhfBvub+AUr+O0lNOh57mob+eJwc0F
Snq9mljS3kgoXbh1DrV9S/seSdYZ7ieCiS3FYEi8h7RsZTGCVMn/STxiq13X0DCC
EC4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEP3eQZI7xmdgaoarujEjNYuAghAA
mXWuV/HZ+MiCJTgt1RWzuHw8hnhLDxcY444IeB0M44fryhiuSkUKDdnvy6GDRiUF
ThwVs2iGHdCgvh/tJNaXmF9fa/Vi/aHq/oL3wJi+cS0qkeeq2kpGSMm82mNBlmgt
uhcwozIru+2n+L0xspYIUx0+dG59NlfB1alRQJd7JmCUWF9AY/wVkGPkj5Vym+Vt
dRqGqcnJPM4Nq572bhxgLwDOCuoU+2rN5pdW1AT31odSdPtHoux3ysK+aMLcw3ch
mL+en9j/euqO40Xr3Re0J/suSzHobI5I0bDtQwaEoXooz6aQIZrFE4TtZLCDzG7o
ZbMf3rkJ1CIelKpbVhjRAjj4X+MvktiOfxVV4K3GYAagHI5jp+4+MWz2yaQcAnRE
7SpHFxuFdmSYYYAq0yTgxkS9opoAwxPytKefqnnY62wAbug26ZCpSM03172cKopA
gkBqljwFEl+YeauN6206vZKuOhNuyQFbPeO+00qKeHw2bPM+PiKWdzAkQKz9N4CO
kFqzOgEHG5HnH8jx9PPuU57g8TmJccDFuUrZ4kZVcfWogH7gsNyW+A06BSu9Do/S
I7VxMwenuQLv1+W/tm+zLqBLpksKOh81HVNVQ+4zEXx/jQBqM/Tv9BcetVdzGTIq
vCNn7KDLwLceNF7hgbNM4SfZZhg5hfV/xxeNpZx0tn86hHntN54FKymO/kXaFebr
W5yoXwvGHukCJJyI87NN7WIM12g5IHC829NIICAGIuZ/kxPb/A51WB8yr8748XXv
QcXKg7OxTzkVgiACGDyS3ye+fZCncBZgfQ0jcipQU7jVYu7+UiUZDAvuQwae/RUd
CSOhdjwtBzMlIazVfbIaHPM5QKvB+MzbAKUMWza+XRpjLrDVdaSFR06V4r4SUMsi
AvKdd/1RFvSTEhtNj1QOUKEa1DvnuRLvYsdjWLDF2TsBCjP4jdGKGG+PtfB4vcSU
NFJSJ5epaUIDxbFkgSolRF+lM8790NdlgkhY6RbW3kXkA0T1CmKIYrN6poYxCSwU
Q+RzGurGDMQTGvfDgZrObvdE0haaNEdti/ci2EbcasYa3um7HCpt/bKDw5sivnh6
9P9E1WMvdAfEinppCZO8yRrkS1l6b9Jgk6ohJWftQMA2OmpKGw6tRbblH0tJ33JR
8ghApEJpSvtoKGc46NTelR6hBgxoaJCebRpxJ9wrNp4EETj0/PbZDiDzNETWDZ4E
Bn74vJ2I3wCltkk16SmnEJadZovBlyqKYB6bmFvX9S00hOBv8TZ4o//mY4nH57f0
5CmUM42ePRS0HMk9SrBjpouTIkw/tbDieZNb4tA09B/c3/s3qpZ2Bo0Bz7RVRI79
D2P8hnp+/7y74rqyUdRdqW6mFXjNojo1A+hsbXWqTfuMcSikbENC59pmhMDxdS4L
GxJCIVoZmhbnjeEhIMqKwa0NtyLLG8uRlzdTF8g/IOI6UwCeFXl/dO3tvLoEB/KA
D/n27IyDILDldYa1Em7I8jQmQghJ1IdMrUlr1n/mRB+sql2IDVlI95+r96IrFdmj
AWVMX+vbq6n/QNcaxfS5nL7ICgV9kQHO9AtzJ4zXxLDj62nkIdoCRupF+IlHXL9G
OmgJJFj0uhgXO67/2G0cT2JME1siW7/F6JHzlGAyeVSoPs2FAJKYMQvvkR6jbn3y
Huw3s9RS31co6D+nvxJHLvr/REVwiLklxPqimC+2pmkUjRYyL/aXRV9pDuNJLtMu
XJxqwrYgwPw9mBXXaYLgo8G+SSUfeBKvwuKa2kd0prB3cWwfIWlZBgZvVGc7Uudz
QzxyMaDt8R7eVG6/CXUeGOMSWKbjzoZwkbB/QCgZetVO3YM7FqhEfvmg0tv1pS0c
nprxkkMurw1NGearPv+faBo09YSswF38ol44A8hdpYIGc3LL4jj4wSPdS+lMVp84
nKWnZJ/asIS74bEH7TK3JK6tgOPEvh+GDMODoXALsnH157oDi0GeN0kwcB7CeUT7
6zYaQT07QcgOUyWMEOlScOi9zibws0ZKL3uNTwmF8p1Jv2TEvepZQiL2/xbENTmf
H+47tdIPUlJOePdjUGo6QTAaqSH5of0e/T/QENueeJOJboPgbaV0OqTFOVVAMMhA
upadP8ROG6TalcPC7X0gV9Yi60vd/WWVTJPPLDf4+FJm7HmkzT5l5fOAuA+mYJUO
F+BPTUCKyeY9VypoXDV0VnTTpiB9jfyOlPJjBnZ/85Bvfkt0eCW5rV7xeq7tgSJT
+LOkTfwDBqlOZt1hlvKe3SFHnsW9hdojlJz/sXw5FcFCxbxqfageVJ60uamENOhB
j4Q2ZRvslLXxpVME0ifG1CxpfAr2ZQsEormIu0zJeZjkDguwNlBInFKHFzvtSEJp
rP4hAqknbSvOqUdAFp9rlII2dYXI4xh3kV3ECvhvwFt39PfVpGL97R92cTK9JCgq
p9IOJZv32FdhEsaHqQIRklw5xy96fTwbrho+LQSZIMUhTQ+hcqtcRX9cDPA+VZO/
0vLgkF1R8rAWOTCxu3pHELjDq9nKKIzvX7tmyKapFgC38uotkvvKzpUzoA2xPoVH
ybrM09g9ujruzT/Oz02cDa9NWh2eYsiTWJvekeNftvakr6U9r7VYzUkmPCtfDDKC
oWSZHgwnU50Psl6UoTFaw1GuVnlC3cOREOUvFNbtV6R9Jdn3y0XJ0T4uZapFHPJf
naojAoE5iu3VXRMxVZB+4vZWhFJoe4QNvc5t0kwUZVmE1nQWNkHuRyVnpfoLqaG1
1+5IpR6yIZDHlWm75oc8hchG9PxrE0O2WWUqf+QSEdsT74cGTJVOZDl6d4x/G5g4
97v1JaCSCgB/J9yrm4olsqgoYfWAbTcIBe0cUHnoNMAstKqH26jAf0Hz1l3V9D7M
zt3POMck+f3lLNUCqyNLcSASWc7jmB170/oF4vNP1EkgwWaz7yBluTLS8sJCIViV
YYyZvj4du48h7lKaxeairWjcen+qeIS+Tn8VHqoJD6+QJinH5bXMKtxX0Orvf69p
r0WjUctKikcjJFRbc6sQyMP6Y44+6/LyFmWILTaV1WPoWLX5MYKOwP1s5GRneGWS
mZRztWt/CL/8DWjpPEG2siCSaS+lBc1u/C5HkD1UVDjPmZTnvuFTHukaTKfteGz1
z0Bxuz9gQMyAgU0OMyl+cGldHeR3HvIC9zUZ0qRj/d/20M8aQ+8NtVodadiMt29p
```

```
THvkrioxuW6MVKXs0gZgdL72swDHtG3lKW1rrbufgjSr0UvSc8/MDgBPJVP2d6QX
P1IJvvBcr766DZ26j9/X0Is5cJjCN7Y0fIrS4RGu5aQR0w+dOulK6v8q8reYZy0K
198CRs3prXRKRPiU0oM16oQdsV9T9LhfOnhWeliL/HzetEltcOSiKgGKVYcArkZU
bzxsxUHF7q7qEzF2fVzWYBnM3qn8Shj3HHlPWYxW6uh5kI6O+mV3Hs56KJjD9zsZ
ZIzTE/5agYXKpliVrGScTUUGeDqrPPyEtOGRTmiQDLISHfW+nviZZcjC4XDxp04b
v6BH3EsSbXN4wJAXypDCY2kfL8wzqMh7qh/8Pk2AuodDtCJQJGsQPkgGwX21lSR2
4C1J1WJqDEaNhvmMf7B9nUu8unXYwwFe7FQN22CYZJOQloj04T1Ukg7wRITeWwc6
xArdNOTn+XQuXfkxVEbiQRhiFt/47qAzoAjPRVr9r4P89Hz3wkTIxirpAjTnKA5v
osv/7+28rRuYRYGu2yPwNeUPmO0YHy3IeTVKcJ/UcmO3cXAe+Q+9ckmZ/MmxaxA1
zvj2pH+INf3eBsQK77PxwsaGUFHqKWS1Wvk/FPsZkGEMX6QcD56sbGRbtsRRryXy
4L0Ul3Jc1P1jwMjHldGEqQohVfKYvHwdOdMaExZh/hhlpfxw1Cwh/d+xuuPlLko5
HTHxwlzQvRgzTlIdX78XItFIYo+eMOb84xr8kAaXwHWpuZ06tymA59kD7LpvWVC6
r/OmqcnvAVDg/eiNh6Kru4BkIiTMtBs313ruZtSe8Hphvm80fYcelpfHs8Y1qrsS
EVohhfxL7073Td6jScN54FZU3dg0EfFg97wyn+2DKeckNr5E/CgdD/FqhkH1IaEO
8wTbc9T/6XC+n27q/kQAMXzFnhn4Ec5E6uQb2MkCJEpW91eg9ZTDRYsZW1/r8yz+
QzbrSDSjVRvZ61FkGdh6m4i024ZtfCUV08AXoOhGKCh8fG/PKmCMzHvqQezO7I8I
DFLTBhWBag9kcNljVFnBYFl0e/hGnAZ6aDc6AQA0HdIZiAF49kEBhCLtOTsa4UHT
npIjhKR6fi1RuiVnFkTqfCMgZawLlZOkaQX2BdH1bsz2Q8wbu/DiNoyXdB/1k3Y2
9yLcVvGRCnyXODjehyoLF/iJUzewsu8fzlTJfV/CCo07cDge2PdnDPVdEl2nM+BH
Qo4scmT4cm1YYNGoecy9wGSgHE4fvhk0Szv0V2Fbt5HpJqsJvKH573AlCxROpumw
rOttrdRvke2vTw2nlw5iW1lPhcIpUQAEZfpxQ2lhJfRvJiWDBvimAjVlHipTd0xA
oNZ383NE4SLWvNmjryk/uSvqoMXvof0Hatm67So0KMVDmBA5AMMq+9TBNBxaN1WW
FIuWMzmMWZYCMYm2Lmz2nUOdqVz95Y6rEsaMqQoft/UitEYyJdqawyMXYKmwtYzN
7yES4hRc3ee3JTyogrEtirg87pJ+RB7wOuI9FVjkKhjgVppGQVZAKcpeTRyrqjNU
oSycr2PbV3RPwzDRXX12PigHgX3suLehccOWAMFvpQvgixXU/Ik5ScDcuLC4o/bs
juzOjy5ENDOjQldvC1bgfPfYUSZAvd/g0SYDc0xzC0Dm7dudNhuwSNDT7R39qh9t
eBZSOEI+1TKIxThFhHjKnWqxAJP9LJZbk7/L9QaKfQnDxQkPgwaFgskPTBflzgXd
4inGVpCfaO3dHbhcb2EdF3jiIzHH84S0w5L1ZmXGgYUfNZHNkFf55VYZoTxNCIuA
Duc6jWMI+BXIxXM1hJ0YYY9OYljhT1vpv0VS6rj8zrr9y4xkH8dIfDdVZh+OIqI5
jGMcCDFrCk03zHtLeYTWzQge5p2UPRRQWoxjKsjDHehxWdtHzfUsAAhx3f9USH3b
+nt2vLL2FuSjJMtqS9ACRFncGCQAPsdXjozm85raGnn8p4j9EbN2MFzQ1/mRA3XM
3mNpZ2/qT2GUOB2d49WLHJvesgKGbrIQBb0eM6//hH84BonFrSR6Sf0uUjTGiu2L
PXWkcsTORuAaaTzM33OVOzQTAhBS27vhMr/kxMZSdTx/14phEaJ4zkYzzPb+T92G
CpiDpwEfU2akyZNalZ9jTo28zq1gZENDRu6tYRsjRvPsDI3JN4702HZf80KFhdO/
ZgQ8egO79JS5iJASxu78DbC8Lo28DzDN7etUTCLKxBmz/IQFIHDDkxmzNgoF399J
BiD2T2KmI8jOgLaSmuAnyw==
```

C.1.4.1. S/MIME Signed-and-Encrypted over a Simple Message, No Header Protection, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIILPAYJKoZIhvcNAQcCoIILLTCCCykCAQExDTALBglghkgBZQMEAgEwggFlBgkq
hkiG9w0BBwGgggFWBIIBUk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6
IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04Ig0KQ29udGVudC1UcmFuc2Zlci1F
bmNvZGluZzogN2JpdA0KDQpUaGlzIGlzIHRoZQ0Kc21pbWUtc2lnbmVkLWVuYw0K
bWVzc2FnZS4NCg0KVGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlN
RSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2ln
bmVkRGF0YS4gIFRoZSBwYXlsb2FkIGlzIGEgdGV4dC9wbGFpbg0KbWVzc2FnZS4g
SXQgdXNlcyBubyBIZWFkZXIgUHJvdGVjdGlvbi4NCg0KLS0gDQpBbGljZQ0KYWxp
Y2VAc21pbWUuZXhhbXBsZQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJU
h6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UE
```

```
CxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNh
dGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MTha
MDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5B
bGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqV
KfqLwaLjj+gBUCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID
lB/wlbdmadXPmrszyidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdS
NRFxrfKeoQEFXgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1
ZkuE4A6l41koaZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv
9w43GG8FtpSX+TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIB
aVv4wPxAf1iPsIVKarUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQ
MA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxl
MBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQU
olNB1UQ8gCkVfAEj8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpn
HGh29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9
eBAuDLsatbtKtl4FzkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLv
Lir3hEUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLro
r2X4P5uXxaP0LIZRzWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSY
kGiWDp1JhqXwfDz8A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzS
WHUz1F00juyuOfQsqm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIIC
t6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTAL
BgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUg
TEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQx
OFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhM
QU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oulls
k4ASvSwjsCNo7sHUa4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpX
mFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2
GxzymsO2kaYWTut3SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wX
VgkWFfiOucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7B
tZcsl7dUy9u9COgEykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYD
VR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYET
YWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8B
Af8EBAMCBsAwHQYDVR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQY
MBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2
p86poGkjd/4KkkOHG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzh
W/JVdYn30UxfyrZlRAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEN
t1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9C
Dr4Opq2JCkzP0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0T
zPCVzUAuBlr+JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+Aq
J5QfH+0e7NSzNnEmMYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYD
VQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQME
AgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0y
MTAyMjAxNTAzMDJaMC8GCSqGSIb3DQEJBDEiBCCb47LkqJUmFpzt9bQAPoWpk+vy
9sGfzpOuEZflV+goizANBgkqhkiG9w0BAQEFAASCAQCd+I+Tr7hDMV3VFvFGduS9
4ysR9dceBgPloLOH71fsoJUl508WspagFkqjkUGPipKfYVrssRi8IHQM682HQqUk
jkB0UYx0hfEBVbsDvhYejzOYfyLRQD6TYI3HTVFJIJIKVk3JQUuQWzx+A5i14oHI
mCeHl1FgRq6D1B3hjpWFFWI35pRZ1gSZ3tPryQwq1Y0bMkiF4CeuUYEKWIdFHZdo
u/IMfLJoJeYpy8cyv6FznuJzkAR9AlUIUw58zXCD0ipCfKH2w6vwqdoCo4V0+cZd
5cZlYQSFab3fduU44viKaXf4VOpWK49oDeR/tV5i1LfM3ZYeH2V1r+pmnjyt8CcW
```

C.1.4.2. S/MIME Signed-and-Encrypted over a Simple Message, No Header Protection, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses no Header Protection.

--
Alice
alice@smime.example
```

C.1.5. No Cryptographic Protections over a Complex Message

This message uses no cryptographic protection at all. Its Body is a multipart/alternative message with an inline image/png attachment.

It has the following structure:

```
└─┬ multipart/mixed 1402 bytes
  ├─┬ multipart/alternative 794 bytes
  │ ├── text/plain 206 bytes
  │ └── text/html 304 bytes
  └── image/png inline 232 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="0cf"
Subject: no-crypto-complex
Message-ID: <no-crypto-complex@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:00:02 -0500
User-Agent: Sample MUA Version 1.0

--0cf
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="6e6"

--6e6
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
no-crypto-complex
message.
```

```
This message uses no cryptographic protection at all.  Its Body
is a multipart/alternative message with an inline image/png
attachment.

--
Alice
alice@smime.example
--6e6
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>no-crypto-complex</b>
message.</p>
<p>This message uses no cryptographic protection at all.  Its Body
is a multipart/alternative message with an inline image/png
attachment.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--6e6--

--0cf
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--0cf--
```

C.1.6. S/MIME Signed-Only signedData over a Complex Message, No Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses no Header Protection.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 5253 bytes
⇩(unwraps to)
 └┬ multipart/mixed 1288 bytes
  ├┬ multipart/alternative 882 bytes
  │├─ text/plain 260 bytes
  │└─ text/html 355 bytes
  └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
```

```
Subject: smime-one-part-complex
Message-ID: <smime-one-part-complex@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:01:02 -0500
User-Agent: Sample MUA Version 1.0

```

```
MIIPIwYJKoZIhvcNAQcCoIIPFDCCDxACAQExDTALBglghkgBZQMEAgEwggVMBgkq
hkiG9w0BBwGgggU9BIIFOU1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6
IG11bHRpcGFydC9taXhlZDsgYm91bmRhcnk9ImRiMCINCg0KLS1kYjANCk1JTUUt
VmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9hbHRlcm5hdGl2
ZTsgYm91bmRhcnk9IjUxZCINCg0KLS01MWQNCkNvbnRlbnQtVHlwZTogdGV4dC9w
bGFpbjsgY2hhcnNldD0idXMtYXNjaWkiDQpNSU1FLVZlcnNpb246IDEuMA0KQ29u
dGVudC1UcmFuc2Zlci1FbmNvZGluZzogN2JpdA0KDQpUaGlzIGlzIHRoZQ0Kc21p
bWUtb25lLXBhcnQtY29tcGxleA0KbWVzc2FnZS4NCg0KVGhpcyBpcyBhIHNpZ25l
ZC1vbmx5IFMvTUlNRSBtZXNzYWdlIHZpYSBQS0NTIzcgc2lnbmVkRGF0YS4gIFRo
ZQ0KcGF5bG9hZCBpcyBhIG11bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdp
dGggYW4gaW5saW5lDQppbWFnZS9wbmcgYXR0YWNobWVudC4gSXQgdXNlcyBubyBI
ZWFkZXIgUHJvdGVjdGlvbi4NCg0KLS0gDQpBbGljZQ0KYWxpY2VAc21pbWUuZXhh
bXBsZQ0KLS01MWQNCkNvbnRlbnQtVHlwZTogdGV4dC9odG1sOyBjaGFyc2V0PSJ1
cy1hc2NpaSINCk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5zZmVyLUVu
Y29kaW5nOiA3Yml0DQoNCjxodG1sPjxoZWFkPjx0aXRsZT48L3RpdGxlPjwvaGVh
ZD48Ym9keT4NCjxwPlRoaXMgaXMgdGhlDQo8Yj5zbWltZS1vbmUtcGFydC1jb21w
bGV4PC9iPg0KbWVzc2FnZS48L3A+DQo8cD5UaGlzIGlzIGEgc2lnbmVkLW9ubHkg
Uy9NSU1FIG1lc3NhZ2UgdmlhIFBLQ1MjNyBzaWduZWREYXRhLiAgVGhlDQpwYXls
b2FkIGlzIGEgbXVsdGlwYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBp
bmxpbmUNCmltYWdlL3BuZyBhdHRhY2htZW50LiBJdCB1c2VzIG5vIEhlYWRlciBQ
cm90ZWN0aW9uLjwvcD4NCjxwPjx0dD4tLSA8YnIvPkFsaWNlPGJyLz5hbGljZUBz
bWltZS5leGFtcGxlPC90dD48L3A+PC9ib2R5PjwvaHRtbD4NCi0tNTFkLS0NCg0K
LS1kYjANCkNvbnRlbnQtVHlwZTogaW1hZ2UvcG5nDQpDb250ZW50LVRyYW5zZmVy
LUVuY29kaW5nOiBiYXNlNjQNCkNvbnRlbnQtRGlzcG9zaXRpb246IGlubGluZQ0K
DQppVkJPUncwS0dnb0FBQUFOU1VoRVVnQUFBQlFBQUFBVUNBWUFBQUNOaVIwTkFB
QUFjRWxFUVZSNDJ1VlRPeGJBDQpNQWdTNzM5bk8zVHBSdzIwZHFwYmZBUlFFak95
d2l3WW5DdGtES25iY0xrNjZzcWxUK3p0OWNpZGtFKzZLd2taDQpzZ3J6ZmNxVk1w
TDJqbzA0NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2loQWY1WUpydzd2anYwWldS
V00vdWxpDQp2ZFBmMVFaMmtERDl4cHBkOHdBQUFBQkpSVTVFcmtKZ2dnPT0NCg0K
LS1kYjAtLQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQw
DQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMg
V0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3Zl
bGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gB
UCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXP
mrszyidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEF
XgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41ko
aZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX
+TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iP
sIVKarUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZI
AWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQM
MAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkV
fAEj8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJ
KoZIhvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtK
tl4FzkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3M
RsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0
LIZRzWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXw
fDz8A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu
OfQsqm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3
QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElF
```

```
VEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNB
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIw
OTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEX
MBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo
7sHUa4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+95
0MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYW
Tut3SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfC
n+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9
COgEykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIw
ADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21p
bWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAw
HQYDVR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwH
Fwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4K
kkOHG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30Uxf
yrZlRAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HV
X524bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP
0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+
JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSz
NnEmMYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1
dGhvcml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkq
hkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzAx
MDJaMC8GCSqGSIb3DQEJBDEiBCBkEM75wgxSOKXxqQLSNadhQ5kDl0ABIYw030cj
kP4nsDANBgkqhkiG9w0BAQEFAASCAQA9zet9PbdeBOdT0TVjIwCXvUjnq1/UN22d
GV2Ql//QcTN3Z7wMvLilhcYHrL8Sl9lIm2XYCV9r2yqvVyiB+qN+69y18HIzZ7ok
rgqQ8TDPt4IW2UXxyXrBOItFirLKklntf4SafPq73ipeZLMc3x3jr84lr7psIknp
EEmNM+okG6FHduKq8nSvbAKlahOE9qvDGcBJBYXtn+/ijqA6Fxu+mJDshCz0Vvq4
uVXp0ZS3pyO+Gg0JJnLD+z5+MPqO8TrSTBhZYQauVQFji9Kjb2A8KZpLjEXvw/JV
NqgxW8weaEV03KYp+fbsIdTSDwrz5w9rmSH1b+ReoY5kMa50eu9w
```

C.1.6.1. S/MIME Signed-Only signedData over a Complex Message, No Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="db0"

--db0
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="51d"

--51d
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-one-part-complex
message.

This is a signed-only S/MIME message via PKCS#7 signedData.  The
payload is a multipart/alternative message with an inline
image/png attachment. It uses no Header Protection.
```

```
--
Alice
alice@smime.example
--51d
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-one-part-complex</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 signedData.  The
payload is a multipart/alternative message with an inline
image/png attachment. It uses no Header Protection.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--51d--

--db0
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--db0--
```

C.1.7. S/MIME Signed-Only multipart/signed over a Complex Message, No Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a multipart/alternative message with an inline image/png attachment. It uses no Header Protection.

It has the following structure:

```
└─┬ multipart/signed 5230 bytes
  ├─┬ multipart/mixed 1344 bytes
  │ ├─┬ multipart/alternative 938 bytes
  │ │ ├── text/plain 278 bytes
  │ │ └── text/html 376 bytes
  │ └── image/png inline 232 bytes
  └── application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
 protocol="application/pkcs7-signature"; boundary="872";
 micalg="sha-256"
```

```
Subject: smime-multipart-complex
Message-ID: <smime-multipart-complex@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:02:02 -0500
User-Agent: Sample MUA Version 1.0

--872
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="757"

--757
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="3ff"

--3ff
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-multipart-complex
message.

This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed).  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses no Header Protection.

--
Alice
alice@smime.example
--3ff
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-multipart-complex</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed).  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses no Header Protection.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--3ff--

--757
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==
```

```
--757--

--872
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
dHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
acKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOa
Gdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXC
N5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj
8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4F
zkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8
A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQs
qm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
a4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3
SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgE
ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp
7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzAyMDJa
MC8GCSqGSIb3DQEJBDEiBCC5KpxWrqp9lc/at0VVROdHn83fXt5r6VC1EPizN3pz
YDANBgkqhkiG9w0BAQEFAASCAQCVWFu4+5JFFOLMcfSgjQsyxsRKPplmT35MrYT1
rZKzBqdb7BgsgtavL6xHs/GKGjbqHwrrPADgsnyeXwotOBZoFzxLxw9fQI7z7wH5
QbGLEj6hRHvrSdYzhlptTnTqc4hXdYwh3jjNJlIf1D01EP9KySaLt3M/aGcNUKDO
z2ngLLtpOQULqGm/IxkIG+Rj9YHlktQVEiPxtT+TQ8qO0eiHZVukT88BpGOBBpCs
9aLUH2JuEF6v6wKp9S+sWj4sxO9bzYmNPOmi8WWyGYx5NVldgzeZxhISConuiji7
```

```
e3Wyda9wa7pqiFz0nsY+/mqILYTxBYMcsjN8uZ8yCaPdcfpU

--872--
```

C.1.8. S/MIME Signed-and-Encrypted over a Complex Message, No Header Protection

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses no Header Protection.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8710 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 5434 bytes
 ⇩(unwraps to)
  └┬ multipart/mixed 1356 bytes
   ├┬ multipart/alternative 950 bytes
   │├─ text/plain 295 bytes
   │└─ text/html 390 bytes
   └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: smime-signed-enc-complex
Message-ID: <smime-signed-enc-complex@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:03:02 -0500
User-Agent: Sample MUA Version 1.0

MIIZHAYJKoZIhvcNAQcDoIIZDTCCGQkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAGaxvLw0XDiDHlLUZffbDPPnrxQvEqUfaDKF
q/0tzSwKuX4GYXwI2srRxm04umoeqcyUdiaBx0Vu4R2mSCSUFspk+W9KACMLqpTO
hAheLjlB2C2Pu0t0NbkbO74Junxy4DM7epIDpMRqfDs78QSJtuLehkvZRSPbu+of
fdEjeihEluJrK171PW04zgCUajmHpT0QFkstBnP8sI631tIKutQ1tn7f7NbXFSkI
gnfZnpO9osQpUI1hfDbKsPE4Lsv0p3R60Bhy3xK27qS53KMH4bzQrIN86FiGRgYL
25s0O3jCSDuNimD1q0Yq3ADJwiN8JE4vxl7ohOvhqkV+cFfiA6MwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAjofQnu1xr50wncKoCmExvdj5
eIbwYUuUrpfriURfX3dhMTAQ5jnQghbIi+zmTuraElTk6Vi65/rpDBz7a4YBAaeQ
jz3GH4ua8j5wrYe44ipXaZnHd2QkS5zYCER/lBD/lgCrgewhy7Ef4QI03drzT3zF
rc2YozxaViKZ/KUaBn27BlIPZoXWtahlSa8TnoZkCl4to5mI5K6vLuxAR7WgFC84
5vpnELyyiXcET0cjDnnvfx2wfUpBPo4gx1S+VTzcCn9i/b35LiLoVWSlWabY62Zt
RRlNH2gTIqNKjw3X6XvSM63e6qilg7vxWf1wv6tS+mlgsVzxc58u1g0zCxKuUjCC
Fe4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEL40oVxNKumsqJAgvAxYpoaAghXA
WAvh2j69ZQKJIU7KRi1TU4RuE4uuPBn+QLa5OYXocxAA8bN2x1BcW14DgROhZ6mA
```

```
aNv6yzK+aNkYpnlKLwo+YWw911hMLdjVBUJxZan9N7RvRTwxvBqxUFP56m/t4Nxw
lKkRICb2yt0+/RzMHA4NqAnugmiOPs1Fcva2vXL5eRn0vrxQCTQOkuPdRLNMlJX2
u1cT59pFStaxkPxE9MEm9ES8+nuvJNX/aOmUrpvYQsED7vCVdlemd/NlQ8fbTiMj
Alg20nrbCxMBgGKb1RqpElmLP8t7ip1JX3Uqw7rB0zVoRpf4q4nMN+WIdSsJevnn
cyyO9kTEhklwTmkldme2XSmuPukBjW1RghHV5hpWDmLssURpb4rMf79l/8mbuZbQ
juHI7gXVdutDH/VxeMx3fPYtYRrkrXia6XHtHFoIfRuYuXeoX3uG36FDrCXUHthq
5TujlJkI2l8gYUsNUl9JpFj5mauVnlWHc1ZdgY7Lu2DCVooybBD4Zfe2laQKl+ZD
KiVi4yxFWMlbZzENMmwUXnrf12xl8uEzNW63Ms573Cp6DgLj5acfSJPA7GuKT25Q
+C2lfP4o48hMdwqL7xZU1cxEjiUE8bhvBVQ7RNvWziANmI+vzAXyPmq+LNjeaig9
yzTEDRrcDISL61wVBf1cakbrDS/zitKy4WZta15pWLpXS5Nm0o/j78H424poEnkl
BLdn9VFjENNYqszWxUmTxMoGE9bMFAOQny4FrMCyuFLVcu2ktQg6L2q8CSw98Eod
KAg1vyKIYUtNMghZpx2dSWaVV/0dFzgV9q3ezgKft3GrZ2MP/vdCfNB0+GM9yJ79
KJcgdsmUv8GeIs0fkihsABdUMZn/kdFdDOQIx4w9K5hmxWXeR37ancwRloBgC2Ke
5Ci/MtKsHtnaAMhAhwHDtaB2jlITWQUvu3uBe4CffQaZblYhro1KedIcMco/Kw3Y
sQgE2SBhKTmiIQC/JPlnn350J93zVEzdouhzjXO9NyJpQHX6l4iJs8V0GevTfcXN
0fsuT0XdX5aRjlFKB4Wv4G6jVf9lQqNHpr/fEnSeuz0bFnGrZetRYHlHu/gxsDDA
BHAirmRhPNUJEMWkeC4t9MWfDMtI0EFb+80E8y27bYh3VlGxJS/Mvfwd1sgRmp2+
17Gyny7MA9xMtIhetzGOpLb/8dwODdenv/Set1qJ3yDDS7S6UnNsbuK1/08OAYBL
hNbO5pGYiQohflHkq0Rrs1ps6lxdz5hk2fm44sgCKtTC3S7g5OUbATSx3zl1aEE0
bnTcNEoh+iHUj4YFRhz/sB8sqeodMJLSlbUlAl2OgmF+cJyLT7+SdAR0/vJxjkgP
vVB1p5Eut27JGaACrXfWE/hGGriLgdiT4UgV9f5pru7w9TVM67jc59+7Flz4bSCt
K+xUskePye1SN4DeaSDOm9hYUZMfKu9lcXAWRdGJd4zWdICBbWcfNvuajuFZbOE8
l6lmS61f7/6zhLSREt0xNP/hsJa2QpnDE5hQWql3lkyC7k4T3bGzvYRKO5D063kF
Mgo2aofZ4QdbsB17POiibSEj0KyxhXCDnjSybQ25gOycg0VoshVZj1loxIDfMZzh
lRuA04q1dm9W3o/MXKLbhWhyFAEJswnz05VxrxYUQLL9mmcp8I8fN1YH9gd/DQQC
BQPkzzFs755rJpdPJ1KKoj8aKefDzNSBszgHdwNUjbrGHRQAgqYg8QHXHzG5SNA+
xX1uvJv7gMcrlSFYTKKgWKM7tdBmD2dhxQL8FGI+ZlZEF9GZ4UIVEMRVJqZ1kQ0k
qsR84dxCejnALehDDAjsYl1E2+OJA8DO+ddjdPlF3h5DNGs/GwJ0CkStf9mWt2LG
uwueWxdEeI3jphF75ttwJ4v81Dv4vEH0suzcQS7O1PZmLoqXu/h60SvKK4txEr2O
60uc8un8a4//WcMotRQMfMmYmNomY/HaayEhbEPWofENsEgsa+70oHFgqcM70Mts
TyW2MOXM7KEgUH8YRsHLx5a1V2TCqVeJmUcq/MeQZs30rxBywGNVRPijc8XSV9kO
fRI+h+d7c2YROk8QLrUmdZdKxg9229I40r5jwGOzwljFCYEsyWC8AEw5TKi0Y6mE
cdkY8viRK1ZkVTfR7od3xgfzjm0Woo1BW/Nj4Q3j9B7eR+TdOZqq26/t7XiqzlMq
jor08wBhE4GtrxBHvIjgvArniBe/z9s4p5ZT5sMWqm7YEzkAWeocT5cvJGZVdmC5
CtNUI1mmTIngy57sIxl6rSXcdrSl8qMvTc0/7D3mSChpj1OQxhP95jtEkYMAyqsr
vJtZMCaumihR3BKbnsPkdpZeXb7VBGW08M1jv9dy2MucmTCyP8inDhMwPuj1sn2f
VRqgyqWCfLH1N47gXtNtKbOvzJ0NkHfJqpJRY6NtQ7mVHT9ZUjh6HjPVU47TikOJ
PU97IYvGhwGnKf6ROUXoUt0X4rba77kgBAA8NqtGFB0O7IZlNzL7hb98TjMOM0pn
piWsihdkP5OKgv9PToRlhmv/g1ZQ3Dli2oFBmdQrdMOfvqWZWtHf6qFXXasjgkKh
Rcr1o4TfRQT/WbHj4Mjcx9/govqtB2ssw30JTI2s6NxVt+0GKk798W4mAClYqSDY
2nXBS0Oa7vr3MRzlmwMtFvLe5WIV4ojjvcjRmgFLVA9d33D0Cvb9h5tk8jcHO7H+
mhcXWhKq+Ugmk1xjKiNqFOUmif6vr9lwv++RGJEuujVWRgucfMuuQJmhOTBeuEHA
nTg3ILoj5I9CFTBCr8w8CGfJsax1gmOpY39aXxgXNBWH8YhGPi9UYu/cUdiXyEQQ
kBmFWvaD45247R1ubkERejEd05zl/K+93KhzVDeoMow/Q0GGEEQ/SZ5als5NpyzJ
Q7qI5jDjSqreiRXRrX1WQTN/7aTaCnw1LwNO5SNHVzZP1vAQIZQlSYxMzrFPtuF2
5uiFKJrUpe48NkLNi8bAKOb3Wc4OvLlPhbBVQuRz0lN8VE8gZMcZzQcdsFvorEor
+4+ABaHVsTbdrrLGSGSpTcqGpTcd620H9JvrrNgfdv7eZ/ZD7TT9XG6coy4dzO33
gaWIY+VZy/poMm+bFjYD8B7bc+qiTYQrIyBmFaC5haFgRnvN9nFq2OmL40g5Q9Ur
eLfPwPc5aBgr+kKjebSMl4ZLV7T21BPDBDZ8JWFWFutw/SUR/7a9S7G8YkztQPxh
/EMrFUsxK+eYu4OCbTGMOdZOAvnLO3Na3AjaSJGVdCKU50Yc4HxZOdTOMm1tfRj3
PZIWjOp5lYue2SK/pqG1GeFztaZbGF19zkLmZMRr1KO71RQeaIl1wlkZYOLRonIS
qE7z6mj//Z5x6zP17i11LhhWMIxZECpMFjKA4dkfXLpa+aMqd8Wc7p1F7UeJbu+x
K4kLfJdRf+YjIc6F+OtJClK98AKxjfX6Hs6AdTBT3SkKci4qPmNOslv+GgyUP4yf
MwXiTn3/TvlrHARaEQrKCTUL6GnedTEFZIPy9UUcG82PerOeyitm6m4SmSo+VxSf
grQQP1rCjz0xxaz5PT0+6rdlki53T4rBUYzw3El1i5r7XA0Pw9+dLLLzRWL5l4Dj
vr4XvuyhKu7PZahKtoYMBKVw423JxNpJkgP2DlhEb78pUeNMaUUwGyxjSLX6mpf5
c4a5Q0+R9fw4Acs/QtDoX5ZMgMoSpdN8x7AdBtxolicWe/iQECurAnRYcrwKXo7+
WVURy5/cq6Z3STIHqdCcGBBJLX9OsGIyBK80mgmhNDjbRe4fdeVXOSWQOcdNQSXT
```

```
KFg5G75UuCkukly7e31XNbhhRQy58jbuhM4bptnxqM7cz++uC1Xfl+zm8TX+1gRM
BODVg/e5OpJT6OBQv/V0aVChRu9pMa7B7Zi44iYZh4jAK2s86f7d7amLQZT+PtCY
g+Q+8Vxf+XUDs1wciqcBZAZ9Jo4Qk/1cb1DBmxj7Vh54liv/nHUErohlUV6CVWOM
Jcb43KIuhkKooVG5e1/u/9SHRt4nE5WK9QQruL3OV0hzfopc5UAV57ocQBMHdgqT
ezq+ntFTFlez7Loed/zUqInzWhE3I7ID+pJX6YK5ti4E5uqOzBYA8bj/a3PTwE2G
2PteVZgcMK3764MB/dRgSPZ8HdpsYcG685aCzs3zEIYVi/Q5Zp4q3UBzRy3TY0mh
djvDk1RcCwkmKxzrQDEJVOcxz5GdMcuLt8WAB5pjK3LG3gIEbfd8h968U+D3+ufV
6KjRsh5cweupN51piLneBEg5TgjZzSMuYakrbezTRfySO9SFIj2JvLfWvuX8grEi
101qRGC8/O7/I4L45Sb8diZaPsNIl/3kuqjGMASYtnEFYcrurCGlC1UweIShOrtS
deHjmBBOq+YyAYybF2ez6AVPr/SDfwxcK+cQB1wmpdftyuLhY3uEQE53aPvxb9EW
RVGOKJv4fxqOgAt99XeXQvgfWWM/Kix/hI+zP5gOrzKW0i/T7wdJBQDBIOwqbauP
fepur9reL75ixWn7AR7iMaEZD6sCfEojPhozeFUZ6KZdGo1baG3bRW5IRq4g9rt8
YpujOEo4dFtflECQHAsoJ6xiCHs4XLgB9iLJd4eMzHuZDaVdPRp4JQT9fi8/st3C
RfDkyIdFb1aAxX/D8xBYkE1zwC4TR3ejTEVwpQUNz8GOW+npz/uTUkjKxyO+P4qX
NSJap6dmxb34lUOtE/OnuMFcy2IrvE5g+NzzqwCFGOEOpk+Ii6HVgmZDhMhzzYzF
eNArxRQP2YA+dnn10X4o3oB2gW47vZ+PF61r6DcUWlTCDaVDU5FvMEu5AOasuwpo
/JSkBafZ0xup8QQHdhIQhuL99Y+CkNDGqh6d24L93bSRFiYu1k/sRO+QdWrNtyZ8
MYOoeEsVP/MDdI1anKEOUn1snSaGc08yaSmHqttLI85KnGOJCNsNvJ/qB7DQXXAd
gUWHM12x/dbbBwwh5cc281352crClDTdm21Vor//Jd8sz3o9dGIRyyf/NiEvuK9A
Y4JJmEHKZ6/XFgBxmgKAXnik642D6zCX7phGRgcVTJX54NhiJ17DT7sw/VIN9lsY
GZoAWFjvu9wtolHAdhzh2OCFtRm8bs/SYyf2hUma9DL8Ejl1Qvtc0KHZxuKNXcqa
+srUOmSq+HrGMBL5SmVdwvRptytopEKPYvMZDS27IacnioEljjCHzQdqFu6zmwRu
5d3gmwY0zuubQPz5FXiuyQ0ombKR4G9MWsLsRwMiwMz5sDaNbSIaKRgLDFxBQmL5
qHlhHPTAZSD8r6BZTwHPsi+jfBH4lpgsdjHRYwk6ApX4lCdra/q5SaubBZkJnxpE
0TgOIxypGPWYPefHVwv2aiy3oHs21k19YpokEe3asKAcpmXFGSkf1Fzhac0ZalbR
cP8fapP8yJY8Ys/fZDHGKB4XL28JKfMUeb7+YWtAN+yoj3YsfdfsM5EL7oZHcb/H
JQhdvTLa5Iyi1IUdk/GUF+YYKuOMG50KClqAX2fm2X9Um30HTCENRuLlbT71youR
ei6dhxqHMbcBoscqFLVbVu5ESGVyjVYpMl6EjzCrkTgjH+OlCI3Zsu0y1JL+L2CN
0H5KQ2y7aMqbiq+122QrjICWNNWrA2qgB2x/NI/BiH5vGs5HDvKTDchafWQiDVJU
k4+CSSnxKs9AJ5VLStkLfEaxvtbBDt5KaLtmCE8yKKc6fGB4ji9CSSdWcfjCdd0K
i/DaW0xKcwwsknVaYbL6evqAk5wEZjacf7kudcYTKBuMdEmM7vKVluXwI671dDdL
BWFsXi2pTpFnppA90RBvNS7nDG0mKhXzTiqjEZx0uWT97yW2DtoalO6VlGLyC+wM
X5TlswenP+r79DxCmpzYkOGI9SGAG2gN0SWrlOwy54M+ZnNynntc39wz355IzhDG
O8DBoZVF69/RUgHVzJm65MMJjNEcv278QHTlyw4B1upAO4CMchGYfFDsQP0297wd
6Ip8ScpKNx04amwDcK6y9EOtrE3I3cW01RrlTt1tIW3bY3iTdjv5NStfZxAhZlpX
twb/BDabvjlDpfPVlRXB17iC7RfI1q9WdpV6Zam4aXjYlvpWREZ1WXuTpi1lxGxv
CMYbRfrgTT6OZRwNeiYl2pO61ODzwQTbVS5L0JE9NSr6Cx/lGQ1Y8wxbJ1AOFAzW
slLnMlkOFE2Qbfyz+6Yg33xD90m5LRnxBDd/zifczhV9+KlJ2u1GvaUAN9CVHrhw
8M/ukjGWwxsq1adPxlBK6OH/vAIhynbYio0lrVxi6xYHfnyjfhab4aFozE98X2hH
UFUFdY2qn8CT5say+QEyiA319gtZ6U1rqGpLD0KVNeIuaJXlZBst8sY/DzvdyflK
N+nGUROgrmuZZMIdkZTL1IHGTklDTRFtZdT4qPz0M3OxDw+DjPE6n3C8vxgWWH7A
v83ecUwyzNfWzfk1WYeQ6Lr5xcu5R7kl9fGM9oFOgQk9ZmQdRKLbZkwxpUhF1kdd
xP8wNf7UQR9OIeve7v6eapjauXzJnXhtcl78YdteFxI6dBXCQ79JemUmPNXFuQJE
lOZDtmjZAGQIHnzXTl8kAOuHRlx2mkBpRwNYGUTQZzdGGJAUnrwBotPfx6310aKb
QbjtsoSyfghUvzp8ULhbxo9FvZm+nwp2OunIiqtKtuyWh19qlKBCXjrsd0IHZ5dO
PELQsof5zWVoPgwqd2QkDUSflUnW2zWvl1FWmTJmVQuLOJoJ4V5SX0O3ZtDGBCLk
Kc1FtP1XzwL+pASF8MBh1mYoJsdAXuUxaEkrDZXqoqY7zx5/XiD/HW27gZk7hrfo
Z/fR1U8Ac4InIoa3FHR1wLro0NJsF6mqRxCr7vMe2bhjmD0KYqqDW2pVtzaYuC3f
Uje6Hv6rIWOjZ+Q1La2Lwx0RzmYafGZB8azGr+7B8eijXppVgn/s80+llMOiNV99
rkvilUvkZg3QCNNoCtuAb4/sfTN/pqXpcdW7Cte6kHPbxtzoGkR2P+Lu6lJdxrG0
as7bh0Rs7fMXCnl3ps44thAbZSje1ZNcuI4bQiYEgiF2wdPCcescz9xA8+Xz7t99
qa1t27+4JaC2w5maC49s6cd/hRi7AGCyy8dMhUfNz+xs8m0BrdKACkQm8i3u817v
nPFC8FcceXCgwVK9lgZMGLdcYcyW31ma2JXJXjTTrW0Z9324r1etODBR75UC2p5s
fHVB/KkHgCQnEiEYshhHmYpHjiTbTYfT6S9HkA2yugwbdFHpxFjLRaS2AVZ/mZPc
Yhu1E8OWnxu0YkntmZMx3TlyR17KGIziGFAzvA4vwD34n+9S7yNeso264eUDd59X
Cn0pGXHB13LsLt2EXxmb0gEZhZnWTdhkzzEXyvZjXeZDDeU4h7ilvJqWJ2CBpWtH
w/CDpK5lffK0VMX62Dce+3QefqFVifhmXQfYRxgJGSh/qGYeLLLdiOWrdeZrFrvD
```

C.1.8.1. S/MIME Signed-and-Encrypted over a Complex Message, No Header Protection, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

```

```
MIIPaQYJKoZIhvcNAQcCoIIPWjCCD1YCAQExDTALBglghkgBZQMEAgEwggWSBgkq
hkiG9w0BBwGgggWDBIIFf01JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6
IG11bHRpcGFydC9taXhlZDsgYm91bmRhcnk9IjM2MyINCg0KLS0zNjMNCk1JTUUt
VmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9hbHRlcm5hdGl2
ZTsgYm91bmRhcnk9ImYyNyINCg0KLS1mMjcNCkNvbnRlbnQtVHlwZTogdGV4dC9w
bGFpbjsgY2hhcnNldD0idXMtYXNjaWkiDQpNSU1FLVZlcnNpb246IDEuMA0KQ29u
dGVudC1UcmFuc2Zlci1FbmNvZGluZzogN2JpdA0KDQpUaGlzIGlzIHRoZQ0Kc21p
bWUtc2lnbmVkLWVuYy1jb21wbGV4DQptZXNzYWdlLg0KDQpUaGlzIGlzIGEgc2ln
bmVkLWFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQpl
bnZlbG9wZWREYXRhIGFyb3VuZCBzaWduZWREYXRhLiAgVGhlIHBheWxvYWQgaXMg
YQ0KbXVsdGlwYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBpbmxpbmUg
aW1hZ2UvcG5nDQphdHRhY2htZW50LiBJdCB1c2VzIG5vIEhlYWRlciBQcm90ZWN0
aW9uLg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQotLWYyNw0K
Q29udGVudC1UeXBlOiB0ZXh0L2h0bWw7IGNoYXJzZXQ9InVzLWFzY2lpIg0KTUlN
RS1WZXJzaW9uOiAxLjANCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQN
Cg0KPGh0bWw+PGhlYWQ+PHRpdGxlPjwvdGl0bGU+PC9oZWFkPjxib2R5Pg0KPHA+
VGhpcyBpcyB0aGUNCjxiPnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleDwvYj4NCm1l
c3NhZ2UuPC9wPg0KPHA+VGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMv
TUlNRSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQg
c2lnbmVkRGF0YS4gIFRoZSBwYXlsb2FkIGlzIGENCm11bHRpcGFydC9hbHRlcm5h
dGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5lIGltYWdlL3BuZw0KYXR0YWNobWVu
dC4gSXQgdXNlcyBubyBIZWFkZXIgUHJvdGVjdGlvbi48L3A+DQo8cD48dHQ+LS0g
PGJyLz5BbGljZTxici8+YWxpY2VAc21pbWUuZXhhbXBsZTwvdHQ+PC9wPjwvYm9k
eT48L2h0bWw+DQotLWYyNy0tDQoNCi0tMzYzDQpDb250ZW50LVR5cGU6IGltYWdl
L3BuZw0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogYmFzZTY0DQpDb250ZW50
LURpc3Bvc2l0aW9uOiBpbmxpbmUNCg0KaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FB
QUJRQUFBQVVDQVlBQUFDTmlSME5BQUFBY0VsRVFWUjQydVZUT3hiQQ0KTUFnUzcz
OW5PM1RwUncyMGRxcGJmQVJRRWpPeXdpd1luQ3RrREtuYmNMazY2c3FsVCt6dDlj
aWRrRSs2S3drWg0Kc2dyemZjcVZNcEwyam8wNDQ3Z1lEcGVBcmsrT25KSGtJaEFm
VFBSaWNpaEFmNVlKcnc3dmp2MFpXUldNL3VsaQ0KdmRQZjFRWjJrREQ5eHBwZDh3
QUFBQUJKUlU1RXJrSmdnZz09DQoNCi0tMzYzLS0NCqCCB6YwggPPMIICt6ADAgEC
AhMPLSW9ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMg
UlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIw
NTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnelN41KImVaTC3D
9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs
165ernT9O5NLFflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZu
TtMc1zy++MxQlqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCqlLqhBwDH
dZ5qDTII2PVX1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy
6SCf58duq/AOEksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/
BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VA
c21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMC
BSAwHQYDVR0OBBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEw
jnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCBSXignLEynBak
DKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9Ii6zyBZVjdao
x644DsiLOQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz53PYDBh4zE4Na
```

```
r2inC0D+VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eDOdu+F2MVtl
uLihne0Bp1GUTkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb744gqoeuD9YSHjKK
49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzlEc2tUpAr4vR
hZjVD6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpqp1zANBgkqhkiG
9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8G
A1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAg
Fw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVU
RjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTk
fCv4TfA/pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY63PQWl+DI
Ls7GxVwXurhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TC
NO12DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtws1q7
ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTM
SiPR+peCrhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90njlsJLOwID
AQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATAB
MB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYB
BQUHAwQwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDT
IGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0B
AQ0FAAOCAQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3Bj
JOd64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIj
So27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahiXRn/C9
cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgkLD59fk4P
GHnYxs1FhdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+u
CDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJcOvT4as6a
qdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkq
hkiG9w0BCQUxDxcNMjEwMjIwMTcwMzAyWjAvBgkqhkiG9w0BCQQxIgQgup+VC4mf
BVNHPJS0b9oKX/dVMKiR3JOz5AXfqv/YG0AwDQYJKoZIhvcNAQEBBQAEggEAJ2XX
xojAdRnBTCRahPos057TnArr1wju76pnJSWXK1flGWjEsSpHVro2t9LRKALqwTnX
YLM1PbrPoMyivqfhFik1h1dR9J2aXisS4FfZB3jj1c8XkD1yZb8qTBBRQ4v17MFS
1bEKW4ecopbd67f73QhUvk3NGJ8Aq8JPY8yxKGgGH9bucecSGYAHC1745wosTs81
aaY3k5UwyHNxRjFkkQAsnMe7HAiVnwsDLYCDOXACbg/DOwOCFK9vzDYkD5HjnqK2
wrhkTs1R4OZW+gWXPhFYClf3fMvrGZvr9rCwgjnwMvrpQjugZi5QGoi/sEdHO5T5
edT2/t+0u3oJtCflrQ==
```

C.1.8.2. S/MIME Signed-and-Encrypted over a Complex Message, No Header Protection, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="363"

--363
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="f27"

--f27
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex
message.
```

```
This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses no Header Protection.

--
Alice
alice@smime.example
--f27
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses no Header Protection.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--f27--

--363
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--363--
```

C.2. Signed-Only Messages

These messages are signed-only, using different schemes of Header Protection and different S/MIME structures. They use no HCP because the HCP is only relevant when a message is encrypted.

C.2.1. S/MIME Signed-Only signedData over a Simple Message, Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a text/plain message. It uses the Header Protection scheme from RFC 9788.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 4189 bytes
⇩ (unwraps to)
 └─ text/plain 232 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
Subject: smime-one-part-hp
Message-ID: <smime-one-part-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:06:02 -0500
User-Agent: Sample MUA Version 1.0

MIIMDwYJKoZIhvcNAQcCoIIMADCCC/wCAQExDTALBglghkgBZQMEAgEwggI4Bgkq
hkiG9w0BBwGgggIpBIICJU1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1vbmUtcGFydC1ocA0K
TWVzc2FnZS1JRDogPHNtaW1lLW9uZS1wYXJ0LWhwQGV4YW1wbGU+DQpGcm9tOiBB
bGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NClRvOiBCb2IgPGJvYkBzbWltZS5l
eGFtcGxlPg0KRGF0ZTogU2F0LCAyMCBGZWIgMjAyMSAxMDowNjowMiAtMDUwMA0K
VXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0KQ29udGVudC1UeXBl
OiB0ZXh0L3BsYWluOyBjaGFyc2V0PSJ1dGYtOCI7IGhwPSJjbGVhciINCg0KVGhp
cyBpcyB0aGUNCnNtaW1lLW9uZS1wYXJ0LWhwDQptZXNzYWdlLg0KDQpUaGlzIGlz
IGEgc2lnbmVkLW9ubHkgUy9NSU1FIG1lc3NhZ2UgdmlhIFBLQ1MjNyBzaWduZWRE
YXRhLiAgVGhlDQpwYXlsb2FkIGlzIGEgdGV4dC9wbGFpbiBtZXNzYWdlLiBJdCB1
c2VzIHRoZSBIZWFkZXIgUHJvdGVjdGlvbg0Kc2NoZW1lIGZyb20gUkZDIDk3ODgu
DQoNCi0tIA0KQWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUNCqCCB6YwggPPMIIC
t6ADAgECAhMPLSW9ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUxDTAL
BgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUg
TEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQx
OFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhM
QU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnelN41K
ImVaTC3D9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt
4jse2Dqs165ernT9O5NLFflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S
6DgCReZuTtMc1zy++MxQlqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCq
lLqhBwDHdZ5qDTII2PVX1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6
vL/PGeWy6SCf58duq/AOEksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYD
VR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYET
YWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8B
Af8EBAMCBSAwHQYDVR0OBBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQY
MBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCBSXig
nLEynBakDKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9Ii6z
yBZVjdaox644DsiLOQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz53PYD
Bh4zE4Nar2inC0D+VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eDOd
u+F2MVtluLihne0Bp1GUTkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb744gqoeu
D9YSHjKK49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzlEc2
tUpAr4vRhZjVD6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpqp1zAN
BgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVs
YWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9P
krYo0jTkfCv4TfA/pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY6
3PQWl+DILs7GxVwXurhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K
04s+A8TCNO12DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMay
CQtws1q7ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN783
6IPPdfTMSiPR+peCrhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90nj
lsJLOwIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgB
```

```
ZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAww
CgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyX
rilqkBDTIGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkq
hkiG9w0BAQ0FAAOCAQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ1
9naIs3BjJOd64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaV
WHg4eHIjSo27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHa
hiXRn/C9cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgk
LD59fk4PGHnYxs1FhdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFX
LJtBiN+uCDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTEN
MAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBs
ZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJc
OvT4as6aqdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEH
ATAcBgkqhkiG9w0BCQUxDxcNMjEwMjIwMTUwNjAyWjAvBgkqhkiG9w0BCQQxIgQg
K3lOLqVxzkFzTCjC4/0WD1uiOJZ/y8y2mKLDM5P/bj0wDQYJKoZIhvcNAQEBBQAE
ggEAiWwxPK/j2eujuwSbftm7fHd+LZyXyhUhfrZghxdPZyunkZmQ+N4ARXGv0zqr
yOgKhBdbd0pFO8sIfqRGvU2eQdvfFWTKz1Nt1UMGMUtTTA2Iua4+QcPdjX6At6k/
pp/OdEIuSLQHW89UkUfNEqYc8SjnhOaTMz7glWEM9jIXuWcmhtRqqsg+yYItvSbd
eXktWzBWuVCzvrsO4Q3oR4B0Aohdf+qCeTOwP5grdU4oIadD4eq1o+OEZfmliN2N
3dNYgd65gF0IXek3a1MMFh6AQF9aJz6451GqO1fwwwX2TtRnjXBY0ucY2Rn6h3PB
GEyYkGT7mRMuLMxmHktDjUBiIA==
```

C.2.1.1. S/MIME Signed-Only signedData over a Simple Message, Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-one-part-hp
Message-ID: <smime-one-part-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:06:02 -0500
User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8"; hp="clear"

This is the
smime-one-part-hp
message.

This is a signed-only S/MIME message via PKCS#7 signedData.  The
payload is a text/plain message. It uses the Header Protection
scheme from RFC 9788.

--
Alice
alice@smime.example
```

C.2.2. S/MIME Signed-Only multipart/signed over a Simple Message, Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a text/plain message. It uses the Header Protection scheme from RFC 9788.

It has the following structure:

```
└┬ multipart/signed 4434 bytes
 ├─ text/plain 249 bytes
 └─ application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
 protocol="application/pkcs7-signature"; boundary="54f";
 micalg="sha-256"
Subject: smime-multipart-hp
Message-ID: <smime-multipart-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:07:02 -0500
User-Agent: Sample MUA Version 1.0

--54f
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-multipart-hp
Message-ID: <smime-multipart-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:07:02 -0500
User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8"; hp="clear"

This is the
smime-multipart-hp
message.

This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed).  The payload is a text/plain
message. It uses the Header Protection scheme from RFC 9788.

--
Alice
alice@smime.example

--54f
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
dHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
acKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOa
Gdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXC
N5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
```

```
B2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj
8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4F
zkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8
A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQs
qm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
a4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3
SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgE
ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp
7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNTA3MDJa
MC8GCSqGSIb3DQEJBDEiBCAfybSsej+1D6r16hb18FcqV4ucPU0CgwMlVVH7gTaP
3TANBgkqhkiG9w0BAQEFAASCAQBwlRSGR8OZHFa+8cUc5th58+DiNkwKWqz4pWWX
0QP9uuxRZjE8Dtg7b88d0HtZWL98qAp+bjFK8ElktpuBiS5Nuiy+Zm3XnMU5GhCM
ywIPUAPJA6jvibT5fzYvMGV11RBmrTFNBZxxrJOAWfGfqf96vx9VajBVbyXdXnV7
hnQCx8wsbIOrbRUUVJHBGqpx+j+bIoUmg3uKxOYkZFz9IShmq8fzsW/CVTBMLfoT
qle2y+4H+RlGioqz8Mvs+XXbL5MG1r5PGjgpa9hHxPKdbFQCoWIJMA6xJNKgeuoN
rA3kHbrX/5Gn9eK8vE5eI6rpEurDGYkws6A9Z/tvsR7Gm9Ia

--54f--
```

C.2.3. S/MIME Signed-Only signedData over a Complex Message, Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from RFC 9788.

It has the following structure:

```
└─application/pkcs7-mime [smime.p7m] 5643 bytes
⇩ (unwraps to)
└┬─multipart/mixed 1568 bytes
 ├┬─multipart/alternative 932 bytes
 │├─text/plain 286 bytes
 │└─text/html 381 bytes
 └─image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
Subject: smime-one-part-complex-hp
Message-ID: <smime-one-part-complex-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:06:02 -0500
User-Agent: Sample MUA Version 1.0

```

```
MIIQQwYJKoZIhvcNAQcCoIIQNDCCEDACAQExDTALBglghkgBZQMEAgEwggZsBgkq
hkiG9w0BBwGgggZdBIIGWU1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1vbmUtcGFydC1jb21wbGV4LWhwDQpNZXNzYWdlLUlEOiA8c21pbWUtb25lLXBh
cnQtY29tcGxleC1ocEBleGFtcGxlPg0KRnJvbTogQWxpY2UgPGFsaWNlQHNtaW1l
LmV4YW1wbGU+DQpUbzogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4NCkRhdGU6IFNh
dCwgMjAgRmViIDIwMjEgMTI6MDY6MDIgLTA1MDANClVzZXItQWdlbnQ6IFNhbXBs
ZSBNVUEgVmVyc2lvbiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L21peGVk
OyBib3VuZGFyeT0iYWI4IjsgaHA9ImNsZWFyIg0KDQotLWFiOA0KTUlNRS1WZXJz
aW9uOiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L2FsdGVybmF0aXZlOyBi
b3VuZGFyeT0iMGY0Ig0KDQotLTBmNA0KQ29udGVudC1UeXBlOiB0ZXh0L3BsYWlu
OyBjaGFyc2V0PSJ1cy1hc2NpaSINCk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50
LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0DQoNClRoaXMgaXMgdGhlDQpzbWltZS1v
bmUtcGFydC1jb21wbGV4LWhwDQptZXNzYWdlLg0KDQpUaGlzIGlzIGEgc2lnbmVk
LW9ubHkgUy9NSU1FIG1lc3NhZ2UgdmlhIFBLQ1MjNyBzaWduZWREYXRhLiAgVGhl
DQpwYXlsb2FkIGlzIGEgbXVsdGlwYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0
aCBhbiBpbmxpbmUNCmltYWdlL3BuZyBhdHRhY2htZW50LiBJdCB1c2VzIHRoZSBI
ZWFkZXIgUHJvdGVjdGlvbiBzY2hlbWUgZnJvbQ0KUkZDIDk3ODguDQoNCi0tIA0K
QWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUNCi0tMGY0DQpDb250ZW50LVR5cGU6
IHRleHQvaHRtbDsgY2hhcnNldD0idXMtYXNjaWkiDQpNSU1FLVZlcnNpb246IDEu
MA0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogN2JpdA0KDQo8aHRtbD48aGVh
ZD48dGl0bGU+PC90aXRsZT48L2hlYWQ+PGJvZHk+DQo8cD5UaGlzIGlzIHRoZQ0K
PGI+c21pbWUtb25lLXBhcnQtY29tcGxleC1ocDwvYj4NCm1lc3NhZ2UuPC9wPg0K
PHA+VGhpcyBpcyBhIHNpZ25lZC1vbmx5IFMvTUlNRSBtZXNzYWdlIHZpYSBQS0NT
Izcgc2lnbmVkRGF0YS4gIFRoZQ0KcGF5bG9hZCBpcyBhIG11bHRpcGFydC9hbHRl
cm5hdGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5lDQppbWFnZS9wbmcgYXR0YWNo
bWVudC4gSXQgdXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20N
ClJGQyA5Nzg4LjwvcD4NCjxwPjx0dD4tLSA8YnIvPkFsaWNlPGJyLz5hbGljZUBz
bWltZS5leGFtcGxlPC90dD48L3A+PC9ib2R5PjwvaHRtbD4NCi0tMGY0LS0NCg0K
LS1hYjgNCkNvbnRlbnQtVHlwZTogaW1hZ2UvcG5nDQpDb250ZW50LVRyYW5zZmVy
LUVuY29kaW5nOiBiYXNlNjQNCkNvbnRlbnQtRGlzcG9zaXRpb246IGlubGluZQ0K
DQppVkJPUncwS0dnb0FBQUFOU1VoRVVnQUFBQlFBQUFBVUNBWUFBQUNOaVIwTkFB
QUFjRWxFUVZSNDJ1VlRPeGJBDQpNQWdTNzM5bk8zVHBSdzIwZHFwYmZBUlFFak95
d2l3WW5DdGtES25iY0xrNjZzcWxUK3p0OWNpZGtFKzZLd2taDQpzZ3J6ZmNxVk1w
TDJqbzA0NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2loQWY1WUpydzd2anYwWldS
V00vdWxpDQp2ZFBmMVFaMmtERDl4cHBkOHdBQUFBQkpSVTVFcmtKZ2dnPT0NCg0K
```

```
LS1hYjgtLQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQw
DQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMg
V0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3Zl
bGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gB
UCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXP
mrszyidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEF
XgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41ko
aZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX
+TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iP
sIVKarUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZI
AWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQM
MAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkV
fAEj8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJ
KoZIhvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtK
tl4FzkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3M
RsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0
LIZRzWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXw
fDz8A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu
OfQsqm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3
QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElF
VEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNB
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIw
OTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEX
MBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo
7sHUa4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+95
0MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYW
Tut3SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfC
n+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9
COgEykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIw
ADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21p
bWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAw
HQYDVR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwH
Fwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4K
kkOHG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30Uxf
yrZlRAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HV
X524bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP
0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+
JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSz
NnEmMYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1
dGhvcml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkq
hkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzA2
MDJaMC8GCSqGSIb3DQEJBDEiBCAXURNXz0Mn7lPPDM1oQHdl876V7RbyfNsR/srF
sVvmLDANBgkqhkiG9w0BAQEFAASCAQAjKgdecJe4TqYBPZ1hQzaeCGP+Y8kB5byd
wtkUDh91bAPCGiA7YzRjyWG/Yq4soSb/bRSpPRr3Jyzubwq5oBsnH9k1L2hVDinF
Yeot2E1Aga5OZTjfS8URVY4IEKKI9hNNUpdnqoehQqm54D4LFnJiujiVrS2COHSj
Z3Nr9SjeZ7ymKzThhsHaZTRJaloCxauGkf8EpeNJeoeNzae2PvcgomrO1aLW3M1o
Q3VqlsOfVsLElmS8hL0Mo08XXVs9KRWuBiuXR+fsXlODlVHwqWJVBR/5wOGLgfn9
bPh7G4quw8SDQNHb/qTjsWYfAfE1K2edTz5z1u0GPm9ElCiFUPsc
```

C.2.3.1. S/MIME Signed-Only signedData over a Complex Message, Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-one-part-complex-hp
Message-ID: <smime-one-part-complex-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:06:02 -0500
User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="ab8"; hp="clear"

--ab8
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="0f4"

--0f4
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-one-part-complex-hp
message.

This is a signed-only S/MIME message via PKCS#7 signedData.  The
payload is a multipart/alternative message with an inline
image/png attachment. It uses the Header Protection scheme from
RFC 9788.

--
Alice
alice@smime.example
--0f4
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-one-part-complex-hp</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 signedData.  The
payload is a multipart/alternative message with an inline
image/png attachment. It uses the Header Protection scheme from
RFC 9788.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--0f4--

--ab8
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--ab8--
```

C.2.4. S/MIME Signed-Only multipart/signed over a Complex Message, Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from RFC 9788.

It has the following structure:

```
└┬ multipart/signed 5518 bytes
 ├┬ multipart/mixed 1626 bytes
 │├┬ multipart/alternative 988 bytes
 ││├ text/plain 303 bytes
 ││└ text/html 401 bytes
 │└ image/png inline 232 bytes
 └ application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
 protocol="application/pkcs7-signature"; boundary="a64";
 micalg="sha-256"
Subject: smime-multipart-complex-hp
Message-ID: <smime-multipart-complex-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:07:02 -0500
User-Agent: Sample MUA Version 1.0

--a64
MIME-Version: 1.0
Subject: smime-multipart-complex-hp
Message-ID: <smime-multipart-complex-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:07:02 -0500
User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="550"; hp="clear"

--550
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="fcd"

--fcd
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-multipart-complex-hp
message.

This is a signed-only S/MIME message via PKCS#7 detached
```

```
signature (multipart/signed).  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788.

--
Alice
alice@smime.example
--fcd
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-multipart-complex-hp</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed).  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--fcd--

--550
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--550--

--a64
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
dHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
acKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOa
Gdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXC
N5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj
8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4F
zkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
```

```
zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8
A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQs
qm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
a4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3
SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgE
ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp
7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzA3MDJa
MC8GCSqGSIb3DQEJBDEiBCAHedgXF/1PPCnjTbv4CNkHl6SU0FJSW9ykndUZcVnS
czANBgkqhkiG9w0BAQEFAASCAQCYePlJ3K4FtJC/4snTsO8l+p0qEkpFh4swjQTG
WUhZHrdzb4kvHTCaoH5ShpVxZ4FOp1InabzulsB1P9m5xDvZveUMaCiC/qgSS+st
KdklsWANoTgTlAAGs9og6Wp5Nq/evf8XIYdQV0ZXavzASl/yylz2uHTpW1ETxTlZ
fkgSqb8X/zRaVGoai20aVbmsIJFrVPIlkpgh+r8tbJOm4791cCU/8lIdreynoUKq
Bsa2Y/uhoez/pldX/5A7Rv+JX2vdt71C2BZAk4166wvDhhlHf9pVCWXdKXSh99c6
Do1TzpnakOm4bKSzPMXTrz1p5GcfDzO94kbNImkcdr8yAdcB

--a64--
```

C.2.5. S/MIME Signed-Only signedData over a Complex Message, Legacy RFC 8551 Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the legacy RFC 8551 Header Protection (RFC8551HP) scheme.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 5696 bytes
⇩ (unwraps to)
 └─ message/rfc822 1660 bytes
  └─ multipart/mixed 1612 bytes
   ├─ multipart/alternative 974 bytes
   │  ├─ text/plain 296 bytes
   │  └─ text/html 394 bytes
   └─ image/png inline 232 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
Subject: smime-one-part-complex-rfc8551hp
Message-ID: <smime-one-part-complex-rfc8551hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:26:02 -0500
User-Agent: Sample MUA Version 1.0

MIIQaQYJKoZIhvcNAQcCoIIQWjCCEFYCAQExDTALBglghkgBZQMEAgEwggaSBgkq
hkiG9w0BBwGgggaDBIIGf01JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6
IG1lc3NhZ2UvcmZjODIyDQoNCk1JTUUtVmVyc2lvbjogMS4wCkNvbnRlbnQtVHlw
ZTogbXVsdGlwYXJ0L21peGVkOyBib3VuZGFyeT0iZmNjIgpTdWJqZWN0OiBzbWlt
ZS1vbmUtcGFydC1jb21wbGV4LXJmYzg1NTFocApNZXNzYWdlLUlEOiA8c21pbWUt
b25lLXBhcnQtY29tcGxleC1yZmM4NTUxaHBAZXhhbXBsZT4KRnJvbTogQWxpY2Ug
PGFsaWNlQHNtaW1lLmV4YW1wbGU+ClRvOiBCb2IgPGJvYkBzbWltZS5leGFtcGxl
PgpEYXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEyOjI2OjAyIC0wNTAwClVzZXItQWdl
bnQ6IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjAKCi0tZmNjCk1JTUUtVmVyc2lvbjog
MS4wCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L2FsdGVybmF0aXZlOyBib3VuZGFy
eT0iMGY4IgoKLS0wZjgKQ29udGVudC1UeXBlOiB0ZXh0L3BsYWluOyBjaGFyc2V0
PSJ1cy1hc2NpaSIKTUlNRS1WZXJzaW9uOiAxLjAKQ29udGVudC1UcmFuc2Zlci1F
bmNvZGluZzogN2JpdAoKVGhpcyBpcyB0aGUKc21pbWUtb25lLXBhcnQtY29tcGxx
eC1yZmM4NTUxaHAKbWVzc2FnZS4KClRoaXMgaXMgYSBzaWduZWQtb25seSBTL01J
TUUgbWVzc2FnZSB2aWEgUEtDUyM3IHNpZ25lZERhdGEuICBUaGUKcGF5bG9hZCBp
cyBhIG11bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5l
CmltYWdlL3BuZyBhdHRhY2htZW50LiBJdCB1c2VzIHRoZSBsZWdhY3kgUkZDIDg1
NTEgSGVhZGVyClByb3RlY3Rpb24gKFJGQzg1NTFIUCkgc2NoZW1lLgoKLS0gCkFs
aWNlCmFsaWNlQHNtaW1lLmV4YW1wbGUKLS0wZjgKQ29udGVudC1UeXBlOiB0ZXh0
L2h0bWw7IGNoYXJzZXQ9InVzLWFzY2lpIgpNSU1FLVZlcnNpb246IDEuMApDb250
ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0Cgo8aHRtbD48aGVhZD48dGl0bGU+
PC90aXRsZT48L2hlYWQ+PGJvZHk+CjxwPlRoaXMgaXMgdGhlCjxiPnNtaW1lLW9u
ZS1wYXJ0LWNvbXBsZXgtcmZjODU1MWhwPC9iPgptZXNzYWdlLjwvcD4KPHA+VGhp
cyBpcyBhIHNpZ25lZC1vbmx5IFMvTUlNRSBtZXNzYWdlIHZpYSBQS0NTIzcgc2ln
bmVkRGF0YS4gIFRoZQpwYXlsb2FkIGlzIGEgbXVsdGlwYXJ0L2FsdGVybmF0aXZl
IG1lc3NhZ2Ugd2l0aCBhbiBpbmxpbmUKaW1hZ2UvcG5nIGF0dGFjaG1lbnQuIEl0
IHVzZXMgdGhlIGxlZ2FjeSBSRkMgODU1MSBIZWFkZXIKUHJvdGVjdGlvbiAoUkZD
ODU1MUhQKSBzY2hlbWUuPC9wPgo8cD48bHQ+LS0gPGJyLz5BbGljZTxxici8+YWxp
Y2VAc21pbWUuZXhhbXBsZTwvdHQ+PC9wPjwvY2l9eT48L2h0bWw+Ci0tZmNjCkNvbnRlbnQtVHlwZTogaW1hZ2UvcG5nCkNvbnRlbnQtVHJhbnNmZXIt
RW5jb2Rpbmc6IGJhc2U2NApDb250ZW50LURpc3Bvc2l0aW9uOiBpbmxpbmUKCmlW
Qk9SdzBLR2dvQUFBQU5TVWhFVWdBQUFCUUFBQUFVQ0FZQUFBQ05pUjBOQUFBQWNF
bEVRVlI0MnVWVE94YkEKTUFnUzczOW5PM1RwUncyMGRxcGJmQVJRRWpPeXdpd1lu
Q3RrREtuYmNMazY2c3FsVCt6dDljaWRrRSs2S3drWgpzZ3J6ZmNxVk1wTDJqbzA0
NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2loQWY1WUpydzd2anYwWldSV00vdWxp
CnZkUGYxUVoya0REOXhwcGQ4d0FBQUFCSlJVNUVya0pnZ2c9PQoKLS1mY2MtLQqg
ggemMIIDzzCCAregAwIBAgITDy0lvRE5l0rOQlSHoe49NAaKtDANBgkqhkiG9w0B
AQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UE
AxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0x
OTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjER
MA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQJ+RpwpODxxzY
60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6
kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b9
7enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMs
```

```
wt41/0HJvmSwqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5
chWfNEbkN6hQury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/WI+whUpqtQIDAQAB
o4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4G
A1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUH
AwQwDgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3
DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0F
AAOCAQEAgUl4oJyxMpwWpAylOvK6NEbMl1gD5H14EC4Muxq1u0q2XgXOSBHI6DfX
/4LDsfx7fSIus8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U
8QzTjqB8+dz2AwYeMxODWq9opwtA/lTOkRg8uuivZfg/m5fFo/QshlHNaaTDVEXs
U4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpfB8PPwDR6chMZee
gSQAW++OIKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTSO7K459CyqbqG+sNOo
2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJc
OvT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UE
CxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNh
dGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MTha
MDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5B
bGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0
iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LCOwI2juwdRrjFBSXkk7
pWpjXwsA3A5GOtz0FpfgyC7OxsVcF7q4WHWZWleYXFKlQHJD73nQwXP968+A/3rB
X7PhO0DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZO63dKvIKp4cQV
tkWQHi6syTjGsgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/
2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGJWiQVC
CpDtc0NT6vdJ45bCSzsCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQ
MA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxl
MBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQU
u/bMsi0dBhIcl64papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpn
HGh29FkwDQYJKoZIhvcNAQENBQADggEBAHOJojanzqmgaSN3/gqSQ4cbbmdj/R40
BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1iffRTF/KtmVEDMR/sYeq
AH83KM5p3el2lVh4OHhyI0qNuz5oShNaACSioQ23WxHGVy9vsdVfnbhsplrWg9NQ
2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6mrYkKTM/RCGnumghxwYTo
j1OyD5Gs4D2IJCw+fX5ODxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDd6h
noQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk22OH4ConlB8f7R7s1LM2cSYxggIAMIIB
/AIBATBsMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYD
VQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhM3
QQV57XV/QqmiXDr0+GrOmqnXMAsGCWCGSAFlAwQCAaBpMBgGCSqGSIb3DQEJAzEL
BgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE3MjYwMlowLwYJKoZI
hvcNAQkEMSIEIJaCe/AYALXLZ8GDGBxF2yvHB9b3uwnKNIvWM0h3y2s3MA0GCSqG
SIb3DQEBAQUABIIBADrTK0kKM1vxG/qmdbFxdKDBjyUXGDaOWqjCmq81OfRF88aY
37JerJhyUUsUPVCd73rlsjskMrxsA53c6ojOcSqj5PM7ZDhXCnGdEg4CiKjOAn1l
C84LXG485qDGcJiQ0hMF/p/V2UguVdfVzPrCLPP2SCDP5BWfCLMII3k4sRVayUt4
FwlYLvsXcRUbTlLZBoJrYvfN6sNOAfcbNwAMTu0rx1A8ZAoNBTbhAbpn/UiTd6Av
YFcisTSEIuZ+oGRyvU3n/wBHp9bUonKVHuNYGYKgycuXowwVx3D3j6+h+XEBOFJE
KTaTKY4sz4qH+3UWjytqrEisWQW0JkuzVOa0dg4=
```

C.2.5.1. S/MIME Signed-Only signedData over a Complex Message, Legacy RFC 8551 Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: message/rfc822

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="fcc"
Subject: smime-one-part-complex-rfc8551hp
Message-ID: <smime-one-part-complex-rfc8551hp@example>
```

```
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:26:02 -0500
User-Agent: Sample MUA Version 1.0

--fcc
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="0f8"

--0f8
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-one-part-complex-rfc8551hp
message.

This is a signed-only S/MIME message via PKCS#7 signedData.  The
payload is a multipart/alternative message with an inline
image/png attachment. It uses the legacy RFC 8551 Header
Protection (RFC8551HP) scheme.

--
Alice
alice@smime.example
--0f8
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-one-part-complex-rfc8551hp</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 signedData.  The
payload is a multipart/alternative message with an inline
image/png attachment. It uses the legacy RFC 8551 Header
Protection (RFC8551HP) scheme.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--0f8--

--fcc
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--fcc--
```

C.2.6. S/MIME Signed-Only multipart/signed over a Complex Message, Legacy RFC 8551 Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a multipart/alternative message with an inline image/png attachment. It uses the legacy RFC 8551 Header Protection (RFC8551HP) scheme.

It has the following structure:

```
└─┬ multipart/signed 5624 bytes
  ├─┬ message/rfc822 1718 bytes
  │ └─┬ multipart/mixed 1670 bytes
  │   ├─┬ multipart/alternative 1030 bytes
  │   │ ├── text/plain 324 bytes
  │   │ └── text/html 422 bytes
  │   └── image/png inline 232 bytes
  └── application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
 protocol="application/pkcs7-signature"; boundary="740";
 micalg="sha-256"
Subject: smime-multipart-complex-rfc8551hp
Message-ID: <smime-multipart-complex-rfc8551hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:27:02 -0500
User-Agent: Sample MUA Version 1.0

--740
MIME-Version: 1.0
Content-Type: message/rfc822

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="cf8"
Subject: smime-multipart-complex-rfc8551hp
Message-ID: <smime-multipart-complex-rfc8551hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:27:02 -0500
User-Agent: Sample MUA Version 1.0

--cf8
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="e8a"

--e8a
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
```

```
This is the
smime-multipart-complex-rfc8551hp
message.

This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed).  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the legacy RFC 8551 Header Protection
(RFC8551HP) scheme.

--
Alice
alice@smime.example
--e8a
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-multipart-complex-rfc8551hp</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed).  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the legacy RFC 8551 Header Protection
(RFC8551HP) scheme.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--e8a--

--cf8
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--cf8--

--740
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
dHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
acKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOa
Gdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXC
N5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
```

```
arUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj
8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4F
zkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8
A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQs
qm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
a4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3
SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgE
ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp
7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzI3MDJa
MC8GCSqGSIb3DQEJBDEiBCA9qnCv8hrAl02HDXOOfVNCH7ucDtJ3vYdKv0vdCnWz
SDANBgkqhkiG9w0BAQEFAASCAQBp4hNammJHK5hpd7ha6lzKahf9hoZZS6TPNUCD
plGKSjV4XN7pLxDu3wXAuzon2zV0FxeA1MG6gZgdSBy/5nGivTc/NBOmXJtlNOUV
6b+IiQ1ZgJcWG6R2Pi0bE+NfadPhxvekgmCNTNl0jHQkXn+ABstolOZ+0QnY7TPe
6JoT6HHamKbV0L1/gkEEQtSvOkaDaZllA+if+Qkb6xus1QA3FGzScPpcryTvupsO
wNIlNwiRTT1Kvk7uMxJkWTvfZnWh2UOh7lJAkXbRfMwXwmnVnVooCFHWWpUBVPnn
URqYcZhz+4DJc9iim5CqXRZzIF6t6fioS8lCBalaWRy4AaEJ

--740--
```

C.3. Signed-and-Encrypted Messages

These messages are signed and encrypted. They use PKCS#7 signedData inside envelopedData, with different Header Protection schemes and different Header Confidentiality Policies.

C.3.1. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from RFC 9788 with the `hcp_baseline` Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 7825 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 4786 bytes
 ⇩(unwraps to)
  └─ text/plain 330 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:09:02 -0500
User-Agent: Sample MUA Version 1.0

MIIWjAYJKoZIhvcNAQcDoIIWfTCCFnkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAERACKkMFfCQBEXqsSFRAOfaa0UcrVI6fcuB
nsfnksstYg/+DabeHHBueVpIuTr5Zqtj8kQMK8hWRoA+yVhA85aZaRadcywsEn3O
oTc5vD6m9DBVOIpK2vhT+aYWJr67cfzlxJgVdRi6Pf+8g3c0oi05fMA17pPCUHYe
//VSeW3cdaMGgaqFamqL+pOi222Hp19p+3Q6zYRUJ5Y1cvD4aOKzaxw0RcWvFg//
KYuy1q6Fn0utZAhoEfnBtEp71fSI5LugUdj3tx3NDfrG1MLJHbBsELqawuWrcvmv
BbewMWR5BYcl1/DQgbGFSbB/yoqBPkpC54A7PP2MXfb97SEquY0wggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAL7PO1rb8J7CwZ+vEvIROxpiZ
on8lc1VRHaE2tthLu8WOekoAyQtPv11edZgydCRbXr++xY2CvOiaE3+jdWrn11am
khzFkHpfEna4o91BHoNoipvl4vuLp7B+s2Dxymwctv1sZYkcHjVC8Eh1SH/43JMY
0TJkBtkO1nLDWTVfVePC/ydbFaXqtgN69SiN03GjaczhHUTuZbKJX41SbGqk3XhH
iscSIrS/QIdK9arBEP7Vlr7WdvVdfAfPEYZvRRrogzZJ5TE95Aes78+kaQO5wJRq
xSCdSgw1M9jcHUrUtZ0kk/pGvs2aa3oNtkKj/7OMDi64SsWwEdiTVsHob5foyjCC
E14GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEGYCTS4JhiRx+ufWgp0alQiAghMw
GgBNjWrIh5GY9ElDx5GWJxbUaCM77I6Q/NAYPVQaM73L5yCBHNEekbAFMFmZF8k2
bYgLyBCp2PcL6BhSAQiFAvDUN8KYTKHYqaz0cwK2C9EgUi1dBtQ7VB+xPvTXZwSx
0sPOiv6keO2FYeIDEnT56jnD2b+JkW4/dwsgBVju3dtPsVR6bIRHICTrk0thCphg
0kUPnjefdDmQh0kCkp8XuN6M9ZTwamzR1gn4ZLXw5LArZ9h7P1yNKZvdoR6D+510
qo6IhBR1fmi+uF60m8blLN8TBJ9y8dt+UPQE3XD2d/r8YHvrItCJD1hse56J3WqG
AAU3dlks76PcxUzECQPmVgdzfWYmQ+ygCnxqIWanRbDsOY9DG0FoozWLbRG0yTsT
awwlH8si81FJPUyqiKRSdhufVMHIQT/rySSmfB2o6r6Z5p60x2sqY5csYemPrFq2
YWp5wCv/nLTkcAbvuCohR22XSlz9n0ihuTQbH3d2vDsUQzbX/7RrPNPOKYLPNZXu
O0XEklYC0IwMMJ4CUGtjgOMalOEpeePuURmXzQHg3704w4ESSiCnmVEVQCLEwgQu
8A1r9P97aQaVV4vvKEtLv2/RpRr5BXY28Kcer/2HQFUJ9nBpkJf+ItZBicO2cab5
o0JelZdoPL6aDwy4eDLVS+SMajO5bQLYMKaTYfcP+nUdYZ5gLU9qBcqRtIjQ5qdB
WH8XhEEiBPZYYHhvBidaK9EovTOJ4touEgOG0iaWoRa8crQgryKR/cnInZ1pWpfd
kmeJ0+NJSfstOLaHhk2x1fiq0KklryMAF9ORN2iZvtbOdr6zv2iR548O1XuN0Q52
ZmLQnWdqj2CSXvXi2kPHz+/1dn/iQl4oXAnDMbvm0QcJxvflFg1zQzRsTwvoyiRn
RBUdbsbGBziZGqg/vMaVnZF8yUl6ADxzqIf5rM/iV76g7sscLhX5Ewcj618QKOgq
n3nGxBd2xuEuX0pv9tS0mRi81qElRUboHV3/HhRnlTLs699fLFOAJMcke43a0jHF
NOECszVjwdXfn9JwlS6ZwWGqtDuCB4qPGjVttiPMn3iWIbWC6y5mtgaJBBAcGMaT
```

```
DXcojNrR3mUEwFmWFZKb/3cn2mzmB26JU9qbfyZrFxvXFPF0EYzqReHSkQLvwnqu
IqWm1ILBuIsLICSUrJw64e+k+qBgqg7lKhTywECC/0D1bjKntE7R7eeUn5IGs4Xd
dLdr0f/UkDhIqIAkn67CnIZi+miCszlk+l8uzIAIM6Vux3a7rXYVcJdSQg59tWFN
mmqdx9BT/bZok1Ijo2qG6JI2EIIjuvD8ufW9LYl2QCNuZ+Qn8S5b4gbRDKZGf9fG
vD2G96t0C8QpnUmVn4dI5B4plXYo77SrvMAY85GOtzha6HCJdIA+5SMxxIF/Qpba
TBinO2Z+4dxTJvbIJpQzZfMUQP4DCJxphpaALMiBxgVMM7FxPn4hpwUUAiu8juQP
GRh/PRKTB+ZjdzysiCYBPUlvd5BO/aM8uhu0CqOal9oA7bOXznd5PyJOBrkac94x
qXCwhwu72jYrt0YFmL9RbpXMZSh/fTGq68NY7j7NOMdlFS8P7Si1Tdfc7Q8fh4MW
w/ODenQPXTRKJ8NTYk7LntGM2NKrUS+e1kjaAwCk/F5fRieF6AkbVkP/vFDQYTui
oQM9LlGW85TIihO/WDWJYzRQCoigVVErwppjuwSDztFtQrtfCFbOVx4sAfbYoEt7
NTVg9V/elgTgAwrzowT9jMmZIDnkAzQ1Y46sD20BhjgxU1YwWSIhKyo7EP0xszPX
DTo9fY5ybayhkYQ59gQcb0mrwZ8q9C95FFxxpA0S9Yee5++j5+RCSosvYIHw5Piv
Rge1Wm1U3SG0BYQENLqYB+G39va0T5yy9lusVMiFnJ6CVGGNufLXNjpCXaNQLfRX
shYBUoUMwt0R9kpBDDg1tOwqHWoh0iG4X8Iy+cLvna2thFv8u94/Riq5pUn1sbC6
wxyu6y0vBdMLx0fm0fP8xyPnBCiG/5WeziARqdAaH8sGp3Q7qc/YApnlIQevCU2b
OlIz6t7dLve9HyYlvIv4pClPWi6AZg/un4Rtas2HuLAndrNV7s55sOFH4BvdGP58
3fR/M9ITOVjyiT3bUit+5qE7MvpUqdxfsdC3SUaPxFJ17khGiimV0gC+x+8YTicE
JebKrihVAosyVVWZpjCIa4hjdMpVgUutyEgVNov9XFoWcNxMb8f5IAgXvNKMsvpN
FMoAfeT1MSj3tM5jdWliV0P5tU8WtlFj3hxixZPaz+w2SykOrHoyoDjCWpXifZ3K
CVgGghueWgLglwuja0FSkvZbq1AiVy6ebtbkx/q5o/jh91oTa0SM2MupcHrHg3Z6
SB6ujw7BlBXWqcNlMMJQS6npXCWsleg8iHQRdTuDGabxuBJmVf6I2mg8Ev+Ki7C1
KAHfAAhHp1E13DXf+E8eHVEPIemv3YeY3ldBVI93+T5V823yYwqwk5PfWZ+fPo+7
lBoq8IuHDu0fpwh21b6iNKEODvokXOPwkixLB7KpMpl9niCkdVwtj8CJJzLD6CSR
ctVnGtFua77wOMEu1wvlXWuWz2IT9a3aKGyciLrgz/CsTmJKWSIoc/f+u6EnPf23
hYMpMxLI46I9VQVcxaX5YD20ywMxTmN2fkGQdoyxa5pAhN75+iBeYH9J0+B+bYHo
HJX9UiEs5Ja6vu37SVje6RqchkLrrXLyock/uTB0pCqsqJaZoFaVC8M1T+jTw8ro
+mioqKVi0JeH/Wn3yhCEHQ5AY5n5dB2OMdPe9BZQ9zzr/WdNx1/xs/FpRj+ggpql
1nEerBbzG9uJQOneKqRLYActvZ3zhe9X7Sl/jS9+pFLLtO2tnRNe/edOunZHrJVt
pb19s+WtaDVez/eRUbjkgdjlBFtfYtFtcldKJBjLO9KiIkLecj49cfZHr2pcXeZS
pnMu3vv1mjapHAbqIvnEnf/jGxGFIiWKP3jeKjgjv7580R3YpNQ62upOe2MP+HAw
3nhYYNrLxD1eFT/TTiFwOfVpvrVuL3vFfJBXVFWyaokM4/sLN4E2EfJ9kdgBVS2Y
RmgXH3/EBYjJzicoVcvb799rXkbfu5LymXGteMZ+XeTDeYkLrx490E4FYmnQFlQX
Grx2cqtzLPe4aVFekZndq0zDenNibLpv2PGL1cJy3mL/FEM85phjxe16wXM/aPcD
2ScKzC7eSfUj01K27nswJ0FogQQv4Q81apSQaVt3884uQfpz8j07NxR7ZfknpnwF
AR208udTix02yEQc0lYEI+vTo48DiI7bHVOXbA4lM7hSCaFyqAMuyb9JXyZGVvdc
v9+mxvNg6ObXhOkLwPxBVfQ+TraGKGvxMBI29/LzfgssSb6k8JoxiBy/qQnBcLZfs
bCqggRM2WDy0mApeyAHBwmybYS1l1nosIGHntnpaPgsRMIcMENNzEpVdWLZOcmwh
fEX++diQFQ9AwzW3zygnYAk/tZSXVe2wUL9ojMRr7kLwUz9n3OZLF3u/4UEra7bD
XRMtTO/UmuN/d16EqBN10gKY96buiRcgAAigMzj+D5VRqXzgj0I0Qq+gu/eXkzr0
tONfZfuoVNDl+q6H//f2kDRHbj0SXz9OSWHOtxaJ6SJbDX60MQFb6mEWJm8kno/e
UpEXjHzTU2xyum8qoN8XdaRBevrBhyPXFPb8QEVD1BXR6ehFockfbnaRqHVaStva
Df6/nos9E7ViCGW8R3YoJ+2qfWTk7RXjmq1ykrdbQxMycOXyRTbLB5ur0ynIif15
oQyz3SiQGSLOaSD1Z501Yty3zTEn8jMlpBOr9KXFkgbbxNY1X6nn3vZ5ZumAl1M/
iwtaPgThkj2RnM0ATEWG9SQva8FaH8zUv3fGepJ37VMPlQ43eWhZavwZi1/fs5vG
UYCyqxjhNXtwSnhEGHI2F4LaffYeim20Wt9HiXZON15vRpSeTWvTGOUGVZWROzx7
OgIeKe/ksjcIlJuzy9fKQlJjsmURWQfuKM2vfRFGAoM3jxKBNDDFzinkL2/kVpoz
rn8LpukkEOZNB++ALIGVOB8L4zNDluePDTYlojthvjJUN0+oU6OB/iYvcnHOKXin
PKmeDe7g5Ywjx0Uj0nuZEwa4L7ALCG2WpmnpMOT1RkHVpqn+29PPQ/Cx+JpGmXO+
uFiHQN+L3uk74rQwJ+LUQBGDrRE94GobEN/sWgk4l6bQrf7Sl3Af0QaXDCN9d2Nn
ebzYvxhxEkpqVnvjvd1Vr3ZT7ECzOFEA2hjK8L12oJz/zF8DXUhSlXxXAER3Nf5n
VzM+OfCpigIUezk5QN3r0sHD1mWEmOe6JgXnDu8BIbBN6NnxFXE+rbRV71vd0APE
q5F0T9a0o95/cVYBcLvhW3QQcp6yP1Xhulaq1zZc/N1482qDNddYDPtUDaa+g7/X
m1+3tK1myLIBhxv8ORgdyVQiXmHmvjWVk8qqSmwrNM7rZNkWo4FZFOYALreVHxHZ
T1bgmQ2Q/OydwRhfpWTlHK1AH4UzUTWKjFDH0j1pZGqtDuc+ghEboZxHdAI/xrvy
ypU3OnP5a9Dvdx4B2GuKHbPpN/yY+jbvjDbb1DX0NROcVqC7JU+mMXYFRkKg6yga
L2KDhI0VChXtzGUGSR7wnfvCPBWOpmi959NSoSRdVnVI6hrCqNopVPvRh9bAtdor
+MoGi2gxmKCLhxY0A9/6VjZnBF498RxRKSAh9EkHZp3Wtiy5T5779j8gHRLwIpeL
YnORqbfW0gcWhjKwL8BoXT95S7rvHWuJbwFXMmZFD7fVJqDl1auaeS8QNFPxEOIW
```

```
91Z+2yidE0MdkfTWWS3WTFy3N4DBYP6JJRIzHV9bYk18ASxvNR7sGjKTsaioRble
3WaKwI7eszBNvgEsrNtJP9PYD3leXc0XXbsZZmUgbu+Q0zIYfrmJwoOwA/4pOjtM
VpF0dAWOvwOMygwsljdOH8MFBBwVMsu95DiM5Qx7JTXNaPAkxKSVrvmPCPi1yH6s
82Tkf9D7MC91TyOV5g5wqR/aNXfHFk31+8tRi/jhDAGcyY+s1AUONPaNCImOjfe1
oRPRpw6noLVW+0X6JuZ+hFoIvOv5oY4mhvXmtm0rxG1/bI+5WFHRfqD3rQNX/RW0
WMepPlKnRq1yNCzwKNrdPf7sus1MHSDCYCuGFUUawRBZnPtd0wM7G4kPiVh6rm0W
EQji3yT1bDp61yVbw6TN0SAhcAzkDwrBNiGyDCDa5naYnnYRNE2j5KkAcFtZv32Q
KFVEAld8dP3+qeuGiNJVpiTNaQMtMT+Zm4IwgHHn7aHKW6su/jjc48gxLU+IHSR6
iW9IwZxRvCWkHLKmUutBN/WkNMgpt/Wmc3waY7LZiFhK+LCXHK1dLbyrkCdSD8DB
iYxV6+MFG9huPj1JtuonFt6DX/PE2S7pgLeTFWDwKxaeNSd6WGVU6KiEpeEgDPmJ
GpLAv1ow/G3Vmv0GhM/oxKd76uY61CosCHlEV6KqSX/c2YA1IVcxu6v8kaPXd2B9
mbafIPVDfEr8ZOD8SswA9jxaf3ZCmrYHhwyV9FSuQn8BNBpYqaa1++YOeOWPJ9tA
7qTDNUJNgc0vKa/nVWPuSVogfaVn5gw/byuNlPHmdLEdHUMyOcal4UyJ28nQrvYR
23WPQKmRT9OASsEMm2UZzB4+yf4/lzt3p2auEks2s3GMlfdyUm7PHu6tz/Kvpvy3
xE6G04qV/cEK9600jwfonvNgf+LV/06GV262QvbVj6eKnNVoE/7qws+QJNuwjqmE
xyOt/dRjTFLomTXFAKWpnXNTPNzUTyM4GG31We+aOkOzvjhC4dAL7lf4JKYqP6WW
wKxjK46KQuew81k08Wwk1VHW+D4DlN2ynIbDM+q8rkrlJNNvIHXw5BA5CSWpsxnu
oYR/fpw6kSbCPGO7b2tWVGmTw3S/Vwy96OLwunw4oYyaaBgenFFBgDzicgiyExtP
K0OPIr3LjEXyol31cLwSBjCNUMt7FwPiB5/TFQwVmtGq5t3uYL3ei5IgTaozbk7p
04bVa2QJQxK4bHHbsgZ8/Vd2JXJJdQ+I1rfC0F6PKFqrfhDeujsF8QzZhvn8M2qJ
y1NPENK9Q4zb77dYvDUXBss4+erFM0wPesScHEbQPh9yyu2zqskpYQMrOqMPCjb6
y7yKppG1pOIrMzpJQkt7WP6n68nhZAlkEoCu7XchopEq1TmlzFVJ0F48ijIXWHMJ
PjsMWj2eh6goyFaAl2tovcyHl14j8vY3JO9ACyLytyns+PzdrqjuZxJQt8wZMd84
axs1klGO2AEuAehpsf7ypMKCBO32kirOMQSYZc4QridRDU5J5TTxMsxz8vXtc748
8fDkhFFq5Bqf6Weo8YiFvspF/Vvow6xjGpcNK6DMgxwwvUb92bxHwhdlyVa90lho
B1fxiQkaA+Oiy4bdYXuDoLHd5p+T8SipMorXJrHe/blq0OwNaHrbGSCje2SXQBqB
+cMVUyvTtEsA+hpI6hIlAZutTZ7qrvIMGafd5CO078+8okboTHysqAIH8WAdDwkv
aXylZnqk5kEiwW3eNjoh0Q==
```

C.3.1.1. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_baseline, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIINkwYJKoZIhvcNAQcCoIINhDCCDYACAQExDTALBglghkgBZQMEAgEwggO8Bgkq
hkiG9w0BBwGgggOtBIIDqU1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LWJhc2VsaW5lDQpNZXNzYWdlLUlEOiA8c21pbWUtc2lnbmVkLWVuYy1ocC1iYXNl
bGluZUBleGFtcGxlPg0KRnJvbTogQWxpY2UgPGFsaWNlQHNtaW1lLmV4YW1wbGU+
DQpUbzogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4NCkRhdGU6IFNhdCwgMjAgRmVi
IDIwMjEgMTA6MDk6MDIgLTA1MDANClVzZXItQWdlbnQ6IFNhbXBsZSBNVUEgVmVy
c2lvbiAxLjANCkhQLU91dGVyOiBTdWJqZWN0OiBbLi4uXQ0KSFAtT3V0ZXI6IE1l
c3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtZW5jLWhwLWJhc2VsaW5lQGV4YW1wbGU+
DQpIUC1PdXRlcjogRnJvbTogQWxpY2UgPGFsaWNlQHNtaW1lLmV4YW1wbGU+DQpI
UC1PdXRlcjogVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpIUC1PdXRlcjog
RGF0ZTogU2F0LCAyMCBGZWIgMjAyMSAxMDowOTowMiAtMDUwMA0KSFAtT3V0ZXI6
IFVzZXItQWdlbnQ6IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjANCkNvbnRlbnQtVHlw
ZTogdGV4dC9wbGFpbjsgY2hhcnNldD0idXRmLTgiOyBocD0iY2lwaGVyIg0KDQpU
aGlzIGlzIHRoZQ0Kc21pbWUtc2lnbmVkLWVuYy1ocC1iYXNlbGluZQ0KbWVzc2Fn
ZS4NCg0KVGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBtZXNz
YWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVkRGF0
YS4gIFRoZSBwYXlsb2FkIGlzIGEgdGV4dC9wbGFpbg0KbWVzc2FnZS4gSXQgdXNl
```

```
cyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gUkZDIDk3ODggd2l0
aA0KdGhlIGBoY3BfYmFzZWxpbmVgIEhlYWRlciBDb25maWRlbnRpYWxpdHkgUG9s
aWN5Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQqgggemMIID
zzCCAregAwIBAgITDy0lvRE5l0rOQlSHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBV
MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2Ft
cGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAw
NjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8GA1UE
CxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQJ+RpwpODxxzY60n1lJ53
pTeNSiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+
IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8goz
R0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJ
vmSwqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWfNEbk
N6hQury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGs
MAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQX
MBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYD
VR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNV
HSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEA
gUl4oJyxMpwWpAylOvK6NEbMl1gD5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LDsfx7
fSIus8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8
+dz2AwYeMxODWq9opwtA/lTOkRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm
/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpfB8PPwDR6chMZeegSQAW++O
IKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTSO7K459CyqbqG+sNOo2kc1nTXl
85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJcOvT4as6a
qdcwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFN
UFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBB
dXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTAL
BgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBM
b3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0iehYOBY+
TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LCOwI2juwdRrjFBSXkk7pWpjXwsA
3A5GOtz0FpfgyC7OxsVcF7q4WHWZWleYXFKlQHJD73nQwXP968+A/3rBX7PhO0DB
bZnfitOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZO63dKvIKp4cQVtkWQHi6s
yTjGsgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKRu0BX
nDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGJWiQVCCpDtc0NT
6vdJ45bCSzsCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYK
YIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1Ud
JQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQUu/bMsi0d
BhIcl64papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29Fkw
DQYJKoZIhvcNAQENBQADggEBAHOJojanzqmgaSN3/gqSQ4cbbmdj/R40BEPr+gXT
+xiidfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1iffRTF/KtmVEDMR/sYeqAH83KM5p
3el2lVh4OHhyI0qNuz5oShNaACSioQ23WxHGVy9vsdVfnbhsplrWg9NQ2WbpCmK+
2oMh2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6mrYkKTM/RCGnumghxwYToj1OyD5Gs
4D2IJCw+fX5ODxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDd6hnoQ9rNeo
zIcBVyybQYjfrgg4DRvw9Ksk22OH4ConlB8f7R7s1LM2cSYxggIAMIIB/AIBATBs
MFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhT
YW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/
QqmiXDr0+GrOmqnXMAsGCWCGSAFlAwQCAaBpMBgGCSqGSIb3DQEJAzELBgkqhkiG
9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE1MDkwMlowLwYJKoZIhvcNAQkE
MSIEIPc7Pk9KNPXyMYThSPlPWV2Qm8CR4vwcxnqIoOjkdUtMMA0GCSqGSIb3DQEB
AQUABIIBAA4QYIyZPmQpKWNUhU2nJc7Fr1Oh66z992rzH2OTpxSHehRBo5dJYSqm
9p/EOWB0XLOuJ8s97cVbdYl1EqEjx9zvp1kdLtvosuonNGHmQlCPVKSFfpBvq4DV
L7YcZkAQgXujN2Z1F+MDlUTYo6reDa2K21zPqa6CJX75zersFb1xS3raFRaNAspW
URatTpJpgf2E7F39o78kRGsbUxurtzm5QTNHIVAqjv4LudNSGVOH++VTmkMR5gLJ
3Xm2E7tz/TLDlGDi+l67tYni3f+sMgyW39dA4/ImkVV3LCjT6TXuKRwvDnLdik1u
eh0Hs/LLI6jCJ82HDBCfgGfbJ8Lfqdk=
```

C.3.1.2. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-baseline
Message-ID: <smime-signed-enc-hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:09:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-hp-baseline@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 10:09:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8"; hp="cipher"

This is the
smime-signed-enc-hp-baseline
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from RFC 9788 with
the `hcp_baseline` Header Confidentiality Policy.

--
Alice
alice@smime.example
```

C.3.2. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from RFC 9788 with the `hcp_baseline` Header Confidentiality Policy with a "Legacy Display" element.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8085 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 4972 bytes
 ⇩(unwraps to)
  └─ text/plain 418 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-baseline-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:10:02 -0500
User-Agent: Sample MUA Version 1.0

MIIXTAYJKoZIhvcNAQcDoIIXPTCCFzkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAHafgwK5Dq1Mk+/BfVcTHIE/bWksOCdgOuo1
ppl3Qdi238REiGsONqPHaLjiK9xhjvTS4pSV3NHEbKTVZpQurzaUqIXL/sA12kkn
TQgbJiemZq2HXKI1feGM86z13FYWPe4g42nffZNi5kErmPI/IZX4CuJ2+6Wy8IoO
tZ3C1vLg6z4V9mialF6IyVDYw2VZUIb/r3I4SKINANa1t6wKHeHTX6TEJxOv3P6W
kWUwpPHGzYXPNVKX+NSLxGqX68vTYOhg86Q+FeKLNHkutnQD1fNU/ZBn/iidZt3u
aUbDpByaxv79j8QpvCHUXbygTIYENNc11+RcJ3WmkCKVkwXG2fswggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEARW1p7eiEdi69X6DKW+FXzEoc
E8KIzTvIpU++vNLVzq+29VTzdjvBVcg/8F8L4BNCIpWSgz5i7Z0o9LjMCw/mHo20
XL074me2zAv3HeGZ85i7gIiA/lsdgIb3f2Qw/+8gQVAIkoYOlBmpocBf6EGyEciU
SWfwp1qJE6/YWhiFbjcTIZYj6UqGy72AkiqGKgCZ/tFWhMJ2KKzbm8t5rG8oC8bD
dgjT2PYo5by8brJohF/zTS5CucfLqqWpA7QtHLHcAeU3NXqVc5tHyGZy89KDpEii
xVCxdE9Rs2AurTjT2/98WF5tTEFOR6LeEdG3svOzmMd0xWEdwP47BA/ePsS53jCC
FB4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEILWJEheEd6fWe0TTJf9JzOAghPw
6igc/NoE/Okf7HXkehS4/7Vs85BKRQ5mdxGN1WfY4nFcchHVWVUCrPXYC9mUC6hW
12YuNkD+i/LBUN0Yunvny5igqNHEUBzMQbJMpRxcgClqS8zMokqB0+kzkGJMK0nC
0DVfneVaPAldMvZhw3BsbJfGaeDVTthp8IuR4PgdCUEBL4QWCvkgDlNquACVYAD3
MD7PSziVb2tAvVBBpXOZ0kRGc3bQm+IhZWRAd65313297+eYKfmInlt+j/K57UBC
i3tnWaNei+ftFBPVpbnMqXm3TbBBKzuWtV8QsOKZFddCtgoZmjpeNPAYMUGtn79c
3eq6fTzQPaMKCY8Z3aEFEv7YfvcdCWrmsbtGndyoQAr0nc8BU7geuHD+MoVIVu07
F6x/hxZyJdEh1vfLP8hPKq9X11gwa8+qq1M92oBxT4hY96rMOMu2dBNvF3g9Tl6v
g1LE2PJs62m4O2XEYd05FlWzYzXjP4EzF3u171duDsdyrbwZBqOJvMXVffqEmfd7
YfiLMvfUihHpNBFsKtgPeSqjVZ7WN2M902CzFa85Z1CcCTrqtXTbVkzSUYBfixU5
mCkZimMFvH9iwNSxxqdovNq6OojFiVNUH4SCKBXDHhwBrHROUqZ7Jap3xQplYp0P
2q9owbJ9irL/2oX9QGRG/g2W9POQ2L7+S9l2QWWpn3hJZwZimG2LebRrIHEVsHhV
nQdEst7lZ8iDw2fDTd9cpSxUjV24LauODLxLHfO2NWnttdykv4RZhrhAYOOIE0H1
YuEhPD7m8rYvhr5Xi6pDEFVGpjkAE0Vk9CQkdmYxjF3nJhL9EBzozTWWkRsiNgyU
DJUkaikV/smnYcwU/0Y4Ug+AZdLhx9fCK5Crv2MjXaB/8btxoutyKUn3oO4ABVtQ
KFt3r/CkYJvyfZQTmlhDLDxry1L/yX78+pFmnsLRSKdNp+Wlhz3GeeI/bDZzR5L3
ETECwXcPjh9uqrgM3HUvKC9HHc+fUXKrQXqGMXRltvA1l7yW9ONOdBZbW+AaS52x
cSSr/z+jQJy6WSIXiPN/Lme8SyK8cSMUGRW44x08jZ17FRCMJwbmET6n/AxX4XFM
MBAJ/Cln9kM0cnC1Aw52X0571xKOS1MNQb5LRr/a6RnpVTTTJpplBQGjc8tjQfAl
bL5l0dPFKq2oOp90C3xjVa0Gvi3Qp8BBR9LKfwTUZSEsrcNhYm05+OiDfKMaD4nX
PJPd47XBR+MuYHRVu/7LYFv9KmhxDsemLmq+8W23AYuPXGoodQDB5upJSoVj2gjw
j/Aa6n7J8NIoNr0omfsavqZBiAiNSKRBnaQZ45h7hkYB40Oel3dMgJNATAE8/5d2
gXV6RkhCxtFQP0ykzbSdrlCVUSW35TtiCzGzEsVUQdJ6ZBy02a2mXIwWDt98Hf3x
Z1pHjfIXlFKG+h9f2S6lxkNZjIATawIwY1+yN246yvdfX4TugEtISyyeu8mGlnkk
md6BJL1fGCapQ8B2u/KFswjNQc9orJAs4PZAYwAMJqZl4jOPbcwjD4yVwxwdgu5W
uQZgUfHVQnig4jT35svTsNmMei//0WYrESkOLT+8I64TuBpP9Nt8kwFbfrJA3MAS
mmLKVZ2t/U5FfOu8hemprMntiAhNGBLuKwwbg2q8cQfZ1XNGyZv006s/9dVX2aTG
ExNCEsfprvsXrgHNT2gFGEbvlDJFEHCWlozu2GucDVo/AH5FAcwSMcyWtFvTkXHV
W2gGKYQd6Ap9flpy4B2PGQHdlinMADUxmaFRsD3fYbG2JkhOaSzAfJOwjXMMu1dF
AYyUmSj/hCCmosqR0QG7UJWQ4QK2S7dMFSnNt9zaPvKJMwPmAc8OTzaxrJxJ7l6H
```

```
DJ5HHAtZm52fGYRrUyXEWYSzIjqPkQFO9pwFhnlMNDLZ99D43VFUkoBeHHQ0Aswh
d+Xp+jGDwEMR62xQhIdRCuR8i7Wyl3+tCdzpfQSvMcfTPU2G3/xdvhDVJ3sDjcIf
7gLQG6/uQmevrL6XdUNW7zI4a09e/knL+trM/847NLjN0RRTABLkTxlTxgJ9ELcw
yx2gvuhvKSt414/1NcnbBZaW3yfA6l32X5t5jY9djW8M6EYLN5HSjy3aIJ8fiaZt
T9kKm5uSsz+7bb8TSc8uQ5lHzAvctgM2k56zGVQnzWkXR/ghaIJnp4ekLGlGZeWv
Wa5lKqMyvIM511VRL5UvuoAA2T99A0BiC0qWjuXpAjXHRDUMKfR1vSJMcxim228V
d6MfqcxJjEFsH1SLDA02jSafk2jAApBZe6Dwx42bw1/w3MOGJv+rPAI7tVyRBqD4
LqD4sgT7R1N4z1CPuxWdRTCmsSN8rqK11pzawJyOwElyimrqjP1GLFGuoG/s+VIH
gsRZGGeL1X9OeyfgFeFb8EAiQ8VCrCr5yzQNL8l+E7CJYCbqFH1HK3+aGqYhg2G1
kYEgcMGS2JVQTioPlohPB9ZVLPmcaCAzsPeZ1qAgkc4FAMHNh6Oad8/ELCtlp8Mf
+ttz3HVVZVkIHbqjag/LVgAGbi2WMvsb1WmtRCEAxzQwuuxvdQ3SrqiJ9QTP0DUR
hpyIzIP7G61EDnI2HPeq0G4L9LspOf/MUzTtYhnjkxRrsqUDVJ4UhWWVeL/rzEOI
/mfltQ+f2odEYOWLYHomhyd23SnWnq86P28wVgEhXBTNFeo+BkXnoenaJyLmjJi2
7HxOEXM6gcO0Y98wt9NQxaLvJ3DPtCQpJf4vQE2fsOblY4YLM5z/sEQSmNhxjRFr
RTO14S6ngOcH5iqdrw0+e9P7HXZahp5c6IuDOgG36DEM6NFxzy7mSDUsKRtStZKk
TQXe1W9LeUo4Vn/oHiR4cijQJ65j4k90FTgfBMKL58z0H82fZUcXZIHJnkMhvjmQ
m8LZLU7n46KC3sAzVJg+Uh374iwqsrNYXqr/IjYyheXLHxbFV76a7RbknTFx376z
Y84Q7NTD+HoydTWtFd7Wyajy8lfcJIddMi7tQtKvrrSZXGWQEhKTA4TmCgVCYRKs
Oo4RynbaFbX7Xb50No8CUtSsD+fVyIlq/fSlhs8cdpxzfQH2K75CdIQ2DAcPTVmh
o6MIBVAmDy8y1DAw8zJUPH5p8mSOvbvRX0y5Bs5dRM7PT9A+Nf67f+RF5xfJNSi4
Gwj6cU1hBN4Uxi8Yre/ze8DgaTb+5b5vt8pTiNpSvgqa0iY1o4TQjQVA+wZ9FZpF
ha48nC9hmpOIEAH3elODip2kuAXx1J8tUCJ6xvWHBfxhYjZZoZfkW5ANh7YRNDmV
cKjdpWyLak62aERncU35lxpg/OHM7fTlChFBl0PBPIownbpWSzuzPFKslu4Maf9h
PLO3jTcKPlw5Yp7JL4ChSqCLcF9KK7ava11UHj4oNgnphejl8ncFAWHvrB3CykN9
xD3IPjQmpH1woMkNspkFHklfq6jiFcuVBPPJ1AFawpKMwrf46MHOFQr85BE5JlXo
ez/pM19tItZyOsm6XUlITumIX0El1kiVr5WQaC4eC8FEd8KDJfD+sOq7RGaRoIQZ
D8vGB5QrdLbB2aNnKxwyTbK+P7p+F3Qy0BVidoGk1J16sEep2Sko7OoVdJCFd4bm
dUwBlvwXc006z821QkfmdLWpuIEIiqB19bEtxyEXyVnt0QG1OhrzJqjY0Q8cFhMs
exyW0aak/pOSPd7f81azE/UmX5U7b8slLwA54N7tqqjoMCLXyQqqaGNdgfU6S5Hd
DcIGHA7KT1tlr64HlzhQOA/iqCrv3/mOdJtx5voztQSqlZqlVs86ZhvW6BigqxyL
oqI52yFPMmkloR+QkPrwCl7EiSQSLRjv06KgdYDRjBqr2mgIOuZy0Urz0LDSSJv7
hdV+TYLwYxb4h/q6sxtQHu5vyzBshNBoF84PK7/xMMw3hASQLEpVZJCv0k/0pFuB
adCXSux6Op8nSYcMfyN8b1vIAPFP4b/s6uE+R9beTss6tWzZrk4rx77qjBOdApIA
PdbtndybZvktflfSq7ftwgiKERN8qT/FRQZVU9Z58MnVCTb3ep3MxTEoiVE47/sg
V5WZsly6Pm87XFCZxGCfZvyePGPU6iEPcbiO7zfhQk+tH/D7ccd4xD3kSVF5S+qX
V9DC5/eiKXDaWVOf+KyhJVuoNztErEvDfuPIqBr8gL85kpcqi4fvPrP4xziKK0HJ
X7hoc5psA27JO0FbvPPPwNCWBcQmjZswIqt/s4JwiKGApZEtv1zaL8qHieiLS5lF
CJGyeQvjdSm99fRGF+dOrypeMGoTPkBL5KjTF6ezt/H3b+BN2A760tphv8YHsa/
GhYwxmbjLnwCNL8bKrLzR211n8XPZcHcZTOKwvuT3/jImgTW47T8tBjP+uzsp6PX
a+I5HTxkw8hhLIN7sqfkzp+zupKlHjHG8AayROTkW8yFNViDZfxWI7shsjOHJApf
6NkaauzObUXYuxGdobMWaY/50ggA5CKS+SEXRXyrmLL0l7NAEWBCqIODK26zZPQk
TABDscOSDevdMXiAKcfUcIJCwZpjUQ42x9yJ0Byd5ood2+489nfz+GJC2yO9ZgZe
SWP1uUUs8maUPglQA8IVik6Jh7hijmoKu6ZMxM0Vg64bkiAMpNxFcZnYQSrlW4nY
6LsHstDs2z6+8oz/1ff68Ig1i8i1EzTXLRF5rKofQNMtBruuxD5O7tpeXDHj2EmA
mxkU5ubRf6Ab0QbAJ/FMB32VXpZnJHt8dIQZJ2HN3dq1H5I8PDwlD/kFuLE6xyYY
PMC3an5+q5VrrLzqaZ5w5uZAupJ+1dHmT2TxuySkUJuwfOHL20d2JVOHmtpJmuZ1
SEUU4EOIwDzS/NlqAVWElN4r5MPWotZ52pzvd2MiTMwrtNDE9wZd+WDOX9evTr6Y
pYOS7XW+NYEz/jABEWJb+Vw9gOL0DOkhwBjYdnUnD5io7LkQsRfvkCun1vHIWv7f
Mn7MdSgnmTu7+advjf0sv+SdHYOMPdCML/QbNQU7d1DP6gv8/WeDoGFvInNRidBg
Ftwm8CHrzXPIEP2/3GPxWh8SSlFyafBKwtpUWZV3pbO1+9UhlDBGX/ysIKFD1/Xd
iSt6B6ZZAResO7sxeSED/7ytHfEb9kAw16Z4d1XIyZ9y8QNRATI8IC2T9PHt2qVb
DDNR7JU+UH+XsPUvqolv0vDCkk6KfrRKiugEfgKZHPCOYQsVwhO+Nych47I7DxJe
AHJUdjh03KjBHalhbT2EZexcDPCMbiQOdQsVKyGSMFTbupZ4jGN2qMul/2nfB5Ed
/lEK3At02aFzSl2eIEeExS/kyL8yJB9g3MAae5hcH67tvQlYIpZvRtKHbaF5nOr6
CxznmHv2Iuui39a/FE+tpzeutxSg8gSmu7RuyYtILhNRJgKhYfBQFqJKJZzLSbgP
MZBPEEymba113dmAjow3trFz33Uy8nw1/bQvWLMMX9qoJM2FK/CFwTvNeW4+ixWB
IHovEIv2Z+0eSS0JcBXAfWaDTha0593PiJ0aMWPwHfa0smahNmBqQ/XYnKGSOtsd
/ijY0m0YoNyjwS36gRnl9BMJ8BXKraxlQiRjLM2zcuAXhl/wieahb8Nl2oPgooNc
```

```
Yn1rgcc3V3UaOjW6qjypkNJOaY9zQ1TNPf//DvlVi3Ut5niLMmroucYho9Cs81z3
IpKi/dvP7nEtfxuyQwTNHhJnDELPBuAQ3BBEptVYZufT6dtCIGeLZoLALShvEgrW
TI7HtACgdBI5+52yCJLhFg/GkgO8BtztAW3XJyfxOj7RH64ijCKpNzW+aBSMdPCx
bPvLjzQzVqTuCpr1VF+uY28NLfFxDcKFoVIVH746nt7flS4UUUP2h/6ISIe/NWSf
IiAL5Pd3zpdCzT2wOhrztHYzFgVM0m8LSATm7Lfvay9j8G92qnzD2kge0J1uApgw
SMJCy6wQ1EubvxtywxML4JZzkDZMwtfTmujaGLNZmlJ9wOW8ZR1et6Oy39326n34
Fv+Jx1ZaLC0Wy6Ap/0lYDeQ4ebCqhRJBLi2e54AeNfFntNmFtxvkL6/ZLvEi3fHC
iijh24iHVLQNKjACp+Ez8/rjWaqA1MEBXhAJsHt7pTKTL5KtfNOujP6Jd2REI5jD
UTmbwOzdEap3xT8pVBLWrJr9D4Me4vu+htyqxdNYtS7M7LP3AaWN+XNbtVszES80
u1gFNKCytavWx3lVTfuMCwT98e3qxhE5WLENxSsHYWUSoYCF0IureNIbmLeYxrCE
gKJ/vYEI5EGYWBXAYRs96Klx3zfmMCgBv7Fi+U+Z6zlh2nhJo4AF9G+DiifeRVTK
syESFZSFYDrrfIQR4M1Hig/yGxZIBSd73Q779Q5x1T3/u5pYwP2Sb0I/45csIWvS
zK1cdjVDwEOGnjlHP3E4z6Dvp58Er8zHkWPhH5bvEzyP5ga14huQ8UgrrVm66/N9
Ob/Rh3iwS4fk4dSQkqBxZ+W8QifsXkWVOjIhjbDjtmj1r/1azJJSvMkXf25ocTjT
3x1o1oRlCHuXa2yPYOHe8uzx6ikrBHmaIWtNORvUIXA5Bqfk6xsDwfswFtSgNUxp
pUVgQawrq5bwFOD6C9Ee756QXp9DGmW4PWi76u5qcnKYeG7JHUd+JLRjcxVvxh0g
mayCxEsRoCZiePnRjSUWTUiFd7SQ3C2/3hRpC7aeH4rEZJ00W9cFBgRzHsZhgjkK
IWEt5kgpX4C7HAhEHmk8NztZRoMXMLCEK/yAj6btTt7aRgPtjkISQ3ZDU66C4MUr
uj2B1Z1HBLVFZsk79z/yzHQarFYooGJUEsOmJ6VDjGj1Oh3kHR72BDLspScxUQe4
oOAsZzzqd5R1io5ABgZD5A==
```

C.3.2.1. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIOGwYJKoZIhvcNAQcCoIIODDCCDggCAQExDTALBglghkgBZQMEAgEwggREBgkq
hkiG9w0BBwGgggQ1BIIEMU1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LWJhc2VsaW5lLWxlZ2FjeQ0KTWVzc2FnZS1JRDogPHNtaW1lLXNpZ25lZC1lbmMt
aHAtYmFzZWxpbmUtbGVnYWN5QGV4YW1wbGU+DQpGcm9tOiBBbGljZSA8YWxpY2VA
c21pbWUuZXhhbXBsZT4NClRvOiBCb2IgPGJvYkBzbWltZS5leGFtcGxlPg0KRGF0
ZTogU2F0LCAyMCBGZWIgMjAyMSAxMDoxMDowMiAtMDUwMA0KVXNlci1BZ2VudDog
U2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0KSFAtT3V0ZXI6IFN1YmplY3Q6IFsuLi5d
DQpIUC1PdXRlcjoNCiBNZXNzYWdlLUlEOiA8c21pbWUtc2lnbmVkLWVuYy1ocC1i
YXNlbGluZS1sZWdhY3lAZXhhbXBsZT4NCkhQLU91dGVyOiBGcm9tOiBBbGljZSA8
YWxpY2VAc21pbWUuZXhhbXBsZT4NCkhQLU91dGVyOiBUbzogQm9iIDxib2JAc21p
bWUuZXhhbXBsZT4NCkhQLU91dGVyOiBEYXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEw
OjEwOjAyIC0wNTAwDQpIUC1PdXRlcjogVXNlci1BZ2VudDogU2FtcGxlIE1VQSBW
ZXJzaW9uIDEuMA0KQ29udGVudC1UeXBlOiB0ZXh0L3BsYWluOyBjaGFyc2V0PSJ1
dGYtOCI7DQogaHAtbGVnYWN5LWRpc3BsYXk9IjEiOyBocD0iY2lwaGVyIg0KDQpT
dWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhwLWJhc2VsaW5lLWxlZ2FjeQ0KDQpU
aGlzIGlzIHRoZQ0Kc21pbWUtc2lnbmVkLWVuYy1ocC1iYXNlbGluZS1sZWdhY3kN
Cm1lc3NhZ2UuDQoNClRoaXMgaXMgYSBzaWduZWQtYW5kLWVuY3J5cHRlZCBTL01J
TUUgbWVzc2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3BlZERhdGEgYXJvdW5kIHNp
Z25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhIHRleHQvcGxhaW4NCm1lc3NhZ2Uu
IEl0IHVzZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBmcm9tIFJGQyA5
Nzg4IHdpdGgNCnRoZSBgaGNwX2Jhc2VsaW5lYCBIZWFkZXIgQ29uZmlkZW50aWFs
aXR5IFBvbGljeSB3aXRoIGEgIkxlZ2FjeQ0KRGlzcGxheSIgZWxlbWVudC4NCg0K
LS0gDQpBbGljZQ0KYWxpY2VAc21pbWUuZXhhbXBsZQ0KoIIHpjCCA88wggK3oAMC
AQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
```

```
UyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgP
MjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBT
IFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpM
LcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrszyidmbuZmOpB5voVQfiLYYy3iOx7Y
OqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF
5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEH
AMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z
5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAAaOBrzCBrDAMBgNVHRMB
Af8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGlj
ZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQE
AwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj8OeOr83zdw8wHwYDVR0jBBgwFoAU
kTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCcsTKc
FqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4FzkgRyOg31/+Cw7H8e30iLrPIFlWN
1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMT
g1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7FOD7PfB5v94M5274XYx
W2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8A0enITGXnoEkAFvvjiCqh64P1hIe
Morj36pgL19oWZD6YrzSWHUz1F00juyuOfQsqm6hvrDTqNpHNZ015fOURza1SkCv
i9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqG
SIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEw
LwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5
MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJ
RVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2Uw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgWPk2af0+StijS
NOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHUa4xQUl5JO6VqY18LANwORjrc9BaX
4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4D
xMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3SryCqeHEFbZFkB4urMk4xrIJC3Cz
WruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog891
9MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgEykRiVokFQgqQ7XNDU+r3SeOWwks7
AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIB
MAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggr
BgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYDVR0OBBYEFLv2zLItHQYSHJeuKWqQ
ENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3
DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOHG25nY/0eNARD6/oF0/sYonX2doiz
cGMk53riugAocCn5zbzhW/JVdYn30UxfyrZlRAzEf7GHqgB/NyjOad3pdpVYeDh4
ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqGJdGf
8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+
Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI
364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCAfwCAQEwbDBVMQ0wCwYD
VQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExB
TVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69Phq
zpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwG
CSqGSIb3DQEJBTEPFw0yMTAyMjAxNTEwMDJaMC8GCSqGSIb3DQEJBDEiBCBARlG4
9zozFh95Jb3qN55AtQaDyR811KUu+Kt9v5+b9zANBgkqhkiG9w0BAQEFAASCAQAv
syHys6sl5UEThDVuQ8xBKoZOktYzIMuwy9TPtVJ0rX1vG4iXMBE+px8wWoyqlypv
KkM+bN307AfxMENsBsWfm9vEzPAC3WjgXl/6T5vhgxWb+Cb0Zn+uaYGkxa43vsS6
fUonAiKB2QTuG4LgHxD1lxsKOYvUx8DcNcS/I4y9Xw+rm74LTjyrGISWmq7qec+s
duAWjkLU5025Opkh86yjSI0L89x0XEqcKeKoxp4O7lxt3LZ6rHC3pr2zHhgGo3uc
xI/5nTWN98HT9N8w/jNkZSskHXbnCxNgLz/CFHXA41Qq0Wd7wrk9vdHammCjdc2U
4RtIRPzk8ehj5ko6LULT
```

C.3.2.2. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-baseline-legacy
Message-ID: <smime-signed-enc-hp-baseline-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:10:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-hp-baseline-legacy@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 10:10:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8";
 hp-legacy-display="1"; hp="cipher"

Subject: smime-signed-enc-hp-baseline-legacy

This is the
smime-signed-enc-hp-baseline-legacy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from RFC 9788 with
the `hcp_baseline` Header Confidentiality Policy with a "Legacy
Display" element.

--
Alice
alice@smime.example
```

C.3.3. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_shy

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from RFC 9788 with the hcp_shy Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 7760 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 4732 bytes
 ⇩(unwraps to)
  └─ text/plain 320 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-shy@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 15:12:02 +0000
User-Agent: Sample MUA Version 1.0

MIIWXAYJKoZIhvcNAQcDoIIWTTCCFkkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAC7eDC6qLlW6dni6TljfOJWAP5P9RzVjPRjs
gJJeEWxC4ddrf6UUR/HNSIEz0R+QFrbuzM45aZZdGpq8WEyRdhfho9R6hHdaDhbL
FWpH5K5KNWVaUbmZkzvhbXAS6/ac9p9prd+0D7lPZySQv7sL43jFS72bx1jTF7O4
Zfd+IoGg5mjroPVQBpP3K6oG/lOQydggNimBy5ISWRYtsHizfrFawjO7V6I8f7sa
eOf6jFB9t1SVbjNzuGSZ8R9hg3nVHjNsQ2x9YTHDzaJoMlvGwDFPOouo2MHEirAK
It62HCddq0tB6fGTUoxztrqPoNNTiZIN1Zb4eXp0JtpnXKMC5nQwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAWMK/5bj6qVYBipvgvm/QXOqT
7iH7R7z8RC0jlU/k/G2Vgcl+9Lk83z46Las0vnk7xgUJCwbFhw+hgd/rBZOuDJPt
Zhrx0G2rI0UaR8dH2YjitHPi12yNGWgxddaGAFD07GU5Sbi2Q/R1jDoVXuYRGIZW
EGoatToIrQLmfKMoF0d2EbSOI6ic+jHNUD0NSzstRdsoqIDKM0PWcb7ap+uNsi2h
eJemWXQ5xwQuMCDNxicYwCzV9TjfaiXZV2EaJjtgSB0YbTxSu3AlpYRIx+Ao1+58
TlK0bdv8EUqxb3ehR7B/yl5GoM7PtF1MbKF5m08JQCLUVULY41BLMEs6JTijijCC
Ey4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEFcKhjcQbc7Lfa9Sm6HsEHOAghMA
Xv//vkE9RSpsfziFKfS2N/SASzpEdcNE1ByKrDHpehYSwXT3s/V+JqxyfxW0dBgR
hrdQ/dw74DBv/Yk/q5auISAwC3ChtX0sgA5p2oMNOcDw1z+ZtniVHSYoDRRq5fnj
lYLZ8yNrziZW2XF6gVLnsCE7mIjuCzliUXpSr3PSlVLTXRgqeXvrzEijprArIh8P
SyoZ4Kd8js+N85yl1Lrh+EERevf184tTeRTjVdP4c6G2b5yPIwPqABM7B4EP5DLR
AWaqEXr4g7xWkiuZLYjJVdTfh0I6oiKVKVoP7X8hMiOE0M4Sx9UG6FGUz7mvuraR
az3wcYWNKhf80XoLZM64on9t2700RT16NOPMi7Ik8nM/Soo9lPm7RxHGN0bzNba3
eVgBV6iDn5bZgMxwocdY/A2b/kM0WReApCXNhcKJo3O1qORrCaTIfKAMDX6lyUI5
bpE+3Bj+S7WYEblQvXs3iAcDqEtA6zLy/A8eCJdgy86i8QS2PKRb81+3496ogtRQ
a3cNoxBQ1nzxSOjnzgvIPi9wTSysSVbtSAZJxeGoDUk3T/pyTki9ODL4GsINGTew
WDUuEHNulCYyj7RN6cDU/IV3ucww4WWvxos/npcQar994ycE+qCob3FEd5GUmQ5t
ESNOrYoHkKhqlc/eNJs4HmICbJnqk3YbXYsa3y0QHYrCAMvtXW4zuwng6nh9tM5f
YseP0Az9tik1y9PWdRUfp1pZBPwYIN+RnDRsj3JGIjPy5Eu+vPyELGzSSm4iMD9f
7LUwuSQAchF2ffKJZNiTmT/HKXB8MIRnowdBfhLIyNy+hv8JX7B78ixpsvsjTsFD
DsqCOIV01Zf+/M/h7+RmV4tozT52KvU8jr1jOIo1PCBvp7QSj0L9M0u/M+2gXd0B
4kB9zNLlByy9zlalHiIEuu1LVZ4zmwx19RtzCB0sgeAquCDBta3Qg1/pMhL9jQRw
wEQTBgoH5Ibs819g/R6LKy7hHvl4Ea/a+b+LVT8Lz9/dCjY6orXgu/8ePcoiAKmY
MFPXLoSHnH9LF81O4UB/Lejo3M4VUFtZzZFs/bVQK8pmzx9bbOMFoKlM5LsgE+RJ
W/oeLsJfF3iVWnvHMVgDTZ6S7OlhfL6ZJtnziwkq3Ub3MjhlhgiuaS1dzihWXv+m
k/U8mMu7t7033YW999w9R8G2jpxU5Sp2GzEuAzzqfEL7eKnbRQJD93dOrwUmY6RY
HzUGJbfm56J8+Uc4GpGmgRqnx96aodf/McUB/NCLD5DVJ3aPvktHrhyB3M2V4jq4
RT/xXUvq+FLqK0nR3XwQicLcc1YREa3jbrf5zHJmcITdQTuZmgPXL2UAPzbdzm/e
sRK6o7b3TQIhwgyEWOAVrf91aDuBiOcw9/IaLDUOwy9moQJHb8g5HH1+XVhYwqfJ
pV0LNGSSxSu7abtgmmD02QC9mTXxh99lcE+z7SJXYjkNevf/SRzIyUIwtxD/Se0M
2LYYArUntyOQmBVzUREV9wkZXCR5cRYS9az+nBjUEmLL0CBcPPl/ar8m/qzoWm9s
Jnn1NQOVP7F8EVoUXyPDchk820ZVJ/WcLpGPoPWQlCfKbGwKOftL8DQPFnZssBeQ
cNxihr1y2iDFGib8vt9vr10hR0XP0zMruXz2CukMILTV1je+UPV1uh41YVKJOsS4
tFyWCvQXxfUZtCELQlaPu00FVvpzLqOmzRTd6os/zCGCo8lJ5VXeuQdEo9lPMebu
FygtuUJBh4WchNieVjoAafg3+51+IY5Ft5qpHUFBQOWQwskA2Ly4KGVKu9XFrUS0
rAPLk3CkPYxKA0AJlwdoc5CI3jE3IWWQf2DTFyQQzDE4/omkFCB3j7uIQVRYXD3I
```

```
lncWsYa+0Ih7r6kLdEWWXBHSAZcMCAwBNK8+7JYtb3tQj0aUaOid6OTO2R0ozwuG
9OAKLcYfI6z/z8ETf4UNQ2UxgoXGEmR2puKx+3+R1BZiIdk8VHbOZQDcW6qNEHdN
5Aq841xFokdjg0AGt3WmUPXI4at4gxLMDYdqK+KTl+JuBBjqaR2ctC6Lpd3VC9jw
io+WNCfLvvbhw2MtFmsOvGjBDUxnNkyhmNochTMsVv2IkxqJofjaGJ3cjFmU3Qi4
ARyuB6tFgtw5pMqw72Hci63gv8pRrmlyEIL6iOXhHvaqc/xzlPPrb5z/o9X3iv3N
etY4PhNF3FKaTmeFGPwGd9czdUUvBphb/zph+xzzA8rE1ItCHwNyv7JlX3veIlUj
dyeKEDqSp1CIx9+HqYhZkCE9XiRfp5UgGJ2uFKgiP3gKHHn1eeLotKASZbaz02fw
M9k5xIom9wHVHnnnPvTzOCI7iswvP7am7moWkMwAzmxEUhVyWTSCvE7Pdnp+XbNA
wcMSf4AzEIlXMSuX0C876naz6LBZDdMQAaSRRjDab3YilCrVEMj4BMDmniPJ/r7I
IBiNCtOJjSCr0IpTL9ASJqsBf/HbvQo5LVieTwVZUGZrCViT6LbLmT8/tBV3Y8Vw
9Y9LbombG3TXMWEgtylKxYDvJ2zOBx1pspXnsGzB2QKxduinTDb6N3PBWR8Yb1ul
lcWEyzx16n9g9DqNOpi8cmVrd5f5bBMOD8CnPK4mWKkvpoQ0IXlNIDOQpjDZGgPl
eYQBlnT0jOqJG1Om4X/qv+1yzTltsYnjWzER/teKsjGXUvMHzNwx6iFdU0KQ/JjV
A419ox0SIwS0N2/1ZgAosqw/N3oDuPEgfFYKsoCMFjn/WCX8LBdd3CsznKhvfsRN
qgNHEVGzQoVT70qWhnNb5F/8tGuQZ3aX2PirqT/S8+e4sPdgtO0e4AZrmCC02wmw
kWytPNtflN4GCmZmPJcAIqirm7ohaTdUSLfDKb2qBL/8OUFQqyL7loJnYnIEguLa
/tNLfWUamgZOEts4ebaa559S6UbINlhwKDpuvuoh+XgloNRfxtLsszAmQJUfC2GM
dWnOeKWMaIntPz5YucKa7nUYQHxzU93Ot9d15WhoqnEi4Fqgo15gJJq9AmODHDXr
+SsBc7mpuE/sJBCIrn9XIvU3QxXniAXx8agQHwaKc4YYXu1EB+pium01HqXtqcCG
iE9NDZRYTb3l5an7cPnC+674y3A3X6EIvFJAQ7yabMIXG7IZc+gdk4CwkG+XoG9R
5zSOjFGt+x6FaWLOs0AbcZtX7htR6R4fnB5thsJ0u5UOOjvj3Ub7cSF4I2Gqf2ul
HA19GZ5cC49or6jABUxQBhexoaI+ywQOXVRYcQ2CGrZkjy1yC/EmHOw+sAmrn95f
wWDdz6izTOOVNsazPzKTSuLV6R+alEjiLqh6AgsYSqzCRTum8dRRflS6KxA6gKAA
6c+XVZje9A2szgblxHFcs/FC3hs7veBPSbgCeA5nSHTk2LjmExQX5n6qsavHqUba
gi01+X0792Ji/dPMNi1UOdN1PJ/LIHPioNcG7oBmF+AjVE64fe8G7Rxpum8JebfT
sv1Pgq/aUsLb2adv/GlYe7vbuLQOyeUJFgcNHCEWxffh+wejHXilxxxZr5wjIkee
2+yK7sHFJoY0VT+dFFdg2MU11hjz5VhE9vQRcwF142XKJqI842xdCvjiAexGDWC8
BIqhNJDL85nJT6RddqoAylblR2AqmebZ78E1LVsfUJ2MBUcWH260Ky1oWp7RUdwz
rKwxbHjoadueEom2DhdBsCl+AiaOW2S6iq7bBffqZTFdM3OXsXsdy6nNaWSviOoX
DgXLK0Kq4uh6SRDl7tKFPoa7rIb0B5n7r82vWKYAcd6FcHTQGU2f/lXXnQuoycDM
HssIDRpSxzMB56ecSBQrApjWS/NXUpAunJr0zW4FNWQiEd143VTFJEg7tgk2/0ln
PG6fzKOiuJdqyCLXhxOsfy/64JAXbAIexyp9B++ZUq6pMZFewPpkqRH17L8EJ2NJ
62jYABnH4S1uiyY5rfTeY+Sz6gwlD+fshZSWFla6D6wqKBT83I7gpvhbGgzctRpB
Uycd/IRV9NGOzF8RjpPtNOYUKV4C6/5cTMnT1NKOJ7qvYdEQRSRLCDVDpd7Zlptw
FjtH5QEXqDA8w/B1UzdVKhvefN5ZQ33bs43/4A42USlEMFsPlntMQa5gibVLVaMj
fZofDE/NoQUUjC8zpqoHXrPnLvnmZQoijSrv08/HEfBBo7NlTQXNmAdfVbVv7L/w
MJziZBEE9ux2rTilRpINcNbGlTTMkaTZMkv9EbiHHQwbujiDjyQ8/3/rgmsigjKc
UpcUX8vL/R6BcRjau9v52ISAMIRuOv2yeiyUT5PyjUdbSABZ4ApgHPjkIusTtGzE
KNut5dmX+YsLQofapHwh84xvr0xBGfFNTpnEHnj+sIYjEiHVxWXbeFPnk/Arshq7
UjOu57IQwtaBl8tO020l7HRxYO+PnjH1qLrvWSYVa4FX7BErCdzQsGDXoBeHdcmM
sLiri6xgXET27TkSculjVYQKMZ6fTXhf+MJUYWlWatAgoW6YegwnfCw5zZgLdSxs
f79eYUy7eePwko6a8jgFucRHrWCjmpCiCarLTbpIeMGMqlIBMl5D1gKKDVmmwmS+
gM4n2XZ4dyrqzJMJHaSGX23gXq1S82rx2B9O82uWKOTrHAgUhDd5qfp63rGZJ/KX
RwfPdjHy4ITGCPsi9sVo/Gt40+PhaH/F+156N6+YlmZ4NemtfxWRotBRla3BObLA
CTw2+T+Nus171wJu3q0nW2aSfHrf8laYCnkKUMqQ4Ju7Yf3c12B8a0EXYamiAvD1
EijcTPQe9VexCXX8zSzK+A20dSxtAr9QhRAAao9ewV0oDbsO7G9dBGqjnAph3OLy
0DY0a9ylz1DwJWeSAZvsQYJ4dCGJloBXHHB8VWjkdKe675lF7eDcvaN882M1jqpb
edoV2QrdqKjITiw+jSMKalldsvM1f/WaIZ7CB+aqOmupKUdK75NJ0GiUBRB7L3zT
Ja9ryWZ05VVTVypRWPsD4m1wLS64GT0ZpSPNWa8FHeKYif3lVPoA6CpDvcL5AtEx
WpwsE4+rSGqMFFvk2MtJswUFVoJYKMxEVHDqYUz9c3Xati/wDDpmUuSeZ+V5yujj
BmWTLKH5jX8gCyhHDWZpRWStMxxIo8KHtcR/q9yf6Fgp3OcN188Tx4hVqDFbDeJo
iEqy27D1SK6zBtSRLaFeZ+t5E9degiG24xufCyXwg5o/Zoh9+J3opef4Hr9qfBk8
GVsg169pNQsvqeAyI4pwlqvNLzl/B72TyRk/O/PibKICikUI/UrOkSKsyNBCj8Ns
N6PN0+KxNIsoCuHdPc7MKnMU4W5d5lRES3SmQI2wKBiq++VO2zz7G5Toi+69YuXE
eTWn3a6+7MxG2NDsxu/YaR2ghqm+a7PN++WtpyLSw2rsdHRlTrOQ6FZBBuuLrR7z
Ll7pEtN4k2p43DURAWr3jQL9/iRdqYaBXMxdL3HKMiD4XTvaNw7vXs/rR77skc7h
lFbOvFIk8FahdGHaXY2/uJUuI/RA9dKD7IizDtuVel9n8gsxfPE68Pm7y2ZT9fBe
FXeoN1SnRCXwKPaBc/C+cErJbSx6/FOaWpraenLxA6bdKnA0dznNotzxZj1J5eky
```

```
SVakMlhLBDCiIZhWQsbdNQPCLWv41XQ3uSdNWgOvWCkX6jxfr0+kq2fF3Ecy4x0o
SU4QTi60lYKIpZmwS7vhyovQmR6h04KUFeagDDMQ31qxT0j+D95XHPRmTLflEpJS
VdOwWXajTs8hOe7dtzfaIqgetdqSqoRIfx+WO7BEux9bD+KIznUWnHsuyaNwfnXE
Ve8+EcR3I9TlBzfpAdXeK8xnWJOIOBrCxN55xhuZGOExt//vaaWXPZb+KP0mvN+G
aXrg1u3wQaEW5v4wai1URgFhCilXa3K+AyfYxSaBYCmKVUafF4tPOUkYUVjLGqLP
TwPIS+PHnZtVtbEjT7vKEbVDz1s8c1mWEAaxVbfxAt5qfI3hTTKvW3y6CyaBWlXM
lwmOFZSx0Q0ss7JKkYlTweuUygsnH4C0tj7tDHNxLDVkyDQoZEi3cgU9tl9xXu3L
A6T0OC2i1Zp82p1CJy8sg42WDjw8af1Xf+KnyzbuZ2GKmCf/5Z8AGn8FBs04SG0P
damoK80/butLsVv2z6HNEdNzkJNkQTQsDfWc0EuLkQTQbHGwtekMr9aRLLEEFkmS
eW+/OJwYC2hcuM2BjNY0oxVR868E3UXgr1evQ5IPsMAr6BlvSi5tFJfOkUuE44Ty
nX/7qhBcsx4ieWZtGO87PRwjdTIFEynhISWn+S5iu27xBVHslSk+8LVHxT5zEQR2
H+J5/ZEwKNN6vV0TfcJXCvGEgdaZSCP9mnLvwpGQL17cROU58KPVpHF/uaFFSmWd
cwHhSD56dLJFog0Kc0phn6Vf6FFJ7lgDVJHj/2igEqEzxJjrnCtaGM32tX6yvytq
CQwIInshpVWWsajcninsn3yCzDuQdiRTW5FnHqEqAi8k9LFDoF06QIvCHxWrg7Zd
oJQBOTOwY6Cl1c77GnYyjg==
```

C.3.3.1. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_shy, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIINbAYJKoZIhvcNAQcCoIINXTCCDVkCAQExDTALBglghkgBZQMEAgEwggOVBgkq
hkiG9w0BBwGgggOGBIIDgk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LXNoeQ0KTWVzc2FnZS1JRDogPHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5QGV4YW1w
bGU+DQpGcm9tOiBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NClRvOiBCb2Ig
PGJvYkBzbWltZS5leGFtcGxlPg0KRGF0ZTogU2F0LCAyMCBGZWIgMjAyMSAxMDox
MjowMiAtMDUwMA0KVXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0K
SFAtT3V0ZXI6IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcjogTWVzc2FnZS1JRDog
PHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5QGV4YW1wbGU+DQpIUC1PdXRlcjogRnJv
bTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6IFRvOiBib2JAc21pbWUu
ZXhhbXBsZQ0KSFAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTU6MTI6
MDIgKzAwMDANCkhQLU91dGVyOiBVc2VyLUFnZW50OiBTVVBIFZlcnNp
b24gMS4wDQpDb250ZW50LVR5cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04
IjsgaHA9ImNpcGhlciINCg0KVGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMt
aHAtc2h5DQptZXNzYWdlLg0KDQpUaGlzIGlzIGEgc2lnbmVkLWFuZC1lbmNyeXB0
ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQplbnZlbG9wZWREYXRhIGFy
b3VuZCBzaWduZWREYXRhLiAgVGhlIHBheWxvYWQgaXMgYSB0ZXh0L3BsYWluDQpt
ZXNzYWdlLiBJdCB1c2VzIHRoZSBIZWFkZXIgUHJvdGVjdGlvbiBzY2hlbWUgZnJv
bSBSRkMgOTc4OCB3aXRoDQp0aGUgYGhjcF9zaHlgIEhlYWRlciBDb25maWRlbnRp
YWxpdHkgUG9saWN5Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxl
DQqgggemMIIDzzCCAregAwIBAgITDy0lvRE5l0rOQlSHoe49NAaKtDANBgkqhkiG
9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8G
A1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAg
Fw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVU
RjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQJ+RpwpOD
xxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+auzPKJ2Zu
5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afH
g4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvv
BZMswt41/0HJvmSwqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1L
Y4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/WI+whUpqtQID
```

```
AQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATAB
MB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYB
BQUHAwQwDgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546v
zfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0B
AQ0FAAOCAQEAgUl4oJyxMpwWpAylOvK6NEbMl1gD5H14EC4Muxq1u0q2XgXOSBHI
6DfX/4LDsfx7fSIus8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1
Ib3U8QzTjqB8+dz2AwYeMxODWq9opwtA/lTOkRg8uuivZfg/m5fFo/QshlHNaaTD
VEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpfB8PPwDR6ch
MZeegSQAW++OIKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTSO7K459CyqbqG+
sNOo2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9C
qaJcOvT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlm
aWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0
MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQD
Ew5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ALT0iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LCOwI2juwdRrjFBS
Xkk7pWpjXwsA3A5GOtz0FpfgyC7OxsVcF7q4WHWZWleYXFKlQHJD73nQwXP968+A
/3rBX7PhO0DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZO63dKvIKp
4cQVtkWQHi6syTjGsgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmj
V3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGJW
iQVCCpDtc0NT6vdJ45bCSzsCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1Ud
IAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFt
cGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4E
FgQUu/bMsi0dBhIcl64papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShl
NhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAHOJojanzqmgaSN3/gqSQ4cbbmdj
/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1iffRTF/KtmVEDMR/
sYeqAH83KM5p3el2lVh4OHhyI0qNuz5oShNaACSioQ23WxHGVy9vsdVfnbhsplrW
g9NQ2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6mrYkKTM/RCGnumghx
wYToj1OyD5Gs4D2IJCw+fX5ODxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJ
Dd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk22OH4ConlB8f7R7s1LM2cSYxggIA
MIIB/AIBATBsMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEw
LwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5
AhM3QQV57XV/QqmiXDr0+GrOmqnXMAsGCWCGSAFlAwQCAaBpMBgGCSqGSIb3DQEJ
AzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE1MTIwMlowLwYJ
KoZIhvcNAQkEMSIEIMFOxgjxvsd6O/C92x9Wv+OPyqNJRSBwoMdr0BlV5Y6iMA0G
CSqGSIb3DQEBAQUABIIBACBPs5toz4DA/xDj8t/B3f8YR7RhxqF+607P29Qd7lvc
c+PRfV9P+SEwlHgLtrvm242i5hDk0jWzwsZFTT9JfJa3fKMGM8ZpSnQQq8Q255PY
OO03qh5xOpUT8KEoKQduLQbEdtUAzndZgfSNbBNW1buT7kaWqhk5ExB4qm+fPyfI
+ZRng4B+PI8l9YpcuzybR10CylZLzJdB2EfHcXFDt91nA+iouUNCpN0ddLENJ6gZ
2338fhZ1xokMqSXo88sEjh9KBr//UMlxsWUJ5rM1DBGs4ysMfmuoz0rAnh5U95NZ
fTDI2hVSCHWx/92NDZXQlak7Te6MFWpluHV8QLwn/Xo=
```

C.3.3.2. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_shy, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-shy
Message-ID: <smime-signed-enc-hp-shy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:12:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-hp-shy@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 15:12:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8"; hp="cipher"

This is the
smime-signed-enc-hp-shy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from RFC 9788 with
the `hcp_shy` Header Confidentiality Policy.

--
Alice
alice@smime.example
```

C.3.4. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_shy (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from RFC 9788 with the `hcp_shy` Header Confidentiality Policy with a "Legacy Display" element.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8190 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 5050 bytes
 ⇩(unwraps to)
  └─ text/plain 506 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-shy-legacy@example>
From: alice@smime.example
```

```
To: bob@smime.example
Date: Sat, 20 Feb 2021 15:13:02 +0000
User-Agent: Sample MUA Version 1.0

MIIXnAYJKoZIhvcNAQcDoIIXjTCCF4kCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBACAU9OH5PSuN9tLWwz3pZCIjfuhDPvElwIWM
FLLaSLuRC5cnMqlxagX4RJaKeAhI+WZQzinX0SRGWosV1ixjq1RhgoLsdnQhXh1S
G3HHdlke+bhxqlyfAxOxozsKYybrkx+dHIhZkOtG9XrEfUC/4QCEAy6pQz1M15i8
NOOxXi7UaEHo7qwyW7NJ5wWe9QrDi8G3nazLEAWEro6kimhdSKiVvGi+7KCjLQpz
HM/BY/ydpgLZ3BiMOOALCK8BiZlMhy//jp6Z8638UmjKDiKA8ExU3EhHO24yBT3y
TVBCVx99bq1FwP1jnBBKg5VjeFpfA4JnUge5J66YIOR7DVeGglowggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAZ+OcEKyP/cfIy34M7u7ZUcdR
HK/hm2UHKlcSixxIDvVZADtdSzJ5qE6gzeRtCzVgIXEWPzuru6ADSFPUNdzV+R9E
G8pDkwzsZzxQ4QY37hkx6/bWDBcBBjF4/hVe4ubxGEvJ9QxixB2B34m0nCwxD6LY
EN2g88Pc9kSSRbduGq4LRfyrVQEG+WpKXzjHQSpzqiDXuMBDDW/+dMHaGKsR24oZ
Ne0Z0U/iOnU0J0VuuJbnPkgYUJXQvafZSJGIfhpocMMPD9Ll42XkMLIOJvDsGqVk
qkp2uEUJ3tzd4Nsg5UAWIrMNWQRdWbdqLcuMfoabNck1lOrJritHc65jAyjv5TCC
FG4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEIp1SKNdHDNw0Ia57jzQav6AghRA
SnD0DeMznPkqrErin0IkCd2tCYouj0vON90o6QkuEMX0SsEL/+9c6JQRVAVxcxip
a/FpEnBMRBGdfeujUTFp/AM89QL0TVc6jdjFRD5XbDsd4VSlk/HTDar0zv8YEZOu
FCHItlAoN04WgyDK2AO16XPAzZN+IZMmh7pWRWS7k4IgWfuo6tcd0Vo0TEtZHlDp
oJkxgSgg2bZwSXq3lb1sTDS1Cs/rG9h3GD6uBATdRKBD0+DRRX+Z/yPM96aFoX+0
+DqPvun7amo+2xeTgJgkchz2XK1sK8OG0vb6aMv3PwK3p0KDVCLNAzkaz0BOQvdX
UFng8/sNNu/P9+WBelewVfGDTdCocA6+9vQa6Gx1RzJz0js2Gt4MhH/MfsSbapjc
omaveE6baODAHMcbqH4r77QrgORmUfBNQC0AsnC5zdm1+w5ULOt9YkKUWWw4F9sB
0+2UeQpe0y+mtyQAtJvjTOcLEcAzRmV6Moaq+EThHfeSoyFJbIUqT7K8epNbhKws
QC1KdD118++t2+GxOjK4vuU0r3YFl2kHhDJIf5H/FJNR4YS+ZZ3S4IRky3HeSx0p
CmJE5x5wbXLvLf6+NTcF1yzYjASQvwqmPSAjHMYzD3t8SDrKO/cJGNdud84FaWfx
zf+0YyRulv7pPvmIK7Ul1Nh4T2We1ecFO7ON5qVLMeH5I+Zc/YwXRkyJGSgaAXHQ
cgh5BtOqQnsstX+nYofSceGgn/Vpop52pwWCf0/KnRi6C4Ih8o1naJOSEcU8Ucxh
D+ggOAvy/gLeag6G1DL4IzxqNHh7Qr9IZfk4doNyumkcOvMz7gSZGFxHoOPdH61S
/ndqe8D1C0zFj446GIpj8hfhVLf8+7eVGK5GPcfAiM/fSjfe6ZVqn5zX398YjHGB
H0HIyp/ZvWwNNMfdeJgG6ukdhqhx/NqK3/Dl0crpCbdGqqTHjl4UDfmMlUEt255N
Mp24Qd+rUeOtj+vGComumU23UueJz9/VDhQFfOPMnhLnqxNhC55R00CzXBla3fOZ
6t4OyRo0JCT9fkGfHFgQxmFLFtXkpHK3HBpP/tu9rFLl9nc8KToOguY6N+c5T9Rq
cpCyRj5yQIwkS5sLREYyNlnVQXBK8jESSqEOuJOp3pHUgNKMnWwfplkuBVK1pAtt
GUUFXZEz24T9urWaJHXFsikB33aks59HrNddwamv2wpgaDmt2e5zDZWKgTB3p89l
oIPbM5X0W2RsTAZwPgbjnQs4y7YZNT+CerPoocgI226Jyhxi6e7dYGrOmpavgYHB
ieale2z0tZdYOyNBS3FspCQWTXOUtte822OFuVu5xF4GOm/11zYRLt85SuAxTsNr
DwrBfLvuxwpx56GPgpoC42qyLbeuw19iTFS8kMXJxoSnfdJq59AwUqwdeFFxm8dj
TL8eCsyfyUoscvZLCD78mHMvB8IRzIQ/iCMESPfeAig5pZoeMMx2gVJFOZkEWqcW
OC7Icm+qKPX6tjSi+EnUASklDfrRhUQ+BdVYXdEhwf6UUG4HZ6OEa+MxpFUC2ulD
3kKddnMJZaDuvr3k23NhlBVhSOt7Uo6Soi/Sz1aow07d25JbLv5AVJJeE+cWPlSI
DQTAlPuYtx6oMVn5lTjLw3KaF/Y5i+RQbvJ/HeNfrstrelx7brLHiIHoCf1wZkgJ
EaQUTt/GZlnKv7xeKleBvJI1mCdy16NZrklHMnPUgj1ZxEwBJ17M23B3hAkYLF0O
EYtKUNushATxhMptM0sWQffDWROKD8c612WrbYo/zz+ApnNRUzEs20+cgvlTl4d9
N6/untoFR0mPe+0ZuZ3iCKmGdw+LNwR3jBeLd0YxYWlQrRBWja4O0ofswqddQ9Iu
99+ksCTch4n4BSDNQV0VLQ7dX9uWSgnno6fD3gpmIJxrNuAMfBavXqsP1Gtjl8uB
wBXn//OiMIOgHYvLMEj+A0Q3/D/6sB7Mki15spxF3KDI+6OiFQJkruTuOF+f/SaG
uGAYgEjANuOLCVu6aQZPf9lu5SV1MJJ3VjXzS2obkkk2lb6aNckXG8jZPzHwCoPJ
XDTwP8sM9VKbwMiv4wA/pxKjGEtJq4sslD2L5CaZBUakhIJtXSaTc93qkH3o7up4
qyChBX3sm2aJPvw8s5fktLauyBrUwVl8/naaCNJq5QXhcfbGxoBaoDaDAZ1auOxa
F802tArlDy3/c8KAcguiZhJTnPdtC//v8AyMYXbocblLoCblM8a2QTmif7LUcXZM
CMiLgynIMMtQA7gfKN9uvAR+Yibh358h6vupmu1dW0LsCb9KYtuNWEIL5CM2sw8P
```

```
1hGKrAxJrbQX3WWJIn1d+nv+ldqk3UOlwoKUTcxq4q7DYG9WjOev6LDGQyzAojrT
1Ob+fAR50Q5ssBnmN8xgw2zk/lVZH69Iaql8vG+zhNJRbSox5hRrovJWyA9XtlUG
9oVWLhg0aqd3FbTvlNth3S17zp2BLvAOfCctyoHHGCEzU/Bx5Sj55RvTlvl5KyUd
KPU2lVox7C+ueMwzG3zwYHFud9YhmI21l4KfjHfaYICjqNY9QX15kJa6oxJKGi68
meRATnQOm8l1fl+p2PVcmqB7Z1qkQwX7Fpjx2r3oJK0XO+s0du4rEvwlggqHbCaH
YZzGHJM0CfI1zIo/BEkG/JkMrZlAT4lo7KIykGGVoE342OVvohXWqH6DyI+4QOzm
CM/MYhcZwdeb2ucEeSlGheMzcksS+x/8h1uAhguFEf+y2+qcAuYCIUYuVPFn+T3O
ee2vdXag6JYUzaRGSxfL7cCATB5O8d24HfiwGiyH/mQzuhk9CnK3IAkbdAcrkrOd
zhbPrJzG5eqohCnarEwsE5cpfTrCveft+xqE/5nhM0zmgvXr6ZZ/i+Cc2e//FUw6
9jdtZsKMHqTZUx5oODaoBTAKXS81PW5pChQGNTCP9klM0nFspLEg7jsDnZm5EXHU
qOfDCPdSvDGg9UkmiYrGujFlOywYn1Q+ai6Z045ILD23Ha//+yHZAms2OA8NWcA/
UU+2kYwS5gYilvGDV7T1lvnfLiL6puNP3Uk0N1HTG/UWOQIBhYbtVfmGWnprz2SX
uWQfrvgkCisjHqTrJ8UzaQaX0iPEewQZzqVoMIolxsnu73MqncRwDTbQv5UWj8zU
UL6I33gCd5v+SLSUfAXzZq3YpiMNku+93VL8PnSh7d/fSD32N7/pBOewxANOR1Je
pV5xHCFTKoAvIg0fNJVgOvPmXTLU7RDrO/0ceGbIxDD6kEle8rFe3PQQYBZGjIHm
l+1Mf4XPHUu2IdQBlL9XJTAfGu7kYxNBfdvf0rx7vFjTwG4neNsgaG9XOTtRIWcq
9LODeZUsP/Nnc+M2GcxMjJGLk+c9pFtoXYvgKA77UlIC84FdcNUiAYx14CYStMti
Smi5MMf7luGRy8JDjmHgUfN3e93nCABa+76VYaXkCbp1svkGJsuBCi7xSBlE0xVu
Qi1hHs6a4yL8STkLyDYkBAsiBxWo4kKJOgd1JL/lfscCUZW/90jbOJBlF9NhWn+o
SCVG+e0JbdN8nbIVgVhd/I33bJMVOk+RyfYY04BU0BCGoV6r40CJtMFKq3SZIdnG
0GfXjGMxoty3mKYrOAGui1+JMxyzabqRQTxc/k/HyPHuNCr6UNGlL+UXyfWAZSSh
dI+mVcsZ7yGWUz/sxLT19NFmv4hq1e8sBtdTF/Ws8SmEVlSmBRhokNkk0+rbM6gP
pdCsz6rcv7d4mmhCx+A7kNlOA0KPenHr18coLApibfWmqliBwNQk+SR5ZYdLAAPc
Us7xikmqXd+AIPfIeigGck+7fTvKf/c6tSG3JMUbXlnYH+18swnrclF4/Jswv1wM
IZ4wCCYSwaAyX/CuIyUGah2OtPsOmg78hLQ0VCETt7Md1wld6NFWhiEGQt96wKL0
215fiLORCfeitnK2Rdjq4OGnGUpQ2P6aXYJEa6TJ0EMKMFKeaoIwB9fiCEhVJhUu
ejUAAh01aciU11MT0ZjyfvQZIbv5GyFsQOjsvYO47xOY08Tfg5ZVKn1Zq+xVe5qa
g3t1laLrcEtAhhgpugHX+bAiwoOeP0QAeRpoIA5wsvvkyy6ou6VaB6+a5Xp3fcQC
4gsr55CoYynF14/xD8obq+o6XzR0JQ7lkAOKYTnBRZirNnctTurdbbOHgYKyiE5a
+0HhGoa9JI3MpfIWKu/RKnOVSwJk93SJww4Xi36ifBJwHW/534W+62DrOnoss4wT
smdYByOOxrQ11yeBNb1yV5/ehfRdAY2dRhOgv9ZQtutFdLopZAai7MZkh63P8PSy
PvBVlpXrx1ZxCRuBeafxJfU+rWSS2x2Bep3rDKtdBLM/816NUvMprDeR75QiESZu
byynANxocATJEkPOh2uGQ1RMlBlFz8dFLgVIRQ7MloIEiEyzdkta2XDKZ67X0F6u
warivnsUCeT/h9SeIg3C3tpxgBpb9NppMY+UVb46HB7XpzjHQObDAwC3VEizrKVm
a/6SynuNH5n/zNU0/MSY5M3GQL4xSfXq8AEId5UhuPiFwmD+sQ+G4VVm7d2HbXbL
9D/NkDep0zvdqbnB1ygTnlnRf/Nl5uFsdu+/1iKOMP5guzqCj0bKh+52lQTBHPDO
nZVM6Xvr+hWZPEZ7auSUqgeBR3DBXiwvRL5sxNysL6wRu/TXVV1ZIew+EiJJ9uZa
f0f+vvd6CeF72Syt7ceE5vs0i7M7z7dHMxiBsskpgQbx/AtTxGQyMU3Ki4DtmmnJ
gYBnIR7n6Ywu33dIeivQwZVywdnwHo6/SujaAX0bEBcPAlQqczLouNtFB+OKbdQt
jG8wMLs8eV/cdGiniwDXtSTp4VZw8lQNIdiGtgWAt/k11zFfn7A/YF0QfC8e1k9s
oLhZTic6SY33HLDJX5/Iq2b3Iw6ijzH8kkgTRCdtoJx+EqRIiV6ybT040cRgVCKp
FSZyuTeJXKDGWFDpbhz/PD4Np+dzp0tVUWw0M8pFy3erWmKPqu5Q4lbwinZPwtUD
PpP8CBKRWXanaqy558CIyJKzhkgGXR2z6OrOXSQtVDbcbQtxixdjV9lGP2qP25t8
PCsHvbNGSvBlmIUWPFn4iQ9T7wnDMtxPDzBb0k6KXWi1IxxC97pfFwt7kVjGT7St
6amDshEfCqLLcwCN6Aa3lKfP58FewuEoHoG5xFaT1+lOW/U6n9F6T2+CUM/3YOxN
kq1oI9e2dCDvz9ND813U9YS8HGHqGQqjSQteWt49xRXqvMi7gurrNz6i2feOmCvI
GMIsnp2rCDyIfmadJam0ElyYnSHbL+PyjhMt8883j+N3m5IKUfA1wo3KbI2zWa2w
mP6rImkJ2WemM2Z5gIQWJ1DOKt3M9fUxwcoX8W8XEXiRVJgOTp00xn+fqXqItZDJ
qkdgt7h7bVnhQbV6fvOCSSwU1ta+bjVGFgHPE1C6+Z6UrHQwn3iM9ZE7A+ytZz2D
CikVVFZANawbp9M5mM7PVPEY69n3WQ3VqpB0rZbCYFgNB0IyUu2yg06sH2wrKYE4
pfMbmLOUyFTbfs8ChQiOVcmtZHux/wOL52MGFyBJkupHwhZ1bBSjZocuXx7pxe5L
5EFMWtj6IQvQtE6XB7Nm5xcKty9EW/eIkd1aUXXRnzRKOZb7eWnRnqe21iVwL3el
R26HfqfCDntOCSSkYdOmeOu/mD4oZoqT/PRcR5i9b6jQUtZyfmbFBG7ZdIuavn5a
orjJCN2i02T7v2zN0aYTnMX+3fue/Ekgdvw7EfuBp73JaySDVByciSQkzDyJnWEb
fw5dEF/Zxl7KhnMud0ZIOZkdaAWyF36jVUgj2znIA2cjVqd9P+CfH9YI6vXPefgE
rWUbg1ijrufE26Yd40Hj7hMVXdeIwDuhZe8AdSmovaqK06N0eBRiyCzznmmaO9ae
VVdLoHyY5l/95Pc4cOZoeFWJ83agzcOrtSHWgAkVsycW9xg+g/oHBu3VoA8rlcs8
Djv73l84caZKdwiQ9sHvsvBBMIT5Ozz9uts+STb4e/h3ElAAkddL7eFowqlVOGIN
```

```
X3zSdDv1sT4D82oAeMDxeCAxG18Bn03Vd8dt/zA8FxVluUuLmcBHVVgy6pPqdiit
buR6Saa08RusmygTIjzbc10ZUD/bLB7YlCWS6mWwriviXBg2ThitwQJL3vXfEWHF
mHiGR5uc8dVhU9CmzqwQiiFFA9WOE8wgOudV419m6RbmW3grmVC8xskOYK7EzX7s
Mhv6dvIIY6in5dYp6hEcQYOsdxekSlltHUVIaijO+z9zxORP4XA2tkyU0ndXuWkg
kivonLqcBXiaO7nICbpwLKDK/N1JE+nKZLUZg51OXig3obIe5C6oALyC5o56zw9q
5opiXEKZBhjcEBdzTfBeYRE60zfqbacTyDS9wBzHo/84wY7fhNQsR3Y8t8bZZJcA
STWQVzhjszD1i+WRnJJO9fc9htipj7I7Sec9nMvrWh+sCeF1/QY+rEqbhQWajyUi
NTnIwHeuYIqtP8xi0vxqmBFe/t/WPrd+r53YOlObp6lJWPk8bnxA+5v76gjHAIHt
utp3kvykjCbJizw0WFU6du/jgCXzaYFWK88smgM1xAJ9dXUkkMekx/kJwUr/5Dfd
eWMKT42eG/JxFMeauuRsOwMIxAuj+AJU3IHej9oYBZWuEMqid5ZvL05ZYO7IaDoO
O/pfhG0YQ1mE8mCwlvqggUYfgVnfxBpAi5yikLMkTKP1YmKqfdDC3PvpDrqlp9Pc
rSMAnsydjO3K3JGoFDvv4RxCuIhn65Lqz1s9YepmHNfFlAZxEPhC5MJlwIXAT3VV
imEMYLUHbb4HsqWX/KR/FuZO0zpHGZhPIdtiS6TdiRm4D9ywPfV7J36zDVFEP6mm
kE7FrgI4Wo5aizOFA4GZFXN6h9IlsFiV9izXUoMjFJwR6Kp/QF1ikD0Pf/aPiUqu
```

C.3.4.1. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_shy (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIOVAYJKoZIhvcNAQcCoIIORTCCDkECAQExDTALBglghkgBZQMEAgEwggR9Bgkq
hkiG9w0BBwGgggRuBIIEak1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LXNoeS1sZWdhY3kNCk1lc3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtZW5jLWhwLXNo
eS1sZWdhY3lAZXhhbXBsZT4NCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFt
cGxlPg0KVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIw
IEZlYiAyMDIxIDEwOjEzOjAyIC0wNTAwDQpVc2VyLUFnZW50OiBTYW1wbGUgTVVB
IFZlcnNpb24gMS4wDQpIUC1PdXRlcjogU3ViamVjdDogWy4uLl0NCkhQLU91dGVy
OiBNZXNzYWdlLUlEOiA8c21pbWUtc2lnbmVkLWVuYy1ocC1zaHktbGVnYWN5QGV4
YW1wbGU+DQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAt
T3V0ZXI6IFRvOiBib2JAc21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6IERhdGU6IFNh
dCwgMjAgRmViIDIwMjEgMTU6MTM6MDIgKzAwMDANCkhQLU91dGVyOiBVc2VyLUFn
ZW50OiBTYW1wbGUgTVVBIFZlcnNpb24gMS4wDQpDb250ZW50LVR5cGU6IHRleHQv
cGxhaW47IGNoYXJzZXQ9InV0Zi04IjsNCiBocC1sZWdhY3ktZGlzcGxheT0iMSI7
IGhwPSJjaXBoZXIiDQoNClN1YmplY3Q6IHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5
LWxlZ2FjeQ0KRnJvbTogQWxpY2UgPGFsaWNlQHNtaW1lLmV4YW1wbGU+DQpUbzog
Qm9iIDxib2JAc21pbWUuZXhhbXBsZT4NCkRhdGU6IFNhdCwgMjAgRmViIDIwMjEg
MTA6MTM6MDIgLTA1MDANCg0KVGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMt
aHAtc2h5LWxlZ2FjeQ0KbWVzc2FnZS4NCg0KVGhpcyBpcyBhIHNpZ25lZC1hbmQt
ZW5jcnlwdGVkIFMvTUlNRSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVk
RGF0YSBhcm91bmQgc2lnbmVkRGF0YS4gIFRoZSBwYXlsb2FkIGlzIGEgdGV4dC9w
bGFpbg0KbWVzc2FnZS4gSXQgdXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2No
ZW1lIGZyb20gUkZDIDk3ODggd2l0aA0KdGhlIGBoY3Bfc2h5YCBIZWFkZXIgQ29u
ZmlkZW50aWFsaXR5IFBvbGljeSB3aXRoIGEgIkxlZ2FjeQ0KRGlzcGxheSIgZWxl
bWVudC4NCg0KLS0gDQpBbGljZQ0KYWxpY2VAc21pbWUuZXhhbXBsZQ0KoIIHpjCC
A88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJKoZIhvcNAQENBQAw
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIw
MDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNV
BAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfkacKTg8cc2OtJ9ZSe
d6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrszyidmbuZmOpB5voVQ
```

```
fiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOaGdmnx4OG/e3p1fIK
M0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXCN5XL7wWTLMLeNf9B
yb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWzB2zNS2OF+XIVnzRG
5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAAaOBrzCB
rDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREE
FzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4G
A1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj8OeOr83zdw8wHwYD
VR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEB
AIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4FzkgRyOg31/+Cw7H8
e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMtjH2x9SG91PEM046g
fPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7FOD7PfB
5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8A0enITGXnoEkAFvv
jiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQsqm6hvrDTqNpHNZ01
5fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrO
mqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExB
TVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24g
QXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0w
CwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUGA1UEAxMOQWxpY2Ug
TG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgW
Pk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHUa4xQUl5JO6VqY18L
ANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtA
wW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3SryCqeHEFbZFkB4u
rMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQsaqpo1d3f9jSkbtA
V5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgEykRiVokFQgqQ7XND
U+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwG
CmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNV
HSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYDVR0OBBYEFLv2zLIt
HQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZ
MA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOHG25nY/0eNARD6/oF
0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZlRAzEf7GHqgB/NyjO
ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524bKZa1oPTUNlm6Qpi
vtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp7poIccGE6I9Tsg+R
rOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtzOKypyQ3eoZ6EPazX
qMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCAfwCAQEw
bDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11
f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZI
hvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNTEzMDJaMC8GCSqGSIb3DQEJ
BDEiBCCSH/VshGTecXJjFa7ucaLu5N5h+XWZDoRRFzjPTfPjqTANBgkqhkiG9w0B
AQEFAASCAQCmZj3YztDO1jbNLEaAm/3QumEiuQzGfQctHOakbQxvEdazDFQuz4XY
tnXnadpjedB8CrzjKdgP8A3ls1mzTSrobnZ4hEd9uhuMDgVRUXaEy+0rx+XCfBek
2fvCIwuVDT5dZ5k2X95CTtcAhBu4VcXo/WJEiPKAu1/p+iZtRiZeV4jZQBfquGT9
sVqKEXkhfyAjl8pynl3yOMoX3AEnPOuFhEDm5Sx383zfzF9jvoaK5wOne/PzZ559
tzHJBnv+nQN7UpC4O6LCCIyjzI+hoEV+GP0m0LpClvUcRaplG5vgwshhHJRyjeOt
veiRr2vhYuXwo3pR+NzQGx3eaqOnksSP
```

C.3.4.2. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_shy (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-shy-legacy
Message-ID: <smime-signed-enc-hp-shy-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:13:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-hp-shy-legacy@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 15:13:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8";
 hp-legacy-display="1"; hp="cipher"

Subject: smime-signed-enc-hp-shy-legacy
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:13:02 -0500

This is the
smime-signed-enc-hp-shy-legacy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from RFC 9788 with
the `hcp_shy` Header Confidentiality Policy with a "Legacy
Display" element.

--
Alice
alice@smime.example
```

C.3.5. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from RFC 9788 with the `hcp_baseline` Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8300 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 5136 bytes
 ⇩(unwraps to)
  └─ text/plain 336 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-baseline-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:15:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-baseline@example>
References: <smime-signed-enc-hp-baseline@example>

MIIX7AYJKoZIhvcNAQcDoIIX3TCCF9kCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBACsFMztj9S2Us6fsAlVzAPVWpbjptMkEGnAZ
b+17E/dDNLBf1K4WiN2WVycsvg58WSEIUfRBxZ6BHePpS3+4Tg4PlmzBV41gGZuO
4eXWbrkGAwBOsckyRgpDLTmRpnN4lczjVx4gSfkEOXeDTU5FCoed4i1jnIHdP1Uw
v7WWq/SnDrwVfBZZKya0RPn58V299JxTjDKL1VKsCK5NV+weQo16deS9d3deg48n
dv/C9Gme0jUoOUilZCngEytRsGhJSoummFm2sieZ+ypP1zl8uZUHfnJXPqPiK2Sn
Ji3nypkjx1BJXO8M3wsaifNGmk/Rj9mz8mXWkAL2RrhP7ViISsswggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAf7w9j/+bUK8AFDQHC69/A/xG
/IygoRihTfsSINKsaezVLHmVvJXqOiPDavHRvHLMQNE0lqLy5edKD9tndyLCkOTy
xa8kQWwzxfRJHBq++paJMNTgdSLWpSMVxxPO7FghXbJoHPRq5T1m4q6V0Hjixfeq
lvtnWcGTFhwDiW09beFZhZInMGJOmRcgqHjToye2RkN8Vna0ySczcoWl5yFqW61J
bW1bHVun8Rn8OyEtw6XDDbnUgiVB3MYa5daDcVUe09npf+04M3gPQrDe27SBbmFm
LD3KfuLs8Be4TBRVaNkiruULjidQ0akI4gEaSpAX3y+ALHPDFH4UbwQrr7wdizCC
FL4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEGKhwDGWZa/xZkxt86e1AK2AghSQ
hTHm2t4nNf1Tgo2kzG18BqDLWQNlUJVQdHShktmLMyXbJ3/qgZIm7wnh+lZecrR2
aJ8yXfgWs8Po3atCKApsxA6eqUJN72NsrLIKiLSASXbsQHbRCtr+uJcs3M4z607H
UHpLSej8FRWJ7iRY1d4wJM5K0TKS+VzbMgo6MzSnhlZKZtqOokDCVgfg7t0fZKEd
mD7fn4qCeMCw3nkorWSBHnTkxaPC2vjPAMaFbxuRgbdEtEOK1DEvn4k1q0ig961i
2b31Ne0VDTFyJLna+3a466wj4I9nnwaQsH/F3p5GAJl1tVBLQXi4VVYrDsn4Xiza
gJMNmNBD4wXm2jKq7oT8KFTWy9vt9noH2qBgXYBvEkT0GDVx3gC5wCZ1YzUzUVS8
X0fA4xsz3nb+YpP2ir6fXPOt7JvyRHV1LA9Gf18cQO9izQR4IebBu05xnn+XAp8/
p7aFpcIJgJtrgUeE96cvO59lGCNb4pIgYTYYZaHyb7xNwbTWqGVhC+DQgNB8xiUT
/jS6QmOvXUMjSWULEaAeMGlB2NdxBPW2tyZxBpAhlOwn1k0yPgxYBa0r0EVoK7o9
p1ah7SOY+GA2UExATAtmionaJdBdBTADN7Cc54tipN6+ILHaSBm1j3F3H/G4C1l6
qHatDbSeT1RucMmPW68GIeRAKeVgMgrttQAoTNWycyj+QYMKsZzRhmFirBsew37E
8s0crEx6GuQ0yXLCQCW+eNIfNqkGelzZmg9oNKSItFfOMbeWKRksu23vKzRzix7s
fBk7HwCWwjSmlbHxr9djjpF2wKLK34k73LJCE6TPktH69tzbQpI+2fPFeGJASyTi
V3h2tjw/pWP8I4BOScHYoJ0pDB2zsio2MPXUKghI3gaS2UEdJiyNEBclh8a4OffA
scxnVAIdKffJcDvuftlmEACd8lIOJSke9+fRNxvhKVk16rtxlovvnAlCL6HddrFD
NMFCbAVERIHYwXUuzj75cL99/X51exRFFMZP43s1thRvwVL0BDAhrm7VebtyXQHn
iKjdKeBLhQ+FovYjve1vMcDPn1iaWKctQqDIK1xzma/YbmOAalrdODv06lwkYWeF
y4G/ylLiPDsn0TisdFwslm8756750TEIXw+y9lLO60Jkm7Q35ldHPAa4I+mIc8w9
1MtqcU0Ly60nRHgdEJDJC5EO5YI2wGUPqrtnNxydU2+JEZ30o58ATJRWhJRW29JX
0QViBhwmbaDkGGhnEQzjngNDqBLSgSN0KeDIYKPoGAza1b/cjhDmckaUM1cdA3Ie
3AsaCNIizoTN4LS5H4TpkD3/ck98B8RiDbWODUigG5dLAMU+096Xw1CPp1BwYc6F
hAF2n94fh0cY/PiSycXJmOVBHVv5K4iP+d+eHpcQrm0utMfccej21Uy8VG6cKCGw
1Gv8YuAK7Sf7yLF8plNhEC4YWr8up8KFkaP26Vf3KvVWWQYI0uVqaTXECiqOA3Xo
BXN37nWnXe+tywkOUWZ2l8xpgirMTtBZjFSxlQV51bZY1D6Pl06qKHU34WijCCOZ
5d9bZ5j3dZmfhEhHUjGHUWxON+JD5sAExSi0/bYGC0DMLSz54PHp0q0S1yPx4XKj
9p45RWpfDTrpdB9iXDJm6qvDOHUZQP6uMjyEAu4nR3XXJlb2rv+qXhrx2S0fu8zV
7T+uu+ZKPVU3AuVw1/ciCRXuXYPUZB3jDEYHLJ8y7fzeic3hN0zq+Dm56BOp/0Bz
```

```
zX/fTa1hwaW0EICeeTTzoCMSKbak494WxpaE/ekoC3T1/RJ6xWhvjrCqBlKeY9km
EQ500ZghhZG9J1wLVuEDD//6cyaMoakTGqv8QlBbfx++GRdUE+4zqFkB6GyjgywQ
wbJGy1rpYdlRpPNJ2/3zS2K+DTzKiuDkVo9Rn++AfLs7blZukE41KTnIO7TTdL3E
MHRYv21JlCWmTsEPLjAbgAlNQNWK+EaIMEnuD62foRyajGvtXahPAqU61Yr1+DmC
fQMLGCph0kTGoI2IJLf1U3dtRvI0eujpkjM0yi4tWVW0NdKF7rV9rP78VnXvCmUw
urP9o4oCICaCkvYPhYpCan+P0JxaGcSNSrY99HHIDoDLk5/sCVyMEs+pXy/9DVDX
luiwZG1dUU4f+2YZ7I76LcNXhUfZScKH6dPxxxQw1ypQWVdLGSQIXResiyI8XmTy
1maF7MZJjUUfm2GhEExFLgjskwg7Tn+dV+KxDek1ucCGxfXQb4tod++ojyFzcpNn
mLRFBj1t6BQV8P2rkq0tbXzJ+uqETp5VgZHY0pMnQqNHu8+U8f+4BWWLZNE9j5du
MDij8uBAdZ8Cjzqlxnv8T2kn0KD+qoohmHzUQibGiVPM1heI5SuScE2wV9Kw5D9m
WApogFxjpPfBhMLtPVVUvFp0dGplSME+5D0b6JPnauwo5Kng+FnDVtpiDPh/C2Xh
3GSBPPebvP1MbOV7DVUxuAQYOeFH43YVACKgQskBH7bqZdrhI70d4R/4xB7kYA0H
D65yTXjKyviGkRuPyEZjjkblR/OpzBCEYh+sJ+OXZjKkOW1gxVsOnYUIjYjUe9qZ
YAavaev/JRFIo2ungs1bwgOfgpnHdghLUW4UAtZdk9bOZkoUY4aIp6Q6ycPX9jbX
zCurW4hjRwjdwaPcgrOROYYTiKrnZ18m1t+SFA7GfVsjDO6ivittdMQptTm0aNI1
I3eTlvfTs7Ol2C0/XEyBJOTswJXNcukDG24bZAyJ2lWyYbqjEfwca3n7jOTZWLGz
1oIJ3qrHRAw2urFXfsyGHKaEqp12QcIdS2Lu0PVDdUdYQ4JL0/BUPqoT/dq2W8mi
ZLmygU/xcPPAYngkyT02FlibbtBMuptz3SfEU3XVzxirHRGnoQXDxKQMpcvbPf/o
bM580RH+E+U6a3ETKi/yHUI0F/5iuFH5AdaWqGbWlAWEx/TNGExGVSRiYLaZpvhX
hw5hCnvqP/cti9fkYwK27EbrHsTSf3jdToTvddHZ0oxWIut+1Er+DKq48uDnF2Ar
vDJJmWQVBTuzxjAYtNn2HyByjSq8zuEZK6IepOhA5v1ltIRnrwpTaa2aFmeZec0H
OyKr087p4Qo6FOztEXd650rzYtYfbaU8HvHfMkW9CeMCBUwj8obBYFuOeLPki/lk
lEU8JQ4/ZgarISB67pRs/sRciMgen9UW3WJXfhlMx2Rk0GPGzsG69t9amb4Vx/WE
3KPSe5YS/hACUL+Hy9ods3ZGQt4yAR1Cx8NHlTE5fhDQL6zzDJOsTOamsXZJGstv
VH+nPsW3AQfAfD/FWyFKJFCG6VsVhh60+p82ZGqBQk1YLZs236QVRmiZUXPeui9+
0YRV1cvcvybx0AWwRCNajEA3fwAGoin5Lw4INIe+oJPN2rQaCD8wwKRzybKRIpSb
r9mHB74aUQjmMd4c/Hn7liLnPbWSOMavxjO0lbykQxjIFVYbC/yq7chADdPpMOAy
jlEKbMGpkUiGqtuU3Gf3r6I8M4yMRAHEKduNEZNRqprs+aHu9DcT5GN8GJ8QRHYx
CCYwAsW1GX+oLkfJliy+hNW2EYC80u/E5ZI7ZzsdIcSZbTEWMrPHTpVw6UJPZ1hF
xVUWYwENBlQNuZnAkR7P9U15ZWnEdheoXaj0O11x4ffgTvap167AOpflKBk3m4OW
N7h9hMX+96FWSg1ee0xuOF4ENYLaWJ7RwJwLvWfc2tos8/Xf9/mEWqsJ2whjf81o
rpi1ze0fQgQmiTFnNe56ghXZcToOiov+GGZAQOEdfFWv2HyvBpfx9hZykW+x81XZ
TJN8LvInqRL/Gr4R1eXmEhNEbvH1PAGAZ2wa3t/ZNEPsGvq7vvGW+rE9dudc1o7P
YooLVpV8g2IeEkFFO9+DjrTg97j2FnJbInOSQGR4Iv0HQOpJ1fMkWOJHQjTjbiNr
VcmrNYlo5yD7F5nQDZJgtJXctXoMNDdjFufOTa0yzrLCOZjrO1SRssFVMPgpm0Xg
Ae/I96d2PxAJA1wZBJWV5xQCekqIHnB2Jud7TxH2Vc4AsEEFbxkBFWGR/kHycX8X
ZMtDpPH/qPaJsh975a12WHQY1cQpHDCl2jadQi5u//6VIg0zxMS1wHB3TU7Mt/FQ
YooIMIjW6n5Lekoi8u8IKQ+sqy78m+DVoL4XRZr9leQpvSukCWPeQEbIOTitYNrb
wTmakYir1Dt+vuzLDQBzF7pBNSxdZh3jKUZ/YYsW8/g/D4niekNP1sHSSYOcI6oi
wh+sSWm746AYtg+dBERBcTjQKhK45zcjUDPkC7tu6HuanP4HvI2fZMXDySUYvISH
GdyPtR29w+XX3n1Hy+TX1NsmyP3WNv6lqdClSWwxXTwyOJwvlk9OEkmGmd6APJpP
0xeTXUozActjge4OxvGa06uuLdXIfDwcuX4yxpj+HEWsHkbOkHcxxaY+byFOr3SU
Jbo56UbDHQS+OGpELp7HeJL5MVvcU9N0OSGfKTFFKOjyCOj2rdeYsf5Hidb/9078
z5C9L5x23ChCvd2ipkOEwcvWYkNwRJW0T193cur5qBGisZQfDbw6xNS2PCI3zp9Y
2lEpegrtxi4pDWA030EWzHCw7kcbtlWdzIW2/iaMOW7S0hHjcRboPgSzuFpDwEFS
M9k33iqH3vqfdrs1SfMXgumEzKAOnslMEzNHPJzCO7UaVlJOBgqTdNbAHqXSAfdZ
UN7z5+xnmdp1llBAbqNG4kS34JDEraArdfn0B5nQSYAPOyvu+Ub2S16/u91RYznb
PcjbtAt1Tc7pw6/OV5xNEpjRYBHbG5kPZ3DjaSKIakKJpS+zfMXbtr0HoM1TryUo
0KSPI/Ll99NbXXpLxW2tVOwNr+FexXYB4IsISC0Z331lqPTtr94rv+GlZ0f5KbFj
Rp30h0Wo7EKnENVLPaijrAhSYI7f51nuDsIi1/ZFqt4lA9Me3Vu/Etv3OZi5EHEq
e+gVbiUb6HIvik/nnfWpDhjO5LFLga7C6rOKSnLRIidj46NnzH6yeRkQuAcU/Fby
zqawmYz+1QfcyKAxNaqrIEbKDOn4ws3XHboxSJWzAQ+72/vqhzSV4ih3MLkDeWHy
rWmuzsTJk2cdmSwt1+dL8UfjRDV02UdHjaBf4MrlKaX3ngfqibiskly/HFSfZrkK
DB+1SMASPLzZ7Gd6pPK3Ie8mzVYnE2SSIpBzgAqIsOooYb1oA4qLLq75HfvEuJKm
mBqcjsGuOFemASbZzsxrPbS4ASQ6L2MlH5HSoY4twvQ3b0SXhzYYKi++hZqB7prh
MujPkThFQ1qyDvFHSdthJb+O+DtD0NRV3yPTkJNQTBEAVEPMEo3q87dkwAruhUpQ
0uTtA2f8ROHW3YM3AKVhR4Zcwbf3Z3CEzg6gR2zdcXSZyD09OvyycryfmhA7Cnhf
Uyy9uShwr4J57q+XE/nYU4vgGhoCyyf4LT3VcX0M+Bun2a0rqx+7cxCyzVlHaaIA
```

```
3sZv5YQ2ZgQBd0YfbcWYGqxDH3SJoon7G7T7QWp3MilTWjtaGXf7GQOfZPJWnlrp
H9ZCvxKJ/vKnM/q8BTsCKpbMqLc0bdL4WOSKioTp1UGqi5Rf0bW55d4b0oNn5tkP
1nRLHdR+vP2KUc6B4pdZa8ZiI9ujg7R9xF/KwQb0B7WYC3a3Gu9IADtj5Z1oCvbK
2JFQOiUER+OyE5VmoPy7QoGmiX1jrLWsuwflnEbUEkd+qkhx0uv84jRHCXFsgxSl
HZ9hdNNvyTyFrmZrv2a2QcSPfnlvqGpYv+7pXL0gonnct5lc8PSVvuucbdV0R3Im
j9Hdiz+TZpE+XCU88jqHx/lCYbdgu6pLgkcmvUx2Ug464aRATy381PTC1eie3Xm/
z3tjOMCrOwkxfUa8VMTmI6gljeqPWodNgNtPLJDuWpHjCO2EWC2REcVAzCJGTnu8
LRfHAPMyY1DmbLg5QmmPh5zmkkjGSlaRbuSr2+k5Cd3XjNbEO8dbJ0AEQtwtBkD0
QSFx8IkCOiR03eV2+Wy43wnaCV5pvCYBHE557V6vkGYeRGrwTlRy/oGRQBKu7xvU
wfKLTS63XAluObZeOREWaNEZd79TqTdsoSz6IYjbF2EKgXJly8tgfkSvAbiFL0MX
3mUdxBUCSbQRw5eITl/MBrZA/VUYxIgJMvOH6H01uCaWxR48SZ2fim/NsE7+BUmq
4+Ihx9ZuV1clIDUxMCuDlOx3EjycQfVuM6loiO/B2qxHVILoMbldTZSavL+iWbCF
z2sLzt4b2ULzXZ/UUIJRY3efPlUzsKX60HAcim2IjCN2fWaPgv13oXT3XiGvtSym
Ez2T7TpTetaK5n40+nEfIDBC5WHOZ744zx04fj42hTbFWzy/I3+aR5vhdk4yJMUt
pq8vrEdhzv4FJulxW7xUdJxgiBE5/YLHEw6EE2I9zhQWjLem8U+HdLaX1blnZu5m
vZgEV0akIGuuMV7dyG7mf8RObqt17V4BOA0+cEugzirykruHnHSxtLAvWiRP2Qrq
b10PErMjdRMQNCz3ZBNL43PHwc5z8S+JjNlgJut8YU14ZnQND+7Msb4bKrPB8IhQ
iZWWR3VmZfqcBeBNpwe8+1sVQcntUNViIPPBOK4XWGbHuYaI38fMFdsvghL1qvnW
ul9n5vE+fayvImn5m6THMcIujGsQd5vYEFAzUZHo4lL4RuN1MmbUTOsBvewyZ3AG
BrcDix/ZdpSafATgAfVFDib26E7k9baX6+3XWfj8be6ND5gF597Yo9Ad12MyVhsO
YXX5DeTswvO0/0OCbZQMluC3hgnPf0fI8FRLx+0ioxx0h8dxvTUhQOvQMdaq9TCw
MNFfkyKt7RsFd18ZivEUVwy/sAIX9W75zjzNdZuZnyeyeNsB/XHR7TXgUKUUYw8Q
fjb0RZ0Iaa9kX+LnWhppOGIAOcB9NSkHv9mwmZ59+ZWoYYjH2gCpbBz8lBZyusqF
MBG2+EWVcXDmJ6H/NHgEkKGqqj74X1j/Zg+hOdrIZWXu8cu6Wcb2UqCYvkLvQB6l
A7Ihrk0TXY6pECERvfrAhWhVQsxrBQqND3Fbc2Nk6vc=
```

C.3.5.1. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIOkwYJKoZIhvcNAQcCoIIOhDCCDoACAQExDTALBglghkgBZQMEAgEwggS8Bgkq
hkiG9w0BBwGgggStBIIEqU1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLUlEOiA8c21pbWUtc2lnbmVkLWVuYy1o
cC1iYXNlbGluZS1yZXBseUBleGFtcGxlPg0KRnJvbTogQWxpY2UgPGFsaWNlQHNt
aW1lLmV4YW1wbGU+DQpUbzogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4NCkRhdGU6
IFNhdCwgMjAgRmViIDIwMjEgMTA6MTU6MDIgLTA1MDANClVzZXItQWdlbnQ6IFNh
bXBsZSBNVUEgVmVyc2lvbiAxLjANCkluLVJlcGx5LVRvOiA8c21pbWUtc2lnbmVk
LWVuYy1ocC1iYXNlbGluZUBleGFtcGxlPg0KUmVmZXJlbmNlczogPHNtaW1lLXNp
Z25lZC1lbmMtaHAtYmFzZWxpbmVAZXhhbXBsZT4NCkhQLU91dGVyOiBTdWJqZWN0
OiBbLi4uXQ0KSFAtT3V0ZXI6DQogTWVzc2FnZS1JRDogPHNtaW1lLXNpZ25lZC1l
bmMtaHAtYmFzZWxpbmUtcmVwbHlAZXhhbXBsZT4NCkhQLU91dGVyOiBGcm9tOiBB
bGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NCkhQLU91dGVyOiBUbzogQm9iIDxi
b2JAc21pbWUuZXhhbXBsZT4NCkhQLU91dGVyOiBEYXRlOiBTYXQsIDIwIEZlYiAy
MDIxIDEwOjE1OjAyIC0wNTAwDQpIUC1PdXRlcjogVXNlci1BZ2VudDogU2FtcGxl
IE1VQSBWZXJzaW9uIDEuMA0KSFAtT3V0ZXI6IEluLVJlcGx5LVRvOiA8c21pbWUt
c2lnbmVkLWVuYy1ocC1iYXNlbGluZUBleGFtcGxlPg0KSFAtT3V0ZXI6IFJlZmVy
ZW5jZXM6IDxzbWltZS1zaWduZWQtZW5jLWhwLWJhc2VsaW5lQGV4YW1wbGU+DQpD
b250ZW50LVR5cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04IjsgaHA9ImNp
cGhlciINCg0KVGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxp
bmUtcmVwbHkNCm1lc3NhZ2UuDQoNClRoaXMgaXMgYSBzaWduZWQtYW5kLWVuY3J5
```

```
cHRlZCBTL01JTUUgbWVzc2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3BlZERhdGEg
YXJvdW5kIHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhIHRleHQvcGxhaW4N
Cm1lc3NhZ2UuIEl0IHVzZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBm
cm9tIFJGQyA5Nzg4IHdpdGgNCnRoZSBgaGNwX2Jhc2VsaW5lYCBIZWFkZXIgQ29u
ZmlkZW50aWFsaXR5IFBvbGljeS4NCg0KLS0gDQpBbGljZQ0KYWxpY2VAc21pbWUu
ZXhhbXBsZQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQw
DQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMg
V0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3Zl
bGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gB
UCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXP
mrszyidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEF
XgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41ko
aZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX
+TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iP
sIVKarUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZI
AWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQM
MAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkV
fAEj8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJ
KoZIhvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtK
tl4FzkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3M
RsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0
LIZRzWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXw
fDz8A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu
OfQsqm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3
QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElF
VEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNB
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIw
OTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEX
MBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo
7sHUa4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+95
0MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYW
Tut3SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfC
n+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9
COgEykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIw
ADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21p
bWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAw
HQYDVR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwH
Fwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4K
kkOHG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30Uxf
yrZlRAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HV
X524bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP
0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+
JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSz
NnEmMYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1
dGhvcml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkq
hkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNTE1
MDJaMC8GCSqGSIb3DQEJBDEiBCAn/5Euey54zEPMTWTi6D1FzMPXZyPmKLehwiHU
u97UIzANBgkqhkiG9w0BAQEFAASCAQCldWAb1Y3QmHJaNLnrFOVTdBYsVLQoKmle
oajirYCQ8fv1D9dknCPl2tRdshOMtV+c7sR4wW6XNQNBdbLh/+zw9aV32quYp1m5
LmvWZJnmbVCuFqZwG/frYlk46SXkggJZCFNuTKRNiBMERuYtyROlQUX3VlchX3NX
n07FBEgy6SwD6avoVEG7pG11J6xlcUhOLl4aPcb94LkcUHpNj5kSet8+klHQw1KR
VCjMvXymn4aygpSkiZT35CjFhZmAoEaFUilfl354sl21RjXMZZ/2fLho2SzWXCR4
qwji+i7VzeP6sQ1Jyt4vpv4R2p9stcSEUpFMRQhqNfHiJd0kZLYo
```

C.3.5.2. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-baseline-reply
Message-ID: <smime-signed-enc-hp-baseline-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:15:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-baseline@example>
References: <smime-signed-enc-hp-baseline@example>
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-hp-baseline-reply@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 10:15:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To: <smime-signed-enc-hp-baseline@example>
HP-Outer: References: <smime-signed-enc-hp-baseline@example>
Content-Type: text/plain; charset="utf-8"; hp="cipher"

This is the
smime-signed-enc-hp-baseline-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from RFC 9788 with
the `hcp_baseline` Header Confidentiality Policy.

--
Alice
alice@smime.example
```

C.3.6. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from RFC 9788 with the `hcp_baseline` Header Confidentiality Policy with a "Legacy Display" element.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8625 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 5376 bytes
 ⇩(unwraps to)
  └─ text/plain 430 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-baseline-legacy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:16:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-baseline-legacy@example>
References: <smime-signed-enc-hp-baseline-legacy@example>

MIIY3AYJKoZIhvcNAQcDoIIYzTCCGMkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBABcSvh6m3bqMqug7JtspPDcpNnbUKLh0maZf
xtgFkNpttPxzoOrbgzttatlfuOHinFXrm9p3onp4B/J+UqntN6mGVogOhpbBeRFD
xDEEI+2rs0NPkOqKSTmIrPSu38mHMtUCfYpXegNs6Ez5pxf813Ack4X504qFKjKc
P77YqBVrOZq/LL20s6+kTABWgPsRP13lUNUbp4HUcaQ+SH3uZpOO5IzFrboYrDb0
vDjLvYKvfjraLgLlzFW1Ie2eGLQl1L3ri8hlMIWq9MX3hUlegecVyKo75l5i3CTo
cdp+8YROM5zWx7ID4y1lL0gy77wZrP1JWLUa5jloPOB9omzvl9IwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAVPIlzTVhXAsgTJZHlgb/wSMv
aGSEh6a4nM5YllTEfvhO0IXIyrzgMC14HCAMLkrmjDEnXtCvMHMd5vLKJB49UX1s
n7x8EKYLqHC3RJkq18DN0mnIJ2mr9qiohxSQN9ie//93a8ar+kKgrl2qRCTtgTcP
b6CXHVwLm9FazwJlC/ZOjS3YY82Up/P8cgXEbAji09ZIryaUUrljr1I8R5ivjIPF
cAFtnkcZ32eyahNU97pmnF8nZD5JUxBpQ7OtOqemBBkJAy2YcqVzzCJG1seO8id5
O5Ogc9YTehBq1EbU7HAUsHMw+3T8cZgH22vec7HJPvrS+BMvPGlNYWBGyvvc2zCC
Fa4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEENgnBbo7rgFT+sfWGsbYpOeAghWA
eDNEsIoFnkJJHiOW+TI6ecod4Gdyku4qQKjULEzI35mhJhbofl/IrffWdG8CAdgf
VYjItKwG0zu0W0RRJtVqaYcjcDXX2HXcgz0QjsLwJETWR6nOZ92PfYwJki0sW6PK
sfnZPRnK7K9Sb24rEOnMLgb3pmLXXx9JsH8LMlTVuN/JMk9wkqSwDgubLMix6eFS
QHtpLYs0YLoIyli/sw+fI58IzplPsCzpUA8z06jptlroij3j6iCWuSj2NlFhea+c
t5PVR6I+UuGhgCj8VaQisat1yFyUL+jeoeD1EvDQK2wMioOiEpP/m7bJuxi1malH
RfDkeAWxLf3A3P1aK8gBxVGEO3hFyWjmdw+hOJoK/AEk+0q2ctSfyc0bmkz8TiHR
x6j68TnDkVUpAUd5NlW2ikitk6nsA4c9Bj99Br/1LqKonmA357r2sYG1vEtxviJ4
pqxZhHiKsIs0D/eWbheXuXkbT/jrEDlr9ibSuRXmgqq8JV40tQtDvUvdVTq/h9Xg
JCR1zjOPWUSAHyz1iCg1yDIO6YLvHPgFlxQtT97EiX1WRAlkEGL//W6v33vkhXTJ
oTYyLr0U3d+oQCiLxQBCIrsBl94p1t1NjeEK79NrMs+yhRAQ6Um7ckddPBWKHM/h
AcOPv8oAyu8eDTiOoJv1ZKNcGIc+itQn0HyMHBBCOsRPVOJ5MIZcgdw8yOe9pYbj
4mY70rq2IiOnrjn+y2zr0rswfKB73fQNdfF04rCTbzLo4x0oH0BODSdQJ67CmtJ9
hBKLRjb4PPd0sdDaAjTFnVYOXjZUOKj2DUhDcDBkiiIrPf+PgOXtE5qc85FgzDZ3
gKyAnaKqEnVqYbmEhSKMRJ/dfAWrFQQBX+5Da5tp4BSRxNJ8glP+fvqr4W6jftPF
9R1SfpltX6xgPRgrHaDKc/l0rAliBs1JaGpR3ggYB+C+Bd9DVD1MAmuVoWTwOLNm
pJnHCHsLsvR9hgcUuobIOEVDspIitfi3Phn5KGfGZ3a7SN5a5gX0+l++DuX3PgZo
x+34fGY00wN9EdtNOqxu3PqfRNYQr6723oHh4aTxwx2P2hr2xCp5t6aDWFie+U+n
yZ89q8f63WUl8GooOKjnuxP4I96w6/eG7ixLvORe2QuAFSEvF88NzN9m8CiZ8yQd
PJGPoqbgeM89CbM1oFoI5p+PsGgtZp1vxPtiOpv0eVyjlwBrGEX6PO8iimAoe1HB
p+Sk+UdmAUGmxGFLLg+Ju2PqyIMRrYc4NV7cTi0S9NXV1lF3PXo4aIQuVv1HGJ9H
7x3KAcM8679WLTjXTNcDifLTXJlH7RO+Ut1UMc4gHZ5MqOI2WLXWjGW/UJOcB0uP
Q0AsWvpDsoOFw69qPooFBf8bt4CjjOx3Z1IWIGLiva61ct2QQjnv2Mo5ccxJ1qoD
/Uw7FjCGj5NHcHd0P0o6fv7Kc2QyJSJB0rjgRI3dbeZ+N6h7kyx430JaLvU4hXiY
B3CHeoea5y6YrAv8nAmhXgXy/kaKISJXyHmWTAP5t/z7eoCPYbUNPyKmNEI1iYqR
swDc5ENFOQFhs6r+xbak4KEVd8RLjP614KxzVrPZyPE5mkmcZ3xWK/YZcUhDKZOh
```

```
XqKx5Jh83yWMQ8VgGxqUd/rhUOltSnjiRpmWOwGft3fLh/x3AD71j3MEKrkJHSBK
eu6HcC9ratgaCXunlbvcx6QOx/q2fb+eyEhFtSoZQwo47NbJHUSYvFOjqoqA3LhH
1j8GfPzN+sLlkZ5HWBtdIAWXTQOC4epY5n1BYWsRCeDjKl/s04wR+VbGJsrPQ1jq
f7143t1T8yMS5g4iIpjEOL1RL/WoPYL3ooIz8tCCMQQh3qL/zaKCi2JZaj1gy4y7
dusQRV0azSNNwjK+1WYbzabodXHsQ3R87TNq2CNWrIEcRkYibeBEA1xWvECf5TGh
jtOnkEZcIFKMHnYpIK+9D8yYtuCarzol8BeOyuQN6LWZyMiNOZXm0rvzCIzqORQF
MI+xL4WJetdEt6wwFIskTVGpJPr3HyjU9ageiNSpXql7+A+DMCSgaQoyMKRtl8Sf
tizJCqGdWD+/S6iZTnr4voJdsJ3nPArNlu5Tf+tz63S3APwbj5uS9qoBR2Vas3cb
IVNgTwURgznpRa5TXO+sDlSz/nNMr5uZAXiSORearVtOyK1aTM6LZ6t1Yf6jVh01
XZlGcmW3hW5bdN0UMbmgZznuSuqA+0rjCJsHoPUw+3ubSdegmBGbIa7lyeuGGyJZ
sNeB9KdddRmOCbk+0RybzDCZJhPTHpw8yqVi2htOs1ZElAa3obCrbVEU10xMs70L
NxdPXZPiv/VDw72JEcmfKUm8fTbQfatWeM10U9mOs7Eub32VH0V3RbB48bnDrslh
XL/ZUs7OY+csMemEVy8XrbBvNuhSZLo3mdD0/XmDYrCxa5pKOhZmIt3PGeamYRdf
IQDN8WsaNGIDsPN3w0M96sJWhn2pYyErwpsSiBMRnLmz71yo+embXKJWTsxTXubN
bmCIG5vxJ1Ew9vxqj88y+sbWrpI+2jUT23GVqy3+/iSruFtqZL7f4QNMemCWq2SC
1m3Bisoq48TObm88Q6BOk8+owhjeG7KylFKQJEZvJE1NSisIsEDQQRfzwGBgpDyU
D1diWrCmpiynhqOmBDeljtjIHQT83knRiY3XbSABr57w4TM9SLCUZ+/b826TpMiX
hl2aKH73/zVPH6PAamxKCub9YP15ZO0BHKKi0zZHQQtesEH54iUGY+O+1/LCSuQ/
Q45Qvu5CnWBFx4sYvFRtJfMynalAjUbWfqK/BGnS9H1rJKYiXlZr0lt+/cqU+r+h
POc4OAeyORsg+szBns4y55gWhGVicyNU2RRqNg3dsyj/sUZhysFiNbyWF+NCXsYa
ND79DR0UL4nm7XVXjz6y34dRV7u00nWRPRWLBhum/ekv08Fv03oOEQ6sfJElhx5M
6fNV8R+8849k5oZ0FxvsMb6sJU6N8hxgpMqlCODGH6KnizJZOxfjJhMgiyEX9h8J
CSV2noFCpbDsIu+JKOSi2LFCfj8wT35q1hsdrn16sUq4/crG2NMOZrYPhh5Uxwim
nCGWJm309+TUh0CRV3JmU4t/Ls1mdduErrO/W/7SF/pD6zCg11hmpHBKFu2mzXTT
GjWlJuHSy23yzQ3x8kaZLkw0tNWVOtWzlHdjBq5TXOGU/IBjOfRbnsSxC8btiIFS
ZlcyVfRphNT2WXgXZ6pX3soWiE7rkj8geEsYkQLIT1yTSYRzlX98NuFUEgrgTWaN
j0VgflqIXfO4UrMhkHp/cTcAE311blLaackHTdRIj3Xciubs0dZrIuc2AlJYJiOe
ITdAzgFKx437Hh9MhVdW9DC6Osa8b5FEesiexc4ZRYBALp+XCQLiSO1flUoQxXLh
8dvr2dAYkITswQNQtSO7FJlvp3ugNNW33BJs2LGmaLhvosBh0YngJx10fr7Fbkyb
YHenw90TSy6gtF37j/xmtUjz4vI0cToRunPh18fUJjxQbaepXFw6M+YC2Up4S0GF
sZEAv0qQjBdXezU5z4V8wz4hgPcuvb5w37l+fP50lmqHjC0FHKwi04JdinaetrpS
Nwg/hI6d5A2s0gMEd472SLP2bR0INNGW+DZKtewTC6WqrniR+WT/TcA2O8NNsZVT
GZOOSf5/Kd+HR2apkmOKq5hIYsDX84Ji/eY32jHZO9K0DfCQ+zBatQ00JUOpYMEq
lDLxoXKV/qUuXEp34foZvZT0699btpmPhaD8aTKLlFV59WD+TwdC15n7V6at9Jnq
kqe5AVV28faXxCi4LVOJunjNlkCA7SUraGVayRPEL5SG7dUsqcP5jFPOwHAZgC2K
Crr+zJZgwYJqTaUI7gKUAsxph0bFqn3RL4Qhnc6b0OZx4zVcwMIWTDt0W39JZrnz
3ia0x9U1KvrNlnLMDl5xPro6XwhqOD1QEGZOGaZmByTZO7Wkvoe0kL3s8s0xCWHW
bjoWydg6rxeyfPW3ZY3Htr3nzqfVovFupFbdj7icm/iPM+B9gw+0sb7IZ11v9Hmy
NFx6DqPDQXvOTijea66hKfIyxPMTfZFZszX/KOOO9MNBX7OzAibgprJ/fK4VYUsc
NPSJlHZ59DWpAaZZEaCaolcWJBrxvb9ycir5ydPudQUpTN8z7agosdkNPT9hxGKz
WrsV5hxe1nhDklG2VJ6ohkCbiJawBO8pZE48nE1r4cwYT8u/CvzfIHX50SmXN20l
ugVbTDygrRG8nCKKkym6hqi+/0kzHKRk2V48HAal8CNv7h/iVz8R3a/PyGD7cc65
w9fDjyjpex40hsTy6tmz/7dZtu3lFznNDUYuU/lDqDAJUG40SGSwCUzlp6TRmTZd
z4U+26pPW74eKJ1isz8QVfrDEsn3Jk/IBE3SrzM1VyfuvxLKYEMXARAJoSSVk5pz
n/rM+gIKQ0hXTUYIyoKgfE75SXV4fSCSy1GHgdbuub461HDEXKVc43qTbQkhOlYp
5u4OjdfdXcq790GfGL9NslVxTVCCpTrQc9n7jjkplvBXQXwDXCfpOqzTar6+Nkcw
EL9r2+5PsVOzw5mpHDY933W9AkVaLsnqxyVsFJz3l7Up0Q7y0yqM8ecA+6SW4gAh
Er7UHcEmljNidhLGdoZKjMijDGRAiCIavFi+nbihkRumrDhStQHKqQhfTU7JyiLq
UmWNlhkPax7Swc/zBW9J272LgYV40mQfjYNacY7KaHu44xGda/SOrMeUnFPZB0mU
edkdsuG/jhVT5UgifL8SXnCL6DzyA9Lo/IDb7PQhUHhEhWfNsWd1F6qAZohJrdqq
lDShd+g3t+MBshapvaXtwjI7DbZ3WKRFeyhdye+Leml+Z0eD58cR1N3GqCPMRyWa
+fEvrVdaJKBizTXgeph3g2Uc3vjGnmNH4x861zuG3+5pKpONV+10z33noByApeZg
GrVOwwXVZQfr76ZSR8wwLpAy6EvJ9E9gCMC9Q2RlJzdZ93hCqQVn1srocqu9RYD/
YL+P0Mafk7TpvEJmYvAMMydiBUfGkrCIOZa5J3D1oYZSd392gt9SYeju+EZ4HRJn
usZhz6T/eZpSNJcVEgrHSoRI9t83o2Dms197VyVElOY52KgpF2H7sGTauWuMwJJO
MmaW7xzG1mP7+4miBs33urlijeToL05EkXD0eEL4lOlddLHmHQ96189+orgzi8qt
kB6yeEFfwK1h+7ilooPmfSaQj5Re6G8HK82CIJaVH59Yo3QoCIeAZhcnxMKrNJSh
GRC5+XEntchPH4iDyGC7k5Du0CfNKNyrFpJ8vwdGmNZiqnEatCtXEtzqEo4Z3ib9
```

```
NHLz/bJzPPDqG1sLIe+fv3Cpb9a7G9uMyn7ZzAcDarsRCJdjdfsT3NG9Jeh2LeeK
vEDFK6XyQiz9QxCqNqdpEGgUff/zuWMHaXN9RmR88uyNPN2mClnF1A2pY8oRhdVC
kvF6urIbOPS2Tiih66duBPd3nF1y8xFwwCCjgeWSffhzVRfvpdqZ7mlN4GimsI71
o6V6ztsVM7A247X1jOZ1/WBIhF1fyMF/jf37Rq6N7FAFnMOZWJSf0b+UTXeXzS6z
6v3PbA4grpEC9U6wDDO6zq1JVdAD69Ecw/IsLa4uhoJNJa4ZmXxhPg9gl301nMla
z5LMulGDSHtgbOUYA6Z7E7WGDm1oTYPeI+O1ZzPDzpcOrKd/QqX5zhSAAaYqcuQP
Zi8S1CON6AYL2r0bAvrBCc3oKUgIAXCgcltiRrt8jW3Tm1HylgtX9hHxmQqx5Fwv
EK/F2qxnZLpwX6y3ooQncBIn14TC2fGTItbAdwReyTZjLv6l13zSgGWNjcDXQFPz
koLT4iykPcFXJARBOn+TQqbEQC/MkZ6Vej9DHYhmN/dXIAX6aVWBgJ8yKRs/8YK3
QhAzQizaOgtluVA7cNcrVk1lk87Ee6aeYKB94fa4Nkl42vukEerCGXNUW+wZfwO7
wK/+yCh8yFIKSeZPRk9hejMCCuhl9rLoVVXvr7kOp55Eugi8ioBBjnJ1Hj73p2dj
Howx+JIEFrT526Zmf1oMxnjT23+mW0UQNxQGVev4/+XdfR+mG6ah9xF0b1MD+9oP
vVqHxsdUuLtqPqFWmcg7JmbWgAB+tvCa4ET9Sg6yID0UH0Fenejcotqa1tZiDRGG
g1YiI3llBU9CASFmzN3bXVfIs4u6RyYHSo2VTNA4A4Uen06chZkWNxYtb1BjIMnl
6IG49GlfTO+yhtk38Z/JZzB2WcVAFNExQdgxlfpQEU47NSTa8EgyJFD+0uwr6A1o
gm1e2S85ViHL26YTzmDP1CH5CjD5/ZlBl6mOBZXt3euA7hr46zFe/XCa5YqlUuOs
PER2c0UlvY58rEiJghTvy3p9sTbAj9m5wUef54wivUXXo04LoZhlleHpiFdi1kYJ
13B1KWkS9HwLIjv3AML+rSOgWZjT1QLDM04RohzDJP1GKRmMp0uNY2RtcQeWt7hv
IgNQyOb0BUtWFiQye9lpF8rmtsfTFfQmFfYmcALTvGqEAL/hQbYYSZLDHJBGt/D0
FMlX8K83o3do1IoAYw2kBcm7bHLAXT6e6WY5URJ6bhpYk29GpLIe/RPtbNLefqwL
OlzomfzU6I21VRqb1A7NrWge3UPIx++mIMi/qK7n6OS4pORq8qvpZqoVSgWNEOwd
QQD6Zh0RzjyB+H52xyGZTSb5GqJBMCJYw/2ZiHOHGMbH6iqChMT5abMzkCFejWlX
LHtD5szlj5Bkc1ptpM3jYoIwFLB1er1QnNktOFFzJejj4f+OiODBIFYxkakc1zKx
JdgkL6orA2jZ6AE5Bv5QbinpUySz6o7hlGvi2bdjnJUti3I3dtaMnzF9BJxl3aqN
sSsm0obh5ds5xURSxhkK1Q7T3buV/hMZlsSbakX+xmHA1eA8uWYROQqf7KCQqGem
6Hk01xjz797mSnpmi4w3LrI52MSjjXdr9sf5aCcLJ0Niok5I6SLoNyeH7TwaKMZf
ReMp83rBGP+KLEyfGMp0/PuMajQAsqXgJG89T22tMq1+G1uGuWqYW4GI3Zuk4mDq
ygZqKCwHiR8wvDjppzTiuvQegN/K6MIwjgKRcfoPmBxI4KryoKK83Xs7rA+z6spK
zJpUtlGSV24ooyVcWy03RQ85Gc/HMMwP+zOg37J/YZASBpqjvlSWxDaK8ZzR+dEJ
1EAhJ3uCRenTRURzMyrysBdLayLFW+gHUDFC5F+INKPGMertJqtYdfOs0tqG2uPU
JX8U3mubey4B4G3j58ok7ZBD4rOll+h/8Z2Nahs8udVMMfSB0xx8bmf7rwaJKf/K
yg/AjedixIkUNA5CfMErF/h1EV+zEux7jyQGdVQ7xJI=
```

C.3.6.1. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIPPwYJKoZIhvcNAQcCoIIPMDCCDywCAQExDTALBglghkgBZQMEAgEwggVoBgkq
hkiG9w0BBwGgggVZBIIFVU1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LWJhc2VsaW5lLWxlZ2FjeS1yZXBseQ0KTWVzc2FnZS1JRDogPHNtaW1lLXNpZ25l
ZC1lbmMtaHAtYmFzZWxpbmUtbGVnYWN5LXJlcGx5QGV4YW1wbGU+DQpGcm9tOiBB
bGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NClRvOiBCb2IgPkJvYkBzbWltZS5l
eGFtcGxlPg0KRGF0ZTogU2F0LCAyMCBGZWIgMjAyMSAxMDoxNjowMiAtMDUwMA0K
VXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0KSW4tUmVwbHktVG86
IDxzbWltZS1zaWduZWQtZW5jLWhwLWJhc2VsaW5lLWxlZ2FjeUBleGFtcGxlPg0K
UmVmZXJlbmNlczogPHNtaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmUtbGVnYWN5
QGV4YW1wbGU+DQpIUC1PdXRlcjogU3ViamVjdDogWy4uLl0NCkhQLU91dGVyOg0K
IE1lc3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtZW5jLWhwLWJhc2VsaW5lLWxlZ2Fj
eS1yZXBseUBleGFtcGxlPg0KSFAtT3V0ZXI6IEZyb206IEFsaWNlIDxhbGljZUBz
bWltZS5leGFtcGxlPg0KSFAtT3V0ZXI6IFRvOiBCb2IgPGJvYkBzbWltZS5leGFt
```

```
cGxlPg0KSFAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTA6MTY6MDIg
LTA1MDANCkhQLU91dGVyOiBVc2VyLUFnZW50OiBTYW1wbGUgTVVBIFZlcnNpb24g
MS4wDQpIUC1PdXRlcjoNCiBJbi1SZXBseS1UbzogPHNtaW1lLXNpZ25lZC1lbmMt
aHAtYmFzZWxpbmUtbGVnYWN5QGV4YW1wbGU+DQpIUC1PdXRlcjoNCiBSZWZlcmVu
Y2VzOiA8c21pbWUtc2lnbmVkLWVuYy1ocC1iYXNlbGluZS1sZWdhY3lAZXhhbXBs
ZT4NCkNvbnRlbnQtVHlwZTogdGV4dC9wbGFpbjsgY2hhcnNldD0idXRmLTgiOw0K
IGhwLWxlZ2FjeS1kaXNwbGF5PSIxIjsgaHA9ImNpcGhlciINCg0KU3ViamVjdDog
c21pbWUtc2lnbmVkLWVuYy1ocC1iYXNlbGluZS1sZWdhY3ktcmVwbHkNCg0KVGhp
cyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmUtbGVnYWN5LXJl
cGx5DQptZXNzYWdlLg0KDQpUaGlzIGlzIGEgc2lnbmVkLWFuZC1lbmNyeXB0ZWQg
Uy9NSU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQplbnZlbG9wZWREYXRhIGFyb3Vu
ZCBzaWduZWREYXRhLiAgVGhlIHBheWxvYWQgaXMgYSB0ZXh0L3BsYWluDQptZXNz
YWdlLiBJdCB1c2VzIHRoZSBIZWFkZXIgUHJvdGVjdGlvbiBzY2hlbWUgZnJvbSBS
RkMgOTc4OCB3aXRoDQp0aGUgYGhjcF9iYXNlbGluZWAgSGVhZGVyIENvbmZpZGVu
dGlhbGl0eSBQb2xpY3kgd2l0aCBhICJMZWdhY3kNCkRpc3BsYXkiIGVsZW1lbnQu
DQoNCi0tIA0KQWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUNCqCCB6YwggPPMIIC
t6ADAgECAhMPLSW9ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUxDTAL
BgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUg
TEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQx
OFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhM
QU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnelN41K
ImVaTC3D9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt
4jse2Dqs165ernT9O5NLFflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S
6DgCReZuTtMc1zy++MxQlqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCq
lLqhBwDHdZ5qDTII2PVX1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6
vL/PGeWy6SCf58duq/AOEksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYD
VR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYET
YWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8B
Af8EBAMCBSAwHQYDVR0OBBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQY
MBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCBSXig
nLEynBakDKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9Ii6z
yBZVjdaox644DsiLOQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz53PYD
Bh4zE4Nar2inC0D+VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eDOd
u+F2MVtluLihne0Bp1GUTkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb744gqoeu
D9YSHjKK49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzlEc2
tUpAr4vRhZjVD6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpqp1zAN
BgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVs
YWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9P
krYo0jTkfCv4TfA/pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY6
3PQWl+DILs7GxVwXurhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K
04s+A8TCNO12DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMay
CQtws1q7ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN783
6IPPdfTMSiPR+peCrhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90nj
lsJLOwIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgB
ZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAww
CgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyX
rilqkBDTIGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkq
hkiG9w0BAQ0FAAOCAQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ1
9naIs3BjJOd64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaV
WHg4eHIjSo27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHa
hiXRn/C9cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgk
LD59fk4PGHnYxs1FhdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFX
LJtBiN+uCDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTEN
MAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBs
```

```
ZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJc
OvT4as6aqdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEH
ATAcBgkqhkiG9w0BCQUxDxcNMjEwMjIwMTUxNjAyWjAvBgkqhkiG9w0BCQQxIgQg
48aQJVg4Ai/QpEFw8rsxq2fGKjdKAo7F9AiyJ9AcdQswDQYJKoZIhvcNAQEBBQAE
ggEAVvcWqGsebWjsEhsQlER/C5Pib2KPH+9KhVGFbCjDFZvBmNklEI2YomGPyrXq
OoPdQEQpVKLXB3M2VfV9BotUyXNQRR48gRU/P2kRGclOnaKOkzJVnBQjuNkcTTDF
+CHduHMFTcBHNmvWn9TsxhzIksqIWWqTS2ugc4JGJ+Oh9IGX5HBpFcuXU3ouznUt
RQDZNZuiqo7MFcw4z8uJXHXiZM4lWici8jlSs7LNtlUX01Wd/K8rTJZZZ01zpEtD
vjVftz2p54sEevwkS++c3eM9MUyNYT+GC/Hm2m3japmH8E7grmssDeo3d4a1aKy9
wd7sRi7PdwAgwUXiOuso3yAoqQ==
```

C.3.6.2. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-baseline-legacy-reply
Message-ID: <smime-signed-enc-hp-baseline-legacy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:16:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-baseline-legacy@example>
References: <smime-signed-enc-hp-baseline-legacy@example>
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-hp-baseline-legacy-reply@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 10:16:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer:
 In-Reply-To: <smime-signed-enc-hp-baseline-legacy@example>
HP-Outer:
 References: <smime-signed-enc-hp-baseline-legacy@example>
Content-Type: text/plain; charset="utf-8";
 hp-legacy-display="1"; hp="cipher"

Subject: smime-signed-enc-hp-baseline-legacy-reply

This is the
smime-signed-enc-hp-baseline-legacy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from RFC 9788 with
the `hcp_baseline` Header Confidentiality Policy with a "Legacy
Display" element.

--
Alice
alice@smime.example
```

C.3.7. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from RFC 9788 with the `hcp_shy` Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8190 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 5054 bytes
 ⇩(unwraps to)
  └─ text/plain 326 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-shy-reply@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 15:18:02 +0000
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-shy@example>
References: <smime-signed-enc-hp-shy@example>

MIIXnAYJKoZIhvcNAQcDoIIXjTCCF4kCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIEN1cnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAEY/MQAP8JUkxGJr2+gL9fUy/gTYqzyKkkZF
GQqKBR98jCom6wtry9FqxMqirqkIXmy6QgPsFh9nf6QmP62K3QjP/aGDI2VLeKJk
beQfZRQRCLqqsP0MRQLT2d8lAJAHCO57N8tdm3jXavSWxaZkEqWF1rtcVCz2QQRg
iKJ99BPNEjwLLK81VCjxTkQOcxRgUNUK21pMQVFoltXE7SGVjV8jeEiEHj9q65nb
ITmfNgmTP9oNk8gojEj/cmTy+hHGPVFjDJZxAHtd4tjU4k/LP46NRAW3tmaxOKMP
v/WkGMcYQGy+qdaXn3n2Fp5VCTfJjFW1bZHdSHwW63kTGr+uOQMwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAk75ys1csbLhA8HayfcCB6yPP
70oO/9hlsazxTzL8NcP/f3vzlVEdaCXKGzQSWRSMgf5RoxQvUrFCTaq/F+rbGM7g
S03e1DfxGb8wUgE2ZeZB1o0GvSd6eNB6gjayEJ9AEHwpT4bEJeh7TQ/Mi3PDwelF
kbmA056B7R7529w55YeQF7ZgsJxicJFp00ADPw8iYGd1bOj3wGt3Kz5uycUqsc+4
Q8VWlU5N+8jeJRDVPtEQJwa+S2HyuaPLUZcyZWkuGtVAOPRyCqSjtgSwenLmRTGU
YtwAFvQ6K5E+vCRPyIAg/HYwaYNeUJn5Cr++YkpNBofnrofxaV8zKRIx96IoxTCC
FG4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEHawOvd97z0NJQe7ccQnSR2AghRA
lqu1gwka8gwMldV4laK3pICEOTa0bvJGWO7wrvSEAgZUObXjd3ekfVtDGWgXhWbB
8uaam5ssV4WViD4h3iZ8HTRPiczbSsJ2lf8CKOwqOYp8VKQ/wy87yVB6Mna3ZHCT
PqyEOTYYsc6nrf9vQIxrE6I0Roa6FJ33+PpS312CglFyMyhs5bS3TTt2xwnBvLJX
HoPF8JwGxe5xkD9xqOC8jjkMdBcUM8y+DRf9vcDYLAONiuJzpaixkEVG8lFdsXtz
95b3Uedf7XdXe9p/gnqfeVvDLvTjUoxWa98KUM+ZC0bm4gHhTwdP2itiUGMiGYZf
yl7WICIW2jVPVZ6GGrcE9fYwqsG6O+5vygpte2juAQUkwQ74PIcVY6sSWMVbFmfu
```

```
iWCQ07OXmNDOtcSHd8Uhz1uqUGQxNElzFQJoKc9RzO4O+jSgSRenVvfwR0AtZy24
WnvbnyUHESgmcn94eHBYow7fqmC7N63kTwtr4NXuMAEH1MvW1iVkJNyB9ZI/DOCr
0fv+/yPfLr3Jobx94CYnP/FRqir1h6dO1M9RonpK5wj+YEl2zNUmegCDizVCcuvP
md2nj91RGccyWgmQ4LPrNdMk2+nQvKNm9Jrv2iHNseyuwGJrc9cczvl/E3Xf0cnu
mS8Y4iMPY/wRnIBN5+D8IzgWXvhMEGumwtT58XFL9KwrLjOKRvai4iNIW6K1fh8J
hh0D7HrdneBas9x0QV7yP2TMuOO9LBln0M9OAlIJAa2LNBoMLlaaeJvv4/AzTIEm
GEYbVIxD3ovj0jm9GCEn1XNgktaTJZt1g+u1v3bsUOIZZcNGdsiUpMXY5a4xnO9N
7KGyn0K/ALBt4dsfY4V0hfQ7HrgAlOs/pO/6bgfGfAul207nzGUV05C2gvn0HApq
tU0RpW7F59q5rr/EMlMU4RIE4RtsKFv/jjLVMqwyQ8c6SAVsdCUNCqWPPN5KPKne
B7NQ397Wfrpd5+f0IiQ/g6GQpSpiQjjfZW/tKq+EGxVpHqrM/wtM9W8phh+rRas9
meavNl9EuB8aJ2gjansk/IezbZkUuN8GUzhFxEQHzSQNADeWjt4rnPaBzPrKzDlh
MqRk1j2LrH8Oh4xBzimpEz4Z+MzEY13pbdu7g1ZWyTCiewHeyZbIoRZNLFtYG6rY
uGjEX1MHkY8HarcAqii4Uk5KTi/cEoH6bOYj8zIlcGxqiA9Xha6jsaG/BkRQS0Mm
/YqBxllLNoyiTV/VC53MoHfA4Ro2/4YrdaykBZEPoAn0mM99EUdgm0vqQeiKLd3j
IePb2udTgpPlHIR6Nw9XNlqiUxFyD5PcBIz/JNY4FbZQ8xWB5OpiQNm8zL4Q7Sim
6RH13Wpl1MIU6FhS1K9966Pjkh/nMnS7hPtsH/rBXxrgFVBv75Kn1gmccadIXvQh
fgZTXjXDgw+7ilNxJn7c0tCgZpuGM37TmjIXANDwBCSJHfeVG4WdJTKsM2NXJrzH
9uFOUnhwY8LLmy0MJ4BgYMqe7cCHBZ+Els7bbUCA3la4tYXQKQY5Z9XtE3bst8rO
2fxWkwF0qncK/giXEhSURyiMr9yc1T0lGfF3jSxMahSohnBA3cKHBww0Y5Kj9n4l
kemATIjN88n7IazxyAztz9n7/I2FXmPAtu0W8FG5QBoIhfBw4cunuHkzAU7yTSNl
MNCjYW7FL/ouvnb/MY5I1LySF0XqfJ5JEdgfk1gXsQKG5g4350i1T3I4XWsK6h5j
dJxTS9v6U2efWIDWYtAKqi0tNnvcbJjQBNx4zt/sPqqU6dCTSz3tn9QdYm40EuiF
aEBcna52jUCncF1EETp2S+yv2ZudNOUysRGAfy7maNGcqrUuLtXRfa1xdJ/TBYhs
wlAwdMKtakFv6dqu/h3kMBDEqcu3y6pWnB7mFlcso2CUkv7/CEl0cg6KNOtPz5k2
WAin1RylzYjBkR+OoMexQXQNSXk1Zf8PKZ9QBTfFOiuifAfAizyAGao3CebY6WNT
1ewkZBAMoyM3iFjvCXjR203l2bkKSIZopA0FFIsDsGWn3ILZmPWq/9TcrNvqPTKI
WzyIKlml2VUse6OtvGShW18wW7BNBlsZeAi8naGvMe/9JmOShIJj/neKxgoivxrV
oM9B8a5k/qB7W9tecEHAyohQPOy11+1HfDTeClJmdhui/uhqFJW6zQv5+qCdx/sl
KRXR2uxdmpFex7u6EfaDUmKyO1PZg7a81808fTaBX+LL8N2LpNrpeoO8feH6nnKE
vvUl4wH1fabHsqUcOr+WADC1Uxsi54HmUszrdK95byESEjaVLJwL8LXj2APu7cx6
tZ/8qsDqz5x3CgsCTS1QXv74GwvnJdzs/O7vE0mG7c1v7ukn9qxd99wPg9vHwkEf
+d/45beotS4F5kBnxL+wXmlPBJ3+k1BgnFYuYodvXaDMUNZDnpPPQuKoC6RRVqYR
pjaOpmi9tuIjURYQMuSuiBUt28OfzhBK+kte8rZIZ+ZwykY/BIVEWbobOZMXEZyG
+3kPPrPxcV5omNiPdE7qjo0Skj8QPAEx4IcT1KBIS9vL6OXgH1tDbz5IYrX5eF3A
jFE38ykxMAJ4Z4NRFzHddZmqiPBWSPcR6+aYSGjiw4T4ywP1ZwKaPtB/2AXDz88b
lViai4VNsa1feH2UIMKY3BPpWRf6ADfWI1n+jIByAc0UkNynB/gL/UOfUOCLaRm0
QUchsCqO6vou+/Yil/czE9VxrW/ARBTw+mmOh7Hn+7aW3jsPxZLdTMaia9exM2VF
rBcyA/1iv+7zEPhlWJv6rVQHR6/goDQsaVfuyeumZRouazmKXpwVRu5i0pV8Ie/n
QQ2UXU7JytaLkeSqqsnLXo2K+NdIp0MXOBCu1TIz7fOZs/iUZphAxhZ+9qZCzHR+
j1X74Pu2lzGDWi9ElfIH5xrb0H9jYnqYWzM2Od5nLG9KB2oGluR8pgVSZ/c6FWaf
7o+2X0QpBdX53Ggpp4LqE/Mi6HbePQyt3c2ldkpOy/IFlg0WvyTWH/G3CBYPLldb
iPv//0yVozh8ZOKRpbNLUAjguDd6+m7cSNloIECRjeZ9VwDU6YFnRwraFDOeTbkZ
/5jjwrKVj+bCX+h6puLsBh+KZDFnw/T5Jlt5Z4CbMv5sPdwMBLjB9AmMCmEHwLVr
E+pWoT7lTl6kfqBd3Kyb8e5WeqqtvOQbYaVuxArxEFsKfzg6T+iN7F3jElfcBG3v
XRIgBkA7MhyMs4ymwjSH3GMKCE72nQ5w//F5L/Pv9kpMzB/t6SJ08TfnYvzqWbp8
HuSnYYYtoyys6+DdmWlPNWESYX4sGYkov2vHbnRojo4qGSqfsf7hmZ4lWKKcbyRp
NcZX8s76oWYpBfGDfRQS0MxOwnuh6B3TL6dD1Xy+HPhNePF+yp6eIDIo/pfji8pz
F0WZMKN+DGqNgF/EZw2m2hZGY2EyWXuDvSRe6C7d7jbbbLE2ydfxCpWjNWwQ6lD/
SKqCgpiyLmLG36Ml7MIDy7xpfra9pqadnoAMzfkzMnjky9pS+Torv+Yn4pP5H3ml
7dE0M43sLRx1ypkBSjd5S7sHYvlmqf1aWYQ5KveElT1Um1UtPz9j3qFyeJMYhBd0
/yBU7AZEHzaM0/Bwjz1fZQTw+5IdfM3CNPhxNC6O+zEgFwXDKlFBGQ8Ys1ygryH6
vXU2Vkg6Int5TWUJw2JPvBznnkqv4eQxK8WoGCeIHCaFryS49nTpa2YL+BAOC3Ct
Du7wF+FEEGr17xsJq6ok4IzqoA5LtTa21lde5PssaeEeJT6kqXyw8XjZ6aOPn76v
0P60mu2Bbp3xC/yU/SbVrAvkekX7Ah9ZTeGlLEG7ZxW+oZg/wnOc7eMkdz8xj+OX
X3an+SsHkf8xuIs/ryPyR1UU877yD9J/eV+1xgP3x7xwnWUrGigan/qK/TGe2WM3
FdzAFloPaq+jAjzItnZ59+RYOBCGiGMzUu7XDN0t15yXL3CeAP42YIi2exVQdj/u
jC27PzoF6+diNsenHt95jedzYB9FjY53++B7jzhqPTmv0QL+pt4O45Rbqtk+whgd
MuSFTsFXvL9L5BkBfM3fg2yYwJTAmyra8516c8TQj9PNtua0weCTf9WYfcmH+j6u
```

```
W2Dfhc6Zuu+OcXFXWhew50PqlfdeYJvxGGOqLP8hSBMN5zhyj8Q5z4MxiyOa0QVH
+4N+pAqiKw9rbrg5JOfMZjI9FgmcVJAbxZpxXk1oDpCgYMp1RcgkMJhaZOl1x959
bpfcbgL6HqyP1T8iQxDJt3wpRAinPVccScBEOJcJcaPXk1pVRfGTfwUtH+PI546h
uKdJF63tGZPIExodinaerZBiqkbP4jxPB4rGbrSJBi928QX5InN+pz3MQ8uJmyND
uGus9+FNgJ7a4j6mvdOz8lfcRn+U3YE1jLIEE0R/VtIg6jgezyt7/Z4J7rbf1pJC
ZHJQ6x6UR1VA53pQKoFVF9bsPl3ZvsvHWT8yblfKL3U3EJm0Yl+GHbVqaZR2XF8a
knL2/j4tpd/73jOvlb7eAR+eFgjh0HQdR/aEQ46eF0gYZTPDoXHB+9lxjtikAO6L
HgAQ6y1OnxuQWRaburXeyXYEoPVLUrYfdueBBRn8lTZY4esZNCAaCeqsICN2eKEl
wbF0oNH9Hn7vuIkdPCbSLMQxs9JBelIjgv1X/V0VVG8xiA3F18Jwf6XZl7AwpWBa
MBD7iBxovI0XAClxcWrB6ZlRYxwMujdIw2Dm98kaAeGpr9vXvkjxpLdcsSZF25cg
iSBoXR8KAbAvO8X0EciO/Or1qptyUgu6tUL+jFox7pC9Byaa4BW9/Dr4biwelUFD
IT3M7OhrYJDEwoF6UIjlcMpymnJYmqGasG59Ah4uaEieQxYk01RRFiytF+N6oc2U
39qNFtxzMs14dQr/+zuLdbugVge7v6DgC65iQl9ontT/lH/EX3hChmY6daUmz4kS
2VmwdoEhuO6H7yeoIhBTZ2v4+vkGihgQTo8xm+6rw/t55+nQfgQYTC/ZZ+9MuAN3
uKSvTsrorp1I6kK5zI8s6rOY+YaqS10ckNrYXmyq9TSIwyBzk/btb/mDvZMF/TpK
QIaHsSVlkIdmfq5YmTr+iNlwK1fcOZjseesYAhehpPJUzuP4KdGWr8Jc/pC0QNYd
iGL23ieFbTHKgPyGCmRdYgEMqpe/THE65H7pGuINigDEgkG4m0Eq7xDVbvy1SVJC
jc7o/O8cONg3kbHyYbGUlaIKBBap285GWNSotQSChkaDo3hT6S6cjPVsrPoqMN8j
PQNPARqKYRriyI3ej8msK311VRTjAGKWwEVgxn4nF02bvg9HBqv/TiFrTrFLSsd8
6g4HpglcnewxmVWjAeCsruK3IJv79JWRNPxOX9+tnd3k28E1QqwuEA02uNuHZLbB
TvlHswfi9xmPwZG1bytwrSB+kv/oE0cVLI9fPCKpe3I9N+oL8xLrlqG7vNqwaZAK
MTd1VoPxWmlvj/z2NahU05eC12yx29sJN9Oqz4DB2juUaLFSA45+rJMQc9Vj8fFr
/Qrq91UVuXQJIJXCWfC598YJ/p4VwL/glK4ofs9ssl5MZbj3IesHFEwN5BQm2BJB
khO/s2kG3dJ5jSHSFcB/EDexFZtdLCyEwjiMNQqniOUwQjaZCKf4U3QYV2vxTL9r
jA7KfBOgAdwgXX+tKRWv0VgIOz6gITE21u9envfZ1eqOfexlfGT1xv/E+iGauIST
qgVKh0ciZMPqhRgaBHrtrjtTyifweXbSKo4AFVNHN3K+swDmXW/XHQ6Y7UAjseZS
ZFtjurmHB+uYz+O4kxAct4fJW7d2e5iU6tEGKseCnBZ//PGgzkLbwigdNhopou/Z
s53h4I2Z0rxJFz33NHwTx2wquT7MLwCZwD/Thttujx6uI2JXMa0zudluK7S+lj2y
d3DBHNGszistpi7cUoOgYVMvFwuTSPgvLfyb3CiyUHlK3TIEqox2BJun3tXL2P9s
7tFBjgqVRqm8AYDRzSpkw5jKL2xWBCI0j9hd2PDOQbhw/EgLNqlHmLK7Yqy5TK/v
CMk2aLkVAORtQlryJ2M8WlObq3RPjwfc/zB9NWKTpX/EuY03nYXQLG951Oajvodu
sNZB4JyeNKbIn9LPNZ+8mfaxHE8Zmqd3A8XSN/KfSGOj5k1wkh2qrWWlhbZQGBnU
ocpwedKqvxKxun/nGsfRmDvMzSMqRfXYxATneXH5IhmCLsBx3qeGLiYoRkLd0434
3Z4937SMWwtg+oZYcd+ndW1OnEVyGqTmWB2UKhJhfIhL1YzpkS6444tdlIV2LKeK
GwhG/6RzVZ+qnNzeEFlJjwUsMTd+4Xa3k2bkMBJQZggOtFxCeiANkVsBzrT6DTLa
L9xJqDPD7SROKHubosXhFwx/cDcFveWL+mbkfQc9/edehffeCvdgXO1CIxPmxXHY
y5vETDTiJqDd6+wjQHRrjoTv17Zz2ZblhhvdxLnoE9IMABvmd8H6fF3L4jIn2k3K
Kc0CAy20FA9K2eMgCOW1+JeYcgA1Sh5Y8x1Fg6Ah0FFH62SMn33B9rMYOB++Sjg0
vh/1cfHXaZPwpMb1gNU9hipbThL+2MH0irtzQ7sn7X9FQqvkQwA57OaXXpUId2Nu
U0rjXrw8AxmaUtFpN43rCk9t58eP+vosfCsG/uA80ptkEqb0Gz3FM9B6Be4crw2O
3Oivl7+0dpJ/rAD1lG3Vq6VAvpAQNT0g0/TmrHJ2rnhX5UUxZB7YPF/eufDDtLF+
BZNXMT9+snguEJHRifIxhFXIsE/MFti9ROSsbT90u4k9WxY0PI5hp95dkvX/PfUO
lNsNQvN/OjVFx860ZCY2UR+l8VhYwUkTL6qlBAeVca2QvdZ8BIhr/GNHfXyge0yo
cIbqf3WQnU/05jV6v1YOq2TJZaN8tLaf+rJait129WW48fCv/oxW00xUeRwB6Fnp
```

C.3.7.1. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIOVgYJKoZIhvcNAQcCoIIORzCCDkMCAQExDTALBglghkgBZQMEAgEwggR/Bgkq
hkiG9w0BBwGgggRwBIIEbE1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
```

```
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LXNoeS1yZXBseQ0KTWVzc2FnZS1JRDogPHNtaW1lLXNpZ251ZC1lbmMtaHAtc2h5
LXJlcGx5QGV4YW1wbGU+DQpGcm9tOiBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBs
ZT4NClRvOiBCb2IgPGJvYkBzbWltZS5leGFtcGxlPg0KRGF0ZTogU2F0LCAyMCBG
ZWIgMjAyMSAxMDoxODowMiAtMDUwMA0KVXNlci1BZ2VudDogU2FtcGxlIE1VQSBW
ZXJzaW9uIDEuMA0KSW4tUmVwbHktVG86IDxzbWltZS1zaWduZWQtZW5jLWhwLXNo
eUBleGFtcGxlPg0KUmVmZXJlbmNlczogPHNtaW1lLXNpZ251ZC1lbmMtaHAtc2h5
QGV4YW1wbGU+DQpIUC1PdXRlcjogU3ViamVjdDogWy4uLl0NCkhQLU91dGVyOiBN
ZXNzYWdlLUlEOiA8c21pbWUtc2lnbmVkLWVuYy1ocC1zaHktcmVwbHlAZXhhbXBs
ZT4NCkhQLU91dGVyOiBGcm9tOiBhbGljZUBzbWltZS5leGFtcGxlDQpIUC1PdXRl
cjogVG86IGJvYkBzbWltZS5leGFtcGxlDQpIUC1PdXRlcjogRGF0ZTogU2F0LCAy
MCBGZWIgMjAyMSAxNToxODowMiArMDAwMA0KSFAtT3V0ZXI6IFVzZXItQWdlbnQ6
IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjANCkhQLU91dGVyOiBJbi1SZXBseS1Ubzog
PHNtaW1lLXNpZ251ZC1lbmMtaHAtc2h5QGV4YW1wbGU+DQpIUC1PdXRlcjogUmVm
ZXJlbmNlczogPHNtaW1lLXNpZ251ZC1lbmMtaHAtc2h5QGV4YW1wbGU+DQpDb250
ZW50LVR5cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04IjsgaHA9ImNpcGhl
ciINCg0KVGhpcyBpcyB0aGUNCnNtaW1lLXNpZ251ZC1lbmMtaHAtc2h5LXJlcGx5
DQptZXNzYWdlLg0KDQpUaGlzIGlzIGEgc2lnbmVkLWFuZC1lbmNyeXB0ZWQgUy9N
SU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQplbnZlbG9wZWREYXRhIGFyb3VuZCBz
aWduZWREYXRhLiAgVGhlIHBheWxvYWQgaXMgYSB0ZXh0L3BsYWluQDptZXNzYWdl
LiBJdCB1c2VzIHRoZSBIZWFkZXIgUHJvdGVjdGlvbiBzY2hlbWUgZnJvbSBSRkMg
OTc4OCB3aXRoDQp0aGUgYGhjcF9zaHlgIEhlYWRlciBDb25maWRlbnRpYWxpdHkg
UG9saWN5Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQqgggem
MIIDzzCCAregAwIBAgITDy0lvRE5l0rOQlSHoe49NAaKtDANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQJ+RpwpODxxzY60n1
lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+
hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV
8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41
/0HJvmSwqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWf
NEbkN6hQury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4Gv
MIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1Ud
EQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQw
DgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAf
BgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOC
AQEAgUl4oJyxMpwWpAylOvK6NEbMl1gD5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LD
sfx7fSIus8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzT
jqB8+dz2AwYeMxODWq9opwtA/lTOkRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps
98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpfB8PPwDR6chMZeegSQA
W++OIKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTSO7K459CyqbqG+sNOo2kc1
nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJcOvT4
as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMI
TEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlv
biBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsx
DTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGlj
ZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0iehY
OBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LCOwI2juwdRrjFBSXkk7pWpj
XwsA3A5GOtz0FpfgyC7OxsVcF7q4WHWZWleYXFKlQHJD73nQwXP968+A/3rBX7Ph
O0DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZO63dKvIKp4cQVtkWQ
Hi6syTjGsgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKR
u0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGJWiQVCCpDt
c0NT6vdJ45bCSzsCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4w
DAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMG
A1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQUu/bM
si0dBhIcl64papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh2
```

```
9FkwDQYJKoZIhvcNAQENBQADggEBAHOJojanzqmgaSN3/gqSQ4cbbmdj/R40BEPr
+gXT+xiidfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1iffRTF/KtmVEDMR/sYeqAH83
KM5p3el2lVh4OHhyI0qNuz5oShNaACSioQ23WxHGVy9vsdVfnbhsplrWg9NQ2Wbp
CmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6mrYkKTM/RCGnumghxwYToj1Oy
D5Gs4D2IJCw+fX5ODxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDd6hnoQ9
rNeozIcBVyybQYjfrgg4DRvw9Ksk22OH4ConlB8f7R7s1LM2cSYxggIAMIIB/AIB
ATBsMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQD
EyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhM3QQV5
7XV/QqmiXDr0+GrOmqnXMAsGCWCGSAFlAwQCAaBpMBgGCSqGSIb3DQEJAzELBgkq
hkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE1MTgwMlowLwYJKoZIhvcN
AQkEMSIEIAsnTrJmG9vhEDGPGAIiq3jNFKAZg/b5qnb8K8AAVkcfMA0GCSqGSIb3
DQEBAQUABIIBAH/7j5oqF/rfVNLmPNfU3UFn3oHiaWt3+y8+fLX1e4uMgFOshe5Y
Iz5rkMeHmP0HHtnqfbPjyktjTR/wlmHazGcasD5/KT2/1/HXOJJdaM/YQ4g5RiBi
h7TDwAfDsNMMeEfYII+gDXrVeTc0BvtrWetxrGYhbMUNLtM5tskMhuUMVYrQBcUh
vkYBamQMVmiZMBOFHhhA9hEay6QFIlAC1v3WtJvyiJCShld1Qetd+NuDbaCr6vZt
+C8LsBh8hQO+TIT8AnV8yBhQnqFGj61JQjwGBRRwQHbvAEG4uxaWr2OwCa0VWOh5
237SKEh0m/haavxKarioAGkbzlAGbNElyX0=
```

C.3.7.2. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-shy-reply
Message-ID: <smime-signed-enc-hp-shy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:18:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-shy@example>
References: <smime-signed-enc-hp-shy@example>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-hp-shy-reply@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 15:18:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To: <smime-signed-enc-hp-shy@example>
HP-Outer: References: <smime-signed-enc-hp-shy@example>
Content-Type: text/plain; charset="utf-8"; hp="cipher"

This is the
smime-signed-enc-hp-shy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from RFC 9788 with
the `hcp_shy` Header Confidentiality Policy.

--
Alice
alice@smime.example
```

C.3.8. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from RFC 9788 with the `hcp_shy` Header Confidentiality Policy with a "Legacy Display" element.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8690 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 5422 bytes
 ⇩(unwraps to)
  └─ text/plain 518 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-shy-legacy-reply@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 15:19:02 +0000
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-shy-legacy@example>
References: <smime-signed-enc-hp-shy-legacy@example>

MIIZDAYJKoZIhvcNAQcDoIIY/TCCGPkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIEN1cnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAAms1ngOySnXdmv6DCfeI7GaiqqHxwOGv1EI
l0jgi8u7Y72KiMZwvjFeRLtLpbE3/D5s/MEJ8AJ9LN63jhEUv+AyF7L29pqX7h1R
SQVY2I51zrm5ilPMkB+v1Dng6GguD8XDqmsxgi1oloDgExg4dsqPbGvYcXqQOUli
B4XdqnREveBuiXp5KetN7RROt3KfD7o3Flakl90pyUIh1gpArSbndjbnjinlwbby
fChri1V9NT99P6BVcdtOoduxEFIUxW8Rb1mmjlbpZQHUN9sxFftA2+qZE4YPGOnn
j5GyLFAmVbJSOXYeWN2S0TMrFl+RF0H5HVfoTqOMtEaKbro+CgYwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEATEB5GYpWDLjGLqDyORR4LW+h
3+Sz2jt7VF8p4jo9c2WubRx1jmmzULRw+Nc12RKtprjftmWXCrzEwiqMy6KKijCI
e9Rd5812SDL6iNp1WUXYbqp1x969IQNvBTfNGutgQogB21jNm/qbaL6fAjwIZXxW
lLvTBi5LDe+K6/dwlRjPJlZ/BBhyj2miqz/x+rYsSaG3REExLsN/uIv3f5DGrqg2
2kHrHjXjIQE8/qYPa0t2fKXFJsmH/4FUT/384aepm8oiN5y8xSxlgeQoW1drFvGC
sqFVHomUGvReor5zM6Q1bwrj2FAKQS+Qd1r5Z8bWatQmMfWGu5Ix8m1/kocX9DCC
Fd4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEPUytcsL/JFRST8refH5jrqAghWw
myavNN8eGoalhPR5erxp3r1BVoRpk1biqcaFsojj2XyGUSqKM3bcnoVAW70KVLCk
HhxzxEFYVeK1BGhW/W9d9JSiwn0OOl7Z0KX0Zf87C9xgnigpjpB8c7/Nm/7bmD7R
Xp4stpyVCjn15E0Yz2R5wLMvh23b7Od/c7UxS4yivIxM8eW6zDsHUVmb8/TT+0tG
kVXIc2I81l4WQfVyY2KsQi7Jn8nYt5WO63CVin+FHoSRSdx8hChedXptVj6YXeKp
24Ugp6cclAEHgcjo0NHNZC6wnOQjEhsra0VyUt2e8FFWAVE58M1HpFNRIgSXNFdY
eq1O5nBt5g2XnYgiJM+AuEuXD/QpZwpdjIrQif4UwLW4nJCUCnyTxquT2wE+CuU/
```

```
8JWm/8xeVmGlXfSHRU9ElHdBTFS3OiIAZBfu+9S7LHnnB2TZraKBqKQuk+K/DQMj
CZMzXLt7HMVvSl0lw8erpkPTz87ugBzXvLq9iCVZ8CirmQouXXTWXyoEf7uhtOBF
t+Y3aNhNnmjoqs7S/Tw2HCyvk6azw9hFibYm7TCqviLhwpEk64Ol5g3OPhpKGZdw
sYY0eTndS/j1uBNT0uUCluwj7Nh60xCmRtzpuFZXG+HN5iTR0wgGpxJH0Mj9QdTV
uctaEakmHfeJZZqo9N7DfqrQV6Cs5MKnWQ9YZQX/mloY2WDtQ62umI+T6avdkfsY
AJPUMnxBZgvS6TYWwpW7xwxWMs+skLRyzdjFBds3A+O8A0k9E1pQ0Cr5VPV9pYNs
n/tZyY+LMgF3VV6+eN+menuNet9BDEqntk2R+waAlLDZ3mQXrsNTgJ8U8MKXEu3E
NdcRRl6ekOmbEW1X0Wn9N+oVndbZbIiERHHLRhmmzo7nNSniBKn/0AHNGBM425kT
HfUYPVsm8o38NAQ0lnSJfa35Q039UucojLLazsEQnPr0T1gSy+CMhz+K/HYF2OHY
S+mV+lNuXrvfZ7sUUdSsKWoqbxwVvrohhXSUrmmwZrd6DVE2GuOjogOAhP4xA1p3
6/NN2/3szADTOXDO78jmchqYu9Beg09K75VByVFzpc+1A9ZCJv6qSZ9GilWoaPbz
RIR8lxox9Vtjj4JD1toPL2Nm5LHdL1napAMNuolktDL2lKuMVCyGTwaMM/T9DSDf
shr+FTB7rD6YKd/GcBCCJehy0cRd3Y/hLFI+vJBaVEtpCSeH+FuYU17ap9+EPGmj
kJwkVqPyBXWlTYr3fthwtWsrwE650RH78vBbkoE8zny6RRTdV0ENPZEsKgCp7wpt
1/JrGN2M5S9P6A0ZTsAkBvkPMD52m6dYJsopIDyaDvtP/QMlIPuS5o7npfvDCsr9
qpE3DObT5L3dRKbDdnW365+13oaZ6JnxOFqL/XZp9h1n6vxAxx7MGm0lrd3sl/nL
QI8w22c+jeJbfINsIzkbgfasPxdbYGcgU5xGCROOTlAqn8cU1W1NRkYGSxTZSp6l
vNGc5MN9ShtJDlcOxoG8nW/GMhx0MGNh13htAfcQB6d61v1tFAT3sJFruaUF1pF3
0DGQtY1Lh8UQRqAYkfVfSeW5oTd52hBZZfeHMDHEwXOHJLjKR4pLTqPskMFSpla3
5F1uw5abtKgDpqT5ilf4919FBPKT/Ev1BRENt2nlq4jSDjSkTm+ZyZtRdWKoUMM6
LDRnA6T1GXv/+WNDS3KcGSSKZvMwQHbOdgs3lBEzvcNka2jGiNiwsWpj/6axZIjl
AyH2ySc1zR47bfb/Gks3NVZiyAmedt4WU8Ph04uZuoSYuV40V8c6ntk5P9g4y+rG
RdXpmUhKN5cTTezrs3EH+p8O/cD0Af5odbWQE0EZtam6Vdnl3afFeJoKdnlBET3K
Q0kTL8aFxKeRAbpFOTbCgNqzcP6iozqlxz2OmBGdNBhDLwLWDzQBJOOO1aeXe9rs
3NvO3t7oZ+ZToy5swk8JdLAkS9JOWAc5ofZwfhwZDLnpLdkWticucEjyn8SoqeLA
tFAG67GGFStNrpPXtIbdndhSlNLP45UxCeZU8eO3fcs8doRjsaTTbpA1MmQMH3+8
pCJci6DlkLvwtb0DwwQ+LWSW9bEHWkGfxHo0y2hiwhUCnTw/DvQRoLa7feb6cSFW
o1wWO8F0kzyD7I4Qc6gTdhnksSepJdlGOFia9R7HNmWhpJL8QY+Okp6WFxF9MlBu
TJkzhwK4XwdNPoX7eKPK+0Mhft4MFedAbPNTgHyJO2JGtUik/h8dduxrhDtgXVw/
jBUg1m0BBslrhuXk77HedXoj2ws690Fb7UdwbyVAl2+8GzGri19zOjYMHpE/V7Qq
u70zUByDhqEQHCeomGS27jv6mBrL8jkqnB+EP7p7prxSwrGsXIfIzg2+cKp53SRy
4eOR2gNzdHFfMH5rRNM0ad8aCBtL6/My/7zTEOuh7Btm1C8XDtkksQuJaTz7BrR5
SyBUrf8g7S5gk3oezrC+U3GQ+B8vOAlQ1yVJbIYpHNuHy4VbiiYC56zDUc5r368O
R0oF3tcbQn39X+sTQbtjjK7dftxgCTwr4irxxCxxAEAOwcgK0XBhIlMIL3Vo/Fsf
wFxjai0LgkNTwY9EwgYNdgArlZzyuSoOZBhQZ6oxf5jXEBh05tYTIunCFIwfFLqh
o8sg3ZoaUS9NHaGEsruz+sBG8zsbwSgGjzPAyJyw95CN3gM6HI/Uaoi9x5Dx/IR8
883bTyK7wcjy4l7P7XZF+Puw9fGoGOADVpjux9brsBluoYQ/Pm3F9RvCOJi/89LT
oMZnU41ZEkFNGOSnTuGr1lbKSdSe9DTt2J2oQwJFnskVYPhGrLIa2UetQBs8Oqve
iMKrNP6CRhKwLbjgwe1fC7WTiYgrhrLUUsjYxlqRsaPlKeefXZzFBWH10o01lkU6
vkrr5Rl9xtv0zJVPGDOjbWVMY9QLWu8Mne8evi2OLSJhyiNcVv4my9Taf1fHCSS7
3xK6rdJPWy27eCNVoQwE6USLwsSybO5hsZCbECWXYM+mvD7EudFSPPRSJzHyB1RP
8h0OwZVM/V0S1G9HTBFJHx05iCxqszlePsKmZPzGQFcl5xIxQdt3xtlIOQy2FQVq
Mfz2Eecw+mgr0Yf5q38i/IxvcJRN9x5u9efAuQNuf5mW2CJTmll2JEtNuYQ3r9W5
QNmSvQZn0+whGIGyfbhvBLhDQJYGN0TXmImoJ93qceLyWoyOTLrTRrM1y6h1sfyp
HrTnW80Mcaeqwx7/K9oDkU5yG3i5LOuy4I80kM1HMuY8zUcuf0tWbqwqb9kJn4ow
/FWhpJWmaUVoHy/Z8J0ca9bVUNEzgs1DV4TJSzYyAJiS8vfCuhpFiwZn9IdEN2B8
xQzKj1gHH8BKzViYNsFyjxPErPlwe3HYH3mYSzketCyMAWqGCLjnx0A7h73FGAe4
qOqkI9Ea1204BH7+zZUuaX3l62SXwwXXNIWPGZquXrvwD1IT7ylJA9quKM3GShUX
ADv4J0tR4GB4VzVijEBJO9Z7Yo47PQwLYU/DpbimfSgKOSKhUyHF0McHzyrLV5Mv
PwB4qCvvvTH1xL6vCKzQBssZPIFfPFSu7G/xUTiSytioTeTn0ecnyVXOGrBuUaQF
IXe1Tn/M3rz9DYBoutCVE8iW3nTPF3v5OP0LfYn0sooxy0mi/5e0fjtoesz7L5sm
nLVwWPjEg7PAHQS5jHSDhRW2x4kd+Rx7DCESIJXEqrc8ge6CQTWe5IoA8IwqN40e
+MwXmCScDSe4OHTqbx7+OtN/HxqbzGWCjITTVEh9QKnCjhjNlLB05KTV4nFlK2YS
eomLT7FdE0LxsNbZIBTZMAxfSGJUCaEylikNHEseRc4AbKML4YdtL/5Mtg/yOzMB
qwIldlXDjjwh87iYDwJoxBGL4GewGbcYICMZu76qnnyfZd0j6R6jDg3rna6v9cXr
8RAI15+3t/bnmGjWV4E/18/9CE/N+8Lk1+LknVbehykbnM9vBb3smEJgESqmn1sT
4quISc3z1Pjv3q47iR+lRWG9F5icqRSu7ZgmCXnWqw6iuep3mSea/HyX23x0U6oQ
dvLIl9vT4ji8wG4F+WXlFVe5acl09Um/30cG3pJTjKcogmBvlyJPJt+1HESmJT9U
```

```
rGfrA9k/94+e2Ye9ksf9irp4rPmBVYTAvnwzr2hLAqlaas8yxGMy15fOuPQ20IWX
sFP/eRuAeVfbYDGGsqmYhSKXbvd5AJtupiM9SBKqBHCjQYT9G1Q3hUE2qspHrweE
hvhdCcK/T0sfVuZrcykUtBo5G8wTtdxSLMUU9prqtYR/brtQGBveM9BchW0iPgTS
/jY1R8V+j37GQG5oWV5EGXS8IObsMYzRM2SugwsE1zb74LJrsM209+n4Z+CQT0Il
e8zOEkBikQMtx6Im2SCYyYXRi3elIhFolCszCQel0bsr8neZOjVS9aQkH6OEdl4C
4JVit2D41Vu7nq2CvWqsjgwz71vD2nVEEBVqPnk3SC6dXXUP47GAiyu0XoL+zFdL
kzQoFuiBSmWavO53kUOLhSWdt/hkIqzRT7uyd3APBIHSG8ZvTqEEYX18c4dzr8Bz
W6Q6o2DNnI82Ht1I7g/ioXI/U/gmc6sWdYh+W+1VxIntu7sjTZz9i+PRQPEvjWdM
bG3hqkOaPj62+2Mp58FHC8CzILViy4uND4AsFrzBYOsybRi48SR8LA0a2QuUPzHa
2/ofW8pehUmhYtqP6kFqtibHdEGBmxz0ntkYzp3bZAPrlyLfSF+aWS8rKVbrgxjv
wGHUxaRvLUKaqJMq+h50HzglaUPPdElq2cshqYVjyIKqrESk4m3si/CKS6GqWW5v
3oaxs+WIn4cil+PUgIKhRtJEwpZnJzXOteK9gyKabPJvNsJWmkkI8OdXafDVdJ7F
iJ3PQGZmrturTlGRavwk+EW6cN9jG7KTrQ1jBgYpA3r3ll7EKe4f2YlScmzLswXO
GeV6FIcdu3xC2a2NOHSSCleglNffJiYJPtCwKiQK2bY07pgL4jXzsa3YqnjoOJ32
pDC5DMaTQPLjNW6hCC7JxVDiDhxCj67b074YDyhWjQMnIDXLVFanRsZVG0Rj5+Yl
QPk27a8EUF65vGFAUAvXOIXNPDK/JwvT8BylHX5HjASqK62i9fuHqOrg/OBsDTKI
XKJnS1T802HuQze1ZZEDs1lDays6Bi4JdIVZZKXt+RqevZ6YoZ2O/1Jj+t4P3cb8
e7GK6vLEelOg3F7N42POF4Nl6NiycFtuF3c1RNvGbPw46HAZvUkU+Bdd+ZFy9OyF
CCaVsHo6/9YGK1oSASdr8wY9yMBZSQFJ5zdA5ytOUSWARmu7YWkGN0vRpUYhOoAN
0WGS+lVSmfak2QplyGHJzkkUVTLgcaBCbdO5RPyLRe/brwvGQo39tTCHlgsspNLO
RyDWZ64ZqFVSBCjcH9ys4BCSxdFzS56fAFQwX/Yq2bIXmbf0RIjDgMju7e5hqXvU
r0Q4uesP3V7P1tOuYz8pJV8L4hBiJHoPb0vgx45wzYrp7n6d4aqBm6h644Q1/OhS
Irf6cCU+ue41dyCOw2pPjNxAaFHPwBRg3J6ogg74LwUWZUQEKycQ1KjI8AHY2jLq
9F9nVb560KPnob7G4BHS+5T1mKZmi6qx8o7VTWLF1gYudHKldF9eNY0dvp9/9kKX
829kbKQQpX0xPiOkdZyOq5O37zcGTRuv6EIfqJTERYkIxHCfsPFHXUloyhgzu3X9
fFJUO/ue/P4ZXT8K2EbeG/9Eegzytw1LDkFn1KjG/G4AVx1+Hd3/UY7ia7ZPMCAR
Sw/l9ZyElbzoE/x1/7elpV3r4rjkJeUh6oRBknd/nENW6gakpFxYvHDnru3AEoxK
kNZCTqyH7iL1Xs8RN1QUHILLXNG9wc+bIgrEpwmqqEAbxVHcmZgX/07bxGmYTHGX
tNHt3QcKaA7EuVTF2Fx5kKXgdeM6P1NaKgnOIArXHdfD4OrLDPa9Sh5TF0APOW6Z
vRvuG1qv9biI7+FMJBUq2TSPCVX6i4VM1i+Tckx18VoBK3fQdOmnc+BaLks4FQNA
ayKrnZBFRvr0n+aUPfb4pfBWn/1YFcJDKXN4Isqp+BD0rqJqXUi0zEAhHsJdjiZP
dXzpKSygdjR8w+d26KKlky6HS5dBuoUA1cKo4kyMTBU7SRv5kHmm8WWKg02YMM0K
/Gj1ApNrNib5wCoBClLrGS1IpeHNjCI15/mQGJPk4wF67GT/37JkDQH+hiWhOvdN
EvCEGqc5YkTFh8OTwDD+5uSLmNvSWdf9BFaQVR2RwbMSVAaUc6dggZe5qlmBqN4R
T3xrkPUADPxYZiP11jUJCFis6wsLP4bOEpvg0KZ/9r4+27UvUbmZk596ptB4I5LE
Ck7Dwf+Hiiui/RL2RHfjPFfRNJX80OdMHjRz4meAWvS/0HlyENc2ruc7lt9dVECW
K11KiuFec8zbEZGDBJcv4V3SvkpLf8H7zZSTER7oBONvi8uNsIaU3l6JdpusAfiV
UHCYJ8kTaVoT6b6h/9cJ2TufSfv14ktvdMiW0wJ1vKEyb3jE3fQgaHQXbihPAX+g
uIIgYYoO/myUIITzSKjOINU9/TPgrs5M6fYDHbrZVDA964EDYIToiGFQZTu5TbyD
ojrdR9FTiuYuoki8fkTPJc6HicaY/rDyKvNlpINpa2jA5qSv+MwtLdLX7c1RcBFF
/z9pOHo7SeZiREWqDJZ6pN7bpAumE5XgLW1WGnUWBbtLATjqyOeAUnRbyXv2RhFW
gHjwk6RDv0ScssPTcribodZWHpKo8jf1GzE/AxkjDXxH7ZkoXfuK2mTNRnynFhqp
328FwkRvik2udbFKa0AXI/phsaVgffz335si9EYxEGa9VXR6K2ikZ1YpTNykvN8N
inJk2YRXjVWp8zlsswNwmyEaRdsv6E5EYmpCTOxFD6YnHanV8t97X1EmWYV8Vg1v
9jaL+nhm8zrEK/R+sG6nM3Mvn+7/igG8QObvZfsmcRTKxjtpHX0aXgz/vuDACgR4
wVMY3xSogDsg+azivtAmhCpkfpbRkjr8PdySvoY/t9FymrZjBFFlHYLsIsr32KKC
y/cEwUm/a8yUcGWzDfDUWeTxpr9kVy6NpKhQopnVlVoYwruYEJFauHcXKI4htemb
VZuUNio46th+9sSzj8AMCpn0PDbVq4Q+XMnXK3seF2tvclwCei4r/pwudKum8ggx
x+Z0pRpLkCn5tYbjgKedS3nDpTEHLOIRa2zACLvsqCbsNn05af11MTOVyRfUWkAI
FkEq7a3esIoeIkbhjv1P4ZVnmWwK0HlmVdI/PxH39qJDIl7Oy9OiXQG9OGA4NRwl
HI+BvWMJJ234mBSUFIZ3N/nfmHl6/S0HE9RhCHgDBTqymCdLiAmEQQO+RXvehrh6
51ecm3eKdxurHuZKq/0LMFykxJH0RJyh1SDLwb3eePI=
```

C.3.8.1. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIPYgYJKoZIhvcNAQcCoIIPUzCCD08CAQExDTALBglghkgBZQMEAgEwggWLBgkq
hkiG9w0BBwGgggV8BIIFeE1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LXNoeS1sZWdhY3ktcmVwbHkNCk1lc3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtZW5j
LWhwLXNoeS1sZWdhY3ktcmVwbHlAZXhhbXBsZT4NCkZyb206IEFsaWNlIDxhbGlj
ZUBzbWltZS5leGFtcGxlPg0KVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpE
YXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEwOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW50
OiBTYW1wbGUgTVVBIFZlcnNpb24gMS4wDQpJbi1SZXBseS1UbzogPHNtaW1lLXNp
Z25lZC1lbmMtaHAtc2h5LWxlZ2FjeUBleGFtcGxlPg0KUmVmZXJlbmNlczogPHNt
aW1lLXNpZ25lZC1lbmMtaHAtc2h5LWxlZ2FjeUBleGFtcGxlPg0KSFAtT3V0ZXI6
IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcjoNCiBNZXNzYWdlLUlEOiA8c21pbWUt
c2lnbmVkLWVuYy1ocC1zaHktbGVnYWN5LXJlcGx5QGV4YW1wbGU+DQpIUC1PdXRl
cjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6IFRvOiBib2JA
c21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEg
MTU6MTk6MDIgKzAwMDANCkhQLU91dGVyOiBVc2VyLUFnZW50OiBTVVB
IFZlcnNpb24gMS4wDQpIUC1PdXRlcjogSW4tUmVwbHktVG86IDxzbWltZS1zaWdu
ZWQtZW5jLWhwLXNoeS1sZWdhY3lAZXhhbXBsZT4NCkhQLU91dGVyOiBSZWZlcmVu
Y2VzOiA8c21pbWUtc2lnbmVkLWVuYy1ocC1zaHktbGVnYWN5QGV4YW1wbGU+DQpD
b250ZW50LVR5cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04IjsNCiBocC1s
ZWdhY3ktZGlzcGxheT0iMSI7IGhwPSJjaXBoZXIiDQoNClN1YmplY3Q6IHNtaW1l
LXNpZ25lZC1lbmMtaHAtc2h5LWxlZ2FjeS1yZXBseQ0KRnJvbTogQWxpY2UgPGFs
aWNlQHNtaW1lLmV4YW1wbGU+DQpUbzogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4N
CkRhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTA6MTk6MDIgLTA1MDANCg0KVGhpcyBp
cyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5LWxlZ2FjeS1yZXBseQ0KbWVz
c2FnZS4NCg0KVGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBt
ZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVk
RGF0YS4gIFRoZSBwYXlsb2FkIGlzIGEgdGV4dC9wbGFpbg0KbWVzc2FnZS4gSXQg
dXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gUkZDIDk3ODgg
d2l0aA0KdGhlIGBoY3Bfc2h5YCBIZWFkZXIgQ29uZmlkZW50aWFsaXR5IFBvbGlj
eSB3aXRoIGEgIkxlZ2FjeQ0KRGlzcGxheSIgZWxlbWVudC4NCg0KLS0gDQpBbGlj
ZQ0KYWxpY2VAc21pbWUuZXhhbXBsZQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0R
OZdKzkJUh6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjER
MA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2Vy
dGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5Mjcw
NjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYD
VQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAJqVKfqLwaLjj+gBUCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg
9r1mAfIDlB/wlbdmadXPmrszyidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07
k0sV+UdSNRFxrfKeoQEFXgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74
zFCWp2f1ZkuE4A6l41koaZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY
9VfVfcrv9w43GG8FtpSX+TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r
8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcG
A1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5l
eGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNV
HQ4EFgQUolNB1UQ8gCkVfAEj8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfx
CShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRG
zJdYA+R9eBAuDLsatbtKtl4FzkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5
AQ/hgxLvLir3hEUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5U
zpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGn
UZROSvSYkGiWDp1JhqXwfDz8A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19o
WZD6YrzSWHUz1F00juyuOfQsqm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgw
ggPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUA
MFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhT
```

```
YW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEy
MDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYD
VQQLEwhMQU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l
078oullsk4ASvSwjsCNo7sHUa4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6
uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEO
ls/gkUP2GxzymsO2kaYWTut3SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBl
fkgKN5wXVgkWFfiOucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4Ku
ElnAtJ7BtZcsl7dUy9u9COgEykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8w
gawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0R
BBcwFYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAO
BgNVHQ8BAf8EBAMCBsAwHQYDVR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8G
A1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IB
AQBziaI2p86poGkjd/4KkkOHG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAo
cCn5zbzhW/JVdYn30UxfyrZlRAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoT
WgAkoqENt1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2z
L3HR+M9CDr4Opq2JCkzP0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF
07rNmT0TzPCVzUAuBlr+JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSr
JNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRG
MREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBD
ZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69PhqzpqP1zALBglg
hkgBZQMEAgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJ
BTEPFw0yMTAyMjAxNTE5MDJaMC8GCSqGSIb3DQEJBDEiBCD7w9aychKiKqa6/sht
F4TUlddh7IbF6DnI0Vaa95yhfDANBgkqhkiG9w0BAQEFAASCAQCEsnuIovDVNOBB
USthxOARiNhm/IrfGyx0uYeIMCR2K+UZIEQ2+aeYGEYKh/2yocr6VfauX0pK2prW
s8bxDewJdOVgw13QbcmgyhOMg/5dQLh0pTcFx/5b0rYQp2dLwpFIOzUrFnycGJI/
6qo82knE2ch/7NMWtKB7Y7n9xKBXTC6kD8LwIrG/li0tSyrqcx/LUODNznTB6xoV
KwNJHBOJiBiqYQFHoH3wyXF7nw3l5dr7OTSpAt2A/SplGSYA6cKzvI3XcEZD3/5g
9IUQmkPXIZPWnBMigxBZX31d+R+RRwSIt5gDOzwFo82KnuHeoDtH0lOcaxXd3ocR
TucFUmr6
```

C.3.8.2. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-shy-legacy-reply
Message-ID: <smime-signed-enc-hp-shy-legacy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:19:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-shy-legacy@example>
References: <smime-signed-enc-hp-shy-legacy@example>
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-hp-shy-legacy-reply@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 15:19:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To: <smime-signed-enc-hp-shy-legacy@example>
HP-Outer: References: <smime-signed-enc-hp-shy-legacy@example>
Content-Type: text/plain; charset="utf-8";
 hp-legacy-display="1"; hp="cipher"

Subject: smime-signed-enc-hp-shy-legacy-reply
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:19:02 -0500

This is the
smime-signed-enc-hp-shy-legacy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from RFC 9788 with
the `hcp_shy` Header Confidentiality Policy with a "Legacy
Display" element.

--
Alice
alice@smime.example
```

C.3.9. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from RFC 9788 with the `hcp_baseline` Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 10035 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 6416 bytes
 ⇩(unwraps to)
  └┬ multipart/mixed 2054 bytes
   ├┬ multipart/alternative 1126 bytes
   │├─ text/plain 384 bytes
   │└─ text/html 479 bytes
   └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:09:02 -0500
User-Agent: Sample MUA Version 1.0

MIIc7AYJKoZIhvcNAQcDoIIc3TCCHNkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAGPIKUbO7uaza7TKuUY2av9QvGOrh+II70JF
jmfXtOq2FRJynyfRCzQtOTh9HmQiuv/0D8oNXyiyMvPZEXbXc2IECoErnn8dCN0j
fpq06OkYn/tpAsUDCLXiLPa581D574tMwb74AZ2AULbEv7TdNT2HtddFA3ZQntsl
8+WB6KiHvr3Q9Bwkf0tyj+fUvvm7MeIn+i6PmdlQjoYyBGzKsYj/dJXFfNM1YHC4
GNuHvUM8flg4r9yUb7QkjMmXksY5CUbVb+FGRy5tMa0qY8AHeM7eSYdu04rdgBaW
PUC8CP+QWU7lau/XoH6Gq9WTgE88fEZpdiaMPEsLXoc4eDuWRxEwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAOLJlujTXnL4l2INjDQAwOHzd
h2yJNC1q02iZ0VHyGxsA8Q0YTHjggbCB7Div5MxlAyAKZ0URNwDkPpkEmlM1l0P8
hH1N46zT740PBerrdR4+tCHoxExhwdwS7D/5gh/5FGZTx+TqLswH4UG9hyVT3fWF
f/bEXPTaTpm1SwUajnJVsBNwhNxzXUR4ANzCIJVStWsxRxCwv/U2v77oCZkmbpY5
yGz+BeLSx5hXl5PbL0AjYiVnMHPx1DeerBU/4fyxLRBiO+2LpouR+K7NjhmDh7JU
6DQabdXzyh97AF5uR1neBztOLx6VLbFh83XbeLBoRh46WsLrFP0HuggyCZV8+TCC
Gb4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEIYh3k6aQwiv/CB/9ZJiM1eAghmQ
WIC9ITS+o9nkZZyCWgZEmdcygI7lzgLRCP66EibaFTqKmbfPUbcSkzKz/yQgTYut
Y7KBMXLh1O66qhEK9HzUlShfQLtt5G/+FI+YcYwgWY3W50HHkGXtAVfFi6quVP5G
fuJEHx7yVl7KCgVSqvgG9S6inZPXDHONHEo0GhpKRvs0OLyVpR9NT7ToDIpLMihT
GwxKw8QtvmIPkp3cxt2zT8+6VZR+M0DsPkqKTZcP+yFd1ekvifdB+TEdx27YO96h
0oCJWxzkKYVqHYHBmI9Mn16p/I42BaHLqL4q9PxlAZlAxG030dHUrVHf3+z0nARC
rTJwolgsxtrAYJ288okEeZUgI4Ia3j7/vSXu51k1ZPgOiui0tw/rOxpHB/XStsJz
qC7Qnhi+FU1nw8icx9d9WzzhVFuY0QcmnvK1xoLuSdDYCVShUvh13punCT+k6/Zo
T2HGqqO39+NYfZBi8DhpefyXyRFT47YB1Xyi4JUa8/e8+9+JrJdzpcRflYPED7Bn
+tDz/OqQOGY9G7hNS+2BIXmIBK7QlKQo6L5wT29MjpQ5fCNh5m+lpCPPP48zi9z5
7duvKwRM+nBObxSFdFhpxr5A91n1OCnd3ptb5XNaIoNQ00COFM5CUYDTn6aHr30A
QK4xKaDX2ktEKwIVifziPtvlsIHEOBqawn1C/ABM7lW/7BRDRddzs21B1IOfS9aH
26bcy4vQw/+NSemAuREIOlhY9HAlDTgY29ogWot3zPE26TRD854eyi/ETKnh1x3t
GlxsDbEitSoykXpuBHncmZeFUyGO10zjCuzDwlMyf9D8zHARm+65Mx7ViKa3XPsv
8x7BK/OhYbqSSQDthDtL/El5icm9Sl/yCZijnVIldPqa3jmPM0QfEy3/Liea8UTS
ODaJ/tyJ3pV9SocZf7DBBXUhkHBb4fRrJKsK/sDFh1CGWFRL0AS+YhaH/qs0NNbA
```

```
9Lns6XbbSC/4iV2IJxoTuJoZ45+05f/q5ZGFgO62m8nvgMAQV/eK2glVa5/jWkwG
lMn6X4JT4wv+uqaAqJWm1Mlb+9gdbV7nM7VY6th10Qm8Cm1bQdvlx9d5MSkm2oK1
/LwSCnf4riZW437lCBucGpmmWcguoQvokf9jew2nzpBf+ED84hEtHX/IiAvzZlHI
T0IvB0jMXd3j2Rt6h7HuhxuBgTb6ZcTvOfoGZsxRMFZEz6niVCq5ob0GjfFO0RNb
v2jCLAQ0h4H9KkpUZxSTKNSypxXIBXyWylQm407WklCLZJb9qkXKWaHswoFGIYmX
VqpmNTsthLgou62KeVssCypiASBLo2fVbJwhkWVHiaqOc2KxYiFecesfyDe4S4Ux
/OluQCDbQKdSNoj/nDX7oFF+iTCCVFSnEr/6ihskWCjnWmYquOUqSYOzZv161F0Z
ajOU6WcUUVkycB6KuHPgzMQqMLbHFgJ8J4lkO9IMg3GYSZubZRq+XnwriAsnuZQX
lpNGh2EzZdjUUp2f7U/FFNZOCVAXinaxJVVuRszi/1lhjNs5D5ZbMZdfb1tWuZ9F
gSRdDvFsnAs2Z79cMD0fowSGefBHp/JmNctqZvGaknvOkwuees36nvxIe2R8Ggpi
HsrgyXWfsJMX47Acl2IHWmXdSBLWT+RG4yuiXvKQ2nXiwFWr1LgyAv7V4RX6oNKZ
YvnQbDx5QfjZuBnBRW1tg3RA6DfJaeacZJLXG/fTAB8Mfi9xMHLXOm0Wrbsjz9Ml
Rn7EjvH0sHlXvos0ayazwQppzynCn6O1MNxVqZpU2MSWanSshllLB76zqZHPNMd1
mM3Qy3w3q7aN/6pI2EPraFTtbNaMufQ7fTnxeLGs6pBgZjBqGl8AZ+w6Legs5AE9
k+tJpmZbaGGyhOW2d8GgYW347y6ZRfRdGv7uSwkvE0iaJt7//zLChnBBx6OVAzqd
fFztNGDShQtJ4Q+nx6uKt9D32kWFsvS6aDwviqWE1oBcStBSNzrDQApVvKUNksh6
P0ORT/hq9QQHM6WnRH55L35CQzyj2UTlQ7mIoZ6C4Iibavx9Ln81SnErr0IUVIyD
QGdAUYtvyvVcc1dgLSPlSw8AIr93BHs9tJ2r33gmpgQS1CZT1nMqjNj+H73A50Z8
lfri5Dz3fP8LT3RnSIfSaxaw6yYTOysL0P/3M5P0D5qFw58srJjq8Wp/NueZKWqH
+5vBpgaxn/pIy2xYSiSsP4o9jk9Yx8ptRBh2Sw3xeoyuLOsgzQzL9CqyncgAaGP4
W1aWsLziQkO2klzDSPaNo41S6w4320EiM7Txi2XJbsnmKq3ad6sv5yuC6sOSW620
ywMHL5PJxG+iFGuOLbeb9zgoxhDU2nvzjOApgZKrotf2Nq8d1K/x1taS1gQrUVnf
hS2M19ifp9ymmZqm0D/wKuvfnSkHkN8pizK9CrpaFzUxNk6X0d3+pqQUHQ4iPBJE
jizY5DUq5AECn1qNJ7/UONjnneZcQMNArfIXzYDyDPNWjs3uptM56AOS3fRP6U7g
lXFgyybC4oKlTo9k6Vx1VALOskWSrT+WtATUMcGXfD73EuqJVpjOOWp4ATiaqIsf
QiXuCB8fsbFxidjcm2tJ3A5k8NKMYTdBOYhEzHKDRk+rlk06xagghXird0fJ5rx0
cPzNvZTcSleLXKHQ8elHAo8NYF+dLaXIrxQoghAjZFqCp9Al8ksvoFUbXVVpaND5
5bRMaaCVMOPXscSORTD/UP95kDstpywBQVC4GjILK1bZ7n9lfKMRuT/3lqqJiW5j
FTId9wmeelCWSUtExyihpJBsBKro900+bTZHOp5Kai8YPjPxf5PNw9lFry9bPFXA
PbziUOVwYXj6EZMtzZFNu0dw9ddsyZw3ZO0RWHVErBMR6j50JkCyBCwbU4F4hcGs
KkyM34GQBrrtCdVWsq0t09rTzFXj/D/oeTegveQelRhAeNWkIl0z3HOV0c7HdM5Z
w5dYd0wlD4pBOJvLiR8B4/9HlSStyuVEeu9Df2qsXdbhnNrghY5KP+nPUOpJxyGe
G9NYxlylCc+b0jMW4gzMUOf+n7vux4ixKqsCfkG/5ju4dgnnJqAZX38dsrL/MaU4
Kfh8skm6ovp6RTBggxQ+js9tG5g+5Qee9y/uq+uKzGic2oOIz0LkXOwH9k70Sm44
d7jlzOsIRG3qeT5MnY/Teq/buX86kcjbK4h3G6u8haDt2QohCFOkQ5elffeZCUKk
/da/WyQNUv2ERmgtfZCnXzafOCnvkZayhBFfeo6rYlbt3S2kJgIjgfwgPuSl+wZu
XV/5URoKKK4RcVeY5pcqkUNjXhLTlMQXnC3Ahw3N+855qbqxsyeFTtS++Y1htM4x
H6Gu/fewKXFTiSyzhyOnVbpo5Hf8gEnITBiMa7Ji0jgscZ4YZyyt5X50misnSRYz
Mf5icnM0BKNddRTRzN5UQk82lKYYoqam2fMSWMTdW9SNvdSPy7B4uX42XVqCHz3u
5rS//1kasqSNmOeOhVxn+2Q3/5AaScU9c2MCu2rqc3Zy1eiVtUYPDkR28jDpGHue
M9UtHfOoysd0l65ihmG1sv8IEpPpVUq2qjIL5FI9Mk3IX3C4geYHf07+85oXV8f7
5QKlJ86eCdJ1DEzcN6MPOzOJ2DycRyPL1wSGBmiZ9x2PS/k1S3N3Qh8tWJ7KTzFR
od18MSEm4n20F01yWHX9fZfzlXH3NIJJTdw4lPUW73lxfrMeE4/j8OrtjQv28aIR
iHQ33hNVXoHaGO3Ws2iEZweYRiroUk7wJXBx+K9U8n9ZuvmaFErfX5uXGcsM9jxf
MbY2/DtDxqTBoxItK7s5cThwFm0tcFfM68JmyqunprH6A5iUikm0cY4Hkz2xSmbo
vW1DYK9/TQhhr/axl+jp1jr8pu1GXG0fbfAT+jc+WM2SJqwnrKgAvcLCMs3QeXe0
2piT0pIWG47aIrAjr5iFkJtBsc7HQEh99zhUTPE5rfISvr5xpPi1nhGTwG4PhGUW
ZSvBkwOcn5BjPqcBM4selB3B1fm4vVcy2Gq+wd1LPhiYSPw0nQrHWysxljkOBbmZ
ln/X/XoBb1/66MosPE5CVkoi5B2kpJCPMfAIuyQEqbH+RGPWLpcg8sP18oQU6HKl
MB13KYNEKOT3o0Yeq1OLEsc+wTmu+zkCJSajRtWX93TtLtjSo7oA5cSgyjvcFepL
tE0CvyS2XVwL7luU7cEbOsMtJRdtm3ZmbqTp+zgbJch10DIc8BN+EqkxOwL8iHuv
JRTv3gp6yeg3M/3jsz7HBMeVPqrrTWWaAMRd2vX+RfoxqPRD13N3A6quD61iXvi0
IYeStHLMsLKRFzLoxc5dpDgxXEqq4UoEsJbLilRqr68Db95zS+3sqAomgDela1fD
Gl3BzdH95Okw2fQuvuMTm5XBEymrsmFxbyslVb5nX3jKoM8IGHn0qiIDN1DoAu+i
CmJxQbDyJ1HcyI6HjTC8jfyp6DT/eEwnKzahiopMemQXBYDQ8tgVhm4IkM+t2gG2
enlGVK0lrubR2EZJ4HQa8adhNjGxf2MkzUfh1Effmy9OxpCvShnQ4xp/Y8JT5B2O
5SduazYH2llyjyP3CtRPa34fPPE/lym6aniPs0R+bRwG/ExVqhdzcNnp2QCJRVaf
hZB7ORvIx6qux5Hf3wdb3HaFqmpH7PH4Q/r+QPk8yE3xtLyjBShmYrx5NfRfBlr3
```

```
2HpjdBCtNlVmaR7yNy5TBORO5ihkMZ4nMXzcP/GJ3Ag4e6kmWZuHkUBo/pTmBBRa
u15Ybtz0emLNYjMiWgFgOXMXxZVpuMwiSmxVj3aJUjMSAp+F7uVlPOi4pCm2/4lY
dBDoU5xZ9nOrijdXm/YW0QFqwOKoMNFuwlx6KtGBMHUgxPeJUlN+oaUgnjomroGS
ZhoarruT7G1NyKSotBiaQkDSEkSWn0WnjcObCdedLGJqkYGeeadITiRWL+zxbDgG
XaRTHuiX13avTwapZPYfD81dXMq69RHfhNGr5rhU9eXMowKALeoT0uD1bzEQvg3M
r/YDtQE53Ysfe0ktAs5Vn5w5kgFMeHxb3B9DnZCE6DK1j9qU6G8/NGe8Ev0tihT6
XVbhFovfwN66igL6MNqm6pBqtIWImVAPeMp8C6VL9EkvcFLRUDSBo1HTPl85UPci
DgJTERFXiS9GmR7Rh9bO1JFjVwMW8DbNwimi+6LZiLA9GtcdRMFG8V4usHDV4OWz
Yv0cjLv94O3QmXZtvcUjBl716UIngAx0bLlZ/kvUh60xo4hkp+FSdnH+R6+XfDG2
44YVX0s5Bnd6xMaxc6Wm8FNlvDYTmkkqVmn2i7z8EaSuif/08VhNNP7sMFodG34y
yhmhtVW3fkod1G3CzeDKDVUuRLKOo79BTh4208GtNLOQmy6iUCxnjAbmgc7LIfzP
J2euFeMD3ysne9tVK3h9J12iBUHEvlpeYVew/BwcnbZgBenQO3PlqfNRxW9pBMQF
rtrv3zeov+H4l8QT8wnOthzTmDQUEu3BYsbyZ+mwKs9Dd31qNvZ/4oV0HBoYjfn7
ETMLy0cFi+L5wfjxHbfOOwgxlf1/cH4tc/0moxqFtsPDzt2kUzfrTPJjaxui1wz9
AFnAR2Vpww4xITn6nZo6UJe6BMAD2TNLMnvA5EFWNXJEoUzbvOQ8uJkfJhLEtCpE
Bwll8N0R7KDUWI39xzKGA9+j/A+s/00zGG5Vet3DdKWW/domeWo+d4rYmpKQDtrr
V0/Dp0rJJkJVItyuDl+0yEJe0mDDhHgffQIhx/Y6lD0KvE0yEG404z1OeGvHoVGX
aSv86D10a8IHVoJbXRtNMF525c4UP7VPh1l1wKD0sjzYkofaJvwPqZp/GSi8wSYo
pyVmrzIWfwDXYrqEIxFDLzXxcGW+L7gl5ntEqP/XLsda9DQFJSg2hTAfhhWgMOog
fmIhHUyOcEUtycb4RvQSM1Pkg5h+kHUmMMpUKuhF50Pgw3+UgxwG2J3CW1DKUQZd
j+cuO3J46b0o4/0eY8NoNqpWK6XksqSH0g1wVsyenFuugRsuESiSiZMTNmCqURSl
PPFUyeMtUgSQ23EDLV9T2RkaabSNmVG35jE0CQMOBaF7XU67reXpLsUqPg2yhQwn
EzX6KM4qioqC2wrqk2a1SdqRB8L8BEKykK2kv1bqvc0DNl9FoUxFt5uEH6iKHArK
SkjLaQZsRmzu+ueHRhTqcSHEKeVstq9jWc/heW4RhP3LQgD43CVc8m7yRqSaOkor
08Pc7O7++t7SDvYMsXFVmJ9MbB34HNgmXk5gTTb0AqI6fKyXEZCfJloUMbWWBsKU
mEGUu0YOmgK3hRCsXBugFIS6K4galFCx22U3hoByZoiVjLduQhRQNPC0mFk5aB+i
NwPL02YlB8rylvz3fV88GH9A1PrIEPJzCVsabxORVQeiJYCISJnvRn+PME02aqBh
7qOtTDOlTChfj7jBgMsDtgpytWEnObAsiL9+Rm4UsnHBbbpOMbn7rhZLyjEKkc8d
Ej/6LTuQGjIOdPEcfIU4LMFh3mZiWojhLtDXi8mEF/+m2BcX77fKgduM3KM1FXzw
Te4TnpIET18zeigaj5ie+BKmac2Jxmxa8sOlrmUP4KLD1kwF7bgTOsahZzkPHmBP
ykrogqTdmYUjkTyQvDzVUykI4PhnthaljLEYOj+LhZ0DSr0hhbsfM7OFUXqpPLeE
+tr2hGdj3YZOIJkfSYWH2DqtEeDlWDbhBfoaT7EbCFi0doFHsAz+BX2PlZJsIqJ2
BuA9mci9XB43ssokteKCqGT4QQn6KAekoEDZ96wHDTudcXIbYPdZIrD1xFHGjS1a
ZONl09Fa2IBuLnMhKuYQXoZwUUnXSI18Ga3Yt2ljCEcKeXmo/juIkt0b9UPTLBq8
r4kb/ExUJ0kUgqUGmL5rSZszWWYmxt1nzOJkEd3v4i7LUk+0mGIdlKOE0hqLSMn7
YVJwhiEqIPHu2PnnDUtqlDPVMGG8wCZfZnnzP/sDBm98/nIJRVXSEc15BYFtiUqf
cqGOgVAv81z40FFg6TlpOAGoZqXjk5It0plTwjWRR5RaoggYzL20DmL7Q054ogDI
5lEgMtbY3jvN6XAA2X3qPUsCwinlxaUMCJJsVEN8c9YkouvsbNG19eBRCpsC70+l
HMp5Ybh3ypJxSqHCn8zEa4KmJYsW+7Q8VQ4nCMekbhH7Z8l+5Mmw4/Y6+Wn3j+Zi
nl95bYnS0S/FF/QVI2CbZAn2IKlwmGVtIsv+XgGSlrPk6YvCgHurK9NhrRSlj/5/
ZbFWKUZmCPBbXwuFWP6yS0UBzTRCTaEGIZQTpNJawmoyHsRJm45Sxxq+q/0Gkieu
u4GD2XQsYZhBKL24NhEW2fMTrqHeuyiouQiOdKJlV21pCDo9cgqbd0Ikz5wx8Zxq
DKVP8yc+RXQHKj6PYnmAQDzsqtO+21rRCrT4zt9I9uhSIAoEhv8ue6TSnhhc0QbM
8aB588Ass35/PGIDRVpBdIEoDrjHx51oss9J0WGN5E0iVkDcwVRpuB2ttM7UmNv7
3lGG+Hji/FconVZjwkSEQ8KUZ1jss7Sx1Ji1Kyv02+aQ0VsTePkh5JJpJoRFPrck
dgjZyCnLl/VysqlGFcwKbop2QfgUqlB4ZWZMsnBT9ZmgkD9pUoS12DnX0PiFqT3+
x7YWr+z13W7br9amR57w7TYwdTB5dYCkfuLFC2th0nR7cHKPxAB5O9pbdtqTIVvB
QtNUy3DpqVpiAp8pAM67ElHjfP/WZrnP8SafvE5tLZtOvcvVF2fHnW4visb/VCSt
xKIKnhsqKJZ8gLZliL/zV6dQmvAVvWeAwsS2D2OUyHlvHKLWnA9fWVq6GsTC1wJ6
2El67XOVbGYPIHgbQ1PgMecWwaapHsmRu8Lh4z6nnv+H3vUG9R+rykvR+D7x8V0y
xXt9hoFbhfp6PaXLhFkEwAcaXE+w3bLyPrWS8rUv26zYL0KN96FeJTysT+/juML2
FQP706NRcsHaxoBp3jddqxdiGMxUJDOugh7zINNZwCryMq95j1jFP+JZFumD43Aj
tPfvfqv0vZ9RJiirxF08skjG14NNovMYs+jyaDv41/1MRt4TJq3Alu9Fwc5DibVy
KWKzf2XlvnYsXwiB7hLc9hv/QG/YTjJbNHoNSlhEP7fgNI5WYZhefmzzkrk1ueW5
IPfgwrQJSG68IpZOGb1r71n74YgtyxtkM8sVpklHz0l/mUFSoUczFLFc78nTjiR4
Zl54J+pfv6dXQp8KBIhDnyjg1pH2Uvg4Ie5YU5twJ0QufhBst7ookPbj4czYBTcZ
dha1mFjbVPTTqaMuZsiRSfMjMvE653QEWAG+bt9bODNFTk6/8ZFnmuLH6M3h56xs
LnAEOUs6ikIKwJON7AxVZ+YfG6WJpHbqelmC2V8MdBltN7kU70tm2KmE0SleadBW
```

```
3p8lzad1pvL/A+F+3ZzcVYqGV62ojnSOHb7iSEttZAlEmLVArtcVCcAqM5IWtjyT
Q+aazgaKMEVov9FY28UB3YOl+6SMPWq/r2jxJcTd2z1y3L9yXDLTLg/eIYZtPOVM
iqIkeQ04Lq7CNwQa1GXbIlYmUSqKra+588IQWG5dbCIctteTtY6iLsquK0Yu6ReP
Cs0IQnGrZ4W+Pp43CEZ2+UtNL775n0WgBF9T14U/toMd6+EwTth53KmKVQWdYJqO
F7NhRuOi3RGHQFHUv20RyOwHMRP3xsCWLpx301zLxKzzy5y81puzEaGcsZ9nbq/1
XGazzMVR4ksU8jkHPdw1nA==
```


C.3.9.1. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_baseline, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
```


```
MIISMwYJKoZIhvcNAQcCoIISJDCCEiACAQExDTALBglghkgBZQMEAgEwgghcBgkq
hkiG9w0BBwGggghNBIIISU1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUNCk1lc3NhZ2UtSUQ6IDxz
bWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmVAZXhhbXBsZT4NCkZy
b206IEFsaWNlIDxhbGljZUBzbWltZS5leGFtcGxlPg0KVG86IEJvYiA8Ym9iQHNt
aW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEyOjA5OjAyIC0w
NTAwDQpVc2VyLUFnZW50OiBTYW1wbGUgTVVBIFZlcnNpb24gMS4wDQpIUC1PdXRl
cjogU3ViamVjdDogWy4uLl0NCkhQLU91dGVyOg0KIE1lc3NhZ2UtSUQ6IDxzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmVAZXhhbXBsZT4NCkhQLU91
dGVyOiBGcm9tOiBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NCkhQLU91dGVy
OiBUbzogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4NCkhQLU91dGVyOiBEYXRlOiBT
YXQsIDIwIEZlYiAyMDIxIDEyOjA5OjAyIC0wNTAwDQpIUC1PdXRlcjogVXNlci1B
Z2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0KQ29udGVudC1UeXBlOiBtdWx0
aXBhcnQvbWl4ZWQ7IGJvdW5kYXJ5PSIzYTMiOyBocD0iY2lwaGVyIg0KDQotLTNh
Mw0KTUlNRS1WZXJzaW9uOiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L2Fs
dGVybmF0aXZlOyBib3VuZGFyeT0iZjMxIg0KDQotLWYzMQ0KQ29udGVudC1UeXBl
OiB0ZXh0L3BsYWluOyBjaGFyc2V0PSJ1cy1hc2NpaSINCk1JTUUtVmVyc2lvbjog
MS4wDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0DQoNClRoaXMgaXMg
dGhlDQpzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUNCm1lc3Nh
Z2UuDQoNClRoaXMgaXMgYSBzaWduZWQtYW5kLWVuY3J5cHRlZCBTL01JTUUgbWVz
c2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3BlZERhdGEgYXJvdW5kIHNpZ25lZERh
dGEuICBUaGUgcGF5bG9hZCBpcyBhIHdlbGwtZm9ybWVkCmF0dGFjaG1lbnQuIEl0IHVz
ZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBmcm9tIFJGQyA5Nzg4DQp3
aXRoIHRoZSBgaGNwX2Jhc2VsaW5lYCBIZWFkZXIgQ29uZmlkZW50aWFsaXR5IFBv
bGljeS4NCg0KLS0gDQpBbGljZQ0KYWxpY2VAc21pbWUuZXhhbXBsZQ0KLS1mMzEN
CkNvbnRlbnQtVHlwZTogdGV4dC9odG1sOyBjaGFyc2V0PSJ1cy1hc2NpaSINCk1J
TUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0
DQoNCjxodG1sPjxoZWFkPjx0aXRsZT48L3RpdGxlPjwvaGVhZD48Ym9keT4NCjxw
PlRoaXMgaXMgdGhlDQo8Yj5zbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFz
ZWxpbmU8L2I+DQptZXNzYWdlLjwvcD4NCjxwPlRoaXMgaXMgYSBzaWduZWQtYW5k
LWVuY3J5cHRlZCBTL01JTUUgbWVzc2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3Bl
ZERhdGEgYXJvdW5kIHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhIHdlbGwtZm9ybWVkCmF0dGFjaG1lbnQuIEl0IHVz
bmcNCmF0dGFjaG1lbnQuIEl0IHVzZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNj
aGVtZSBmcm9tIFJGQyA5Nzg4DQp3aXRoIHRoZSBgaGNwX2Jhc2VsaW5lYCBIZWFk
ZXIgQ29uZmlkZW50aWFsaXR5IFBvbGljeS48L3A+DQo8cD48dHQ+LS0gPGJyLz5B
bGljZTxici8+YWxpY2VAc21pbWUuZXhhbXBsZTwvdHQ+PC9wPjwvYm9keT48L2h0
bWw+DQotLWYzMS0tDQoNCi0tM2EzDQpDb250ZW50LVR5cGU6IGltYWdlL3BuZw0K
Q29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogYmFzZTY0DQpDb250ZW50LURpc3Bv
```

```
c2l0aW9uOiBpbmxpbmUNCg0KaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FBQUJRQUFB
QVVDQVlBQUFDTmlSME5BQUFBY0VsRVFWUjQydVZUT3hiQQ0KTUFnUzczOW5PM1Rw
UncyMGRxcGJmQVJRRWpPeXdpd1luQ3RrREtuYmNMazY2c3FsVCt6dDljaWRrRSs2
S3drWg0Kc2dyemZjcVZNcEwyam8wNDQ3Z1lEcGVBcmsrT25KSGtJaEFmVFBSaWNp
aEFmNVlKcnc3dmp2MFpXUldNL3VsaQ0KdmRQZjFRWjJrREQ5eHBwZDh3QUFBQUJK
UlU1RXJrSmdnZz09DQoNCi0tM2EzLS0NCqCCB6YwggPPMIICt6ADAgECAhMPLSW9
ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnelN41KImVaTC3D9zFCrS3i
4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs165ernT9
O5NLFflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZuTtMc1zy+
+MxQlqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCqlLqhBwDHdZ5qDTII
2PVX1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy6SCf58du
q/AOEksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBSAwHQYD
VR0OBBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCBSXignLEynBakDKU68ro0
RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9Ii6zyBZVjdaox644DsiL
OQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz53PYDBh4zE4Nar2inC0D+
VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eDOdu+F2MVtluLihne0B
p1GUTkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb744gqoeuD9YSHjKK49+qYC9f
aFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzlEc2tUpAr4vRhZjVD6FY
MIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpqp1zANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/
pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY63PQWl+DILs7GxVwX
urhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TCNO12DRVB
DpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtws1q7ktkNBR2w
ZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR+peC
rhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90njlsJLOwIDAQABo4Gv
MIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1Ud
EQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQw
DgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAf
BgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOC
AQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJOd64roA
KHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27PmhK
E1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahiXRn/C9cy31wbqN
sy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgkLD59fk4PGHnYxs1F
hdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+uCDgNG/D0
qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMAsGA1UEChMESUVU
RjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0Eg
Q2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJcOvT4as6aqdcwCwYJ
YIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkqhkiG9w0B
CQUxDxcNMjEwMjIwMTcwOTAyWjAvBgkqhkiG9w0BCQQxIgQg2xAxJLd5cNPk2o3i
Jrcgqk/WAtQzwmzkVadbd10R1gkwDQYJKoZIhvcNAQEBBQAEggEAWsHGjwENgVc0
GRVd3mp7i5QJPmYvHhAuma75gcRKwPleEQdka1P95xnNFTJiDmaMzf+5wDEuj27L
zgf7UffeIJns/d/xIGGXTuUR/IPvT1ROsY9dS74mzFHl5fY309iHtBLgaBjJ76WD
JQ+9To+vEIk/gFhx931G9fYBZ3i5wqMCcoG0UhYG2AXTNLfEDhW3+7Yz1leqS6NH
yCcfwEB8iLvLs9hIGoCbsczkgYPSbbQx82NzQjaEHOtXqLHXAn/c7a4zn8y6qV2k
o9ewCiLmqimEsacO9ZJYmi7XdwDolB50ylpcM45Mvn0n0WIjaLcU3Ooqw8LPQWS2
ybK5q4kRvQ==
```

C.3.9.2. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-baseline
Message-ID: <smime-signed-enc-complex-hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:09:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-complex-hp-baseline@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 12:09:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="3a3"; hp="cipher"

--3a3
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="f31"

--f31
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex-hp-baseline
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_baseline` Header Confidentiality Policy.

--
Alice
alice@smime.example
--f31
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex-hp-baseline</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_baseline` Header Confidentiality Policy.</p>
```

```
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--f31--

--3a3
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--3a3--
```

C.3.10. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from RFC 9788 with the `hcp_baseline` Header Confidentiality Policy with a "Legacy Display" element.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 10640 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 6870 bytes
 ⇩(unwraps to)
  └┬ multipart/mixed 2373 bytes
   ├┬ multipart/alternative 1423 bytes
   │├─ text/plain 480 bytes
   │└─ text/html 640 bytes
   └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:10:02 -0500
User-Agent: Sample MUA Version 1.0

MIIerAYJKoZIhvcNAQcDoIIenTCCHpkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAFzRRJ4ae2Mk8l1B7yZRDGmCK9wJNrPFJTno
34WR+wNG0/sDCZCYzBvpNXScUVbk/+Y90xyCKLXZYvP89rkPvPPEDjm0faAKPw7r
```

```
9CodT58+Zxc+mW50t1G/ERj0yLlMFa+yAvWjuAXuQ25+mZ1fB2TkMQ6pZPg38smk
Gtl3Dzqx31lCmB3JSYfBJQ3SCNOeRQzZENp9dpo0o4+wfxBCukVTGPexmnX9GIkL
9bfoTfqcOt9gPQBXKnOG/hg6vmEQN0avXjI71fCMUwj6nUr7Jmd5e5P9Js01/4Qa
jScrAk/JdFNixNiVarqYWEWiIeTRu8NidcW3L941Fb/3CSfcgR4wggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEABb5CqsgXnqKOQb8V12/4362F
J3hgPcMNbwO/59c8Fmn1ETL5R85beGapoHKD9hlejMVgyVPJucrSzVX458JBx7F8
Q2gcINWqe4i1Vul4vGwFPQVsyK5ufH7VnNYJ3rwaig1mc+3zb2NaF8rS41xnCHVD
0Fcl9lpsN3iQ4hqzUNKTupjVKmZJfIVvjdwwrTnqdSbovmCAFYe4b5h+lIPfGJ9p
RZNDWB4mZk+adxhK6qYxoAqzJE1HmF4NwJz0BKaknBPr9jWPa6Y6A+ap3Fn4OfYV
NXqRS0LSsqkT8D31CoSDbWsBH2SlVWHmOtSZvQfNh1jXDRfQFssgg4dOXiL+LDCC
G34GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEMGuYxUySDVL/ohXx2NMvHaAghtQ
poigIUJ21hyg0R0MwSilmOnxXu6RlAVjlj9LiS9iEfWStaxj1wv7I03AnTJDMpEn
4JUC6w+ZKkG1N7KF0viOCi1l/dIBCmBrUIBH6GTb1AVVlUI8NwnIR0Edv/RqlNSj
dViDiZerCe6EJeD0oirYPPjzofrD56glnYCetuDXFnMas2ECP7pu6YaB3MiuLO1G
McK9B5G5ior0BiAigYPpMW1dmufoOJFYX6F7v5+1ZrIlTOYvGGYU0WeOvM3mY1Js
49qkzg8l/6qc89+vlAMDa3f6P5Iv0g10/s37Yz3N8roT78C9ZegPC/85RgA2KY6t
U6wgGDllqgPUfg0Fd9yVd/konoBN4Nxik2YmM6mJTj73Ii3H2LFSWD9HRJjXwpda
JZqkCjWHOjbugF+z1wpLSFLznRxdgje5Q4BkQDSw7BJsm9a04EgRg/4IDZTXsY6e
zncUIslIJvf2dKCMzLzNA/KNBoSZPxvZo3MDIBr4z9Mp07I2jbtdM5OAQCbWwNGz
oUuu4p1NvUJDJoLae/w2j8v2RDpI7rss5hWLqmwEnJJNPMmR7PtqU5tL7kbonPjs
ew6t4aAN2AakJOjHBHV+ABtScANhCDacMa15/0MyS0CkxAIU9ydf4WHtvQlsu81i
4XXLgm8JYgu1znbsil+FSJtVIrsasEtHny5xJAHAlCwFCr10Wt9gqCv/t8tji5Xl
gKoxdtM2mp4zsXurP7BsKDXSA27QGVyuL2l6Oq7VHrwg2ex/7AB31qCP0hZni86K
Fk3O3ZxjjN3aZo7iXeN/IjaQDhmKEg4qaZ/Kfs+gGA31alBopZKL4UyFehX5Le/J
BbXPCFaXCxU1eztGqLA4BPSNSuDoUXzHMnvm/nRsuUF/d0YHsNp7iVORUVMj9JQP
891eNWch1R7OI2q5THAFJVLWwCCScO89vFeeFhZDJHMZ1EdZRP5hdE4pGOj11Om9
DGYIWjd59fN26eSbB8Eh0R72L/K8ziXIObxLd1pLy7F0ae/WyDKl5fykSTd581MB
UqRflyAiTn8lojH9b1svp2XXNVBNRDuCtJCjqd2VT5NqO0UNN5Hy9ojVyCyqTFZa
pwbyx3V5MCZfnZMtEr9A4y8e37ogWC6zm2Hg/3/mgapslPJsWBZHRqPaIhnytKDq
J3WlegHY6f4WF1XyTVOKZ98mjTytcwRZ+D5QwrNdULT3EYOeFGdBJ6Ao11+2EDZh
0vMVjdxfLAXxIyZ3srdqf1jFoLnAqsmJMolWBT4eX1379SQK4UULoGVIUOrjsCd1
YK7vKED3e502hQc1IKHFD79OTg2VssER5QTLXkxHvoLXzL35fif9gZN0K5WEin6K
aBHSMcFzT2sFtESHpzs3Kl2FlEUBnxA4QfvmiFcvH212yUAvnwczoH69w3+xaaqW
mmOqMpNRMxMap1j1lLI9lzGG4bp4sHNPd/t4uN/RPjq71+f6HNjbJsu+My0bNTIc
zfmwTlsg8zN8L1biu0U1Nfn79XY01xsLpJqFYGoYUiTuY0SBPz77LT3BE6j2OsLp
H8NhlJVlrfBeYWdJJnwkGbElwbQwI9eDkjxf38oUv79Az7NFcg3VLtuUgr4VWdBv
6e4vEwamNB36hEtHZuTL7tPuv9mSZD4wzK+sPHxrVyw7Qvnln0PDmzS8Bs2l1dQI
RIi7/oN7bLJ8YUZwALukzJ919wuiCYjfJg43l5Gvhwh1PBZ4mHNUsU6/EUmmm+rC
ULCIyQqAY0CAzjO70EeI96JOZHh9Yh06ZOdh2iNGaZmQ6QRCIzlEiikKPKK6euhf
RtzTM2pFQNu+BUj+vB7rQ8aGD2snw72kD175+Mup85Ac7VJiJU25mR8ojNgnku3x
tPRvU0z+/bWw/l2RhRfvNUy7Eh4CTB1jixlabRWHQFgs69cLrPly4kJxIR0yw1/Y
7l01or7cL2mFwRzoBJVcu+/pVr9DKya2E65ZrmitUUBF/QWUBEzc78adBHQcT2Ih
2bkfB/E7I7KVQd1p7n7eo95RnVtS0WbwFHcXkr3cK5PzJAOQwGi9sj3CSk6cHrzU
GSi5iGA51V5MAo38pYJdhBPPzAHsD1PLRYcFP8McjBTuBT30xKE6BO8voV/9NsAk
a0OuhpABP1GwQl1l84a8mECVCHkfPge/HJ8T1d9my+Ra8jYakMIWiudd9a2q4/hQ
VzL5Lp2TjAqO9IWbpPZvT0GFej+4KCb5nfW4vgqGwRc3XSX1PNsrDpfrFPUyQjdQ
mAcfjK+kYYBaYgsTYZBaZxOOoCqs5BbstQ+Ibs2M3IPqDaPhY5pZ/cWiDtMGRliy
y6yyM2B4oLUdXJH7wbjIlUeG2Zip56QmFbiob4s3v8w2iOfPaP69+tIeGZSCdpky
nqKWZejZetqwhdbiXIapD3+CsKNmmJHDTnwWqr/kRzatdDIYICZtf+WGLGoIo2tx
g+y4N57sn+CZLEnI7wKwZYcPTSXsWrsdA7+h9EZT8FIagdesKx7B59SNXPQO/7EG
qzH1ko+s4NbuyZJbyiXvEVmD5bNQ7w2VrvOtZMekQa4CtDusF0zjStqHSZTJ16J7
785dMVo8xO/72VlP805jokuTJNGTYddY+Jh5FbotALz6qtrQiQQ0xRqv1oKlcC71
X/dsH+xzBFvPCq19dn2zEcgrJuLyu4Ojmy5jLGfg33xVMYEMNVaiNd45SU/cEbDX
rBxtsKJs/e3zmKqi7siJ/GvAIVGrVQzMOT1iZvJyQ/OUZMFh1vUbvBTFAY8e7LjA
wbVB9PD4VdtwjPZdeXkGylCjskNUmlTGi4hO4mKnOFbuLxOFMTDrU73RE58tsdqk
MI1Z7AnhyyTRWUj6s+jBoXtRXwWZgvGb1Ro4CZ6EC1c5Z6DFFcy5ICgI52r+Pz6x
```

```
cdINTvTgPedoDqDXv+5kPy1+EyT5/pFzRfp+eIzZmfnzXvrUzXSK2UEyxVxvJe+t
eS+jmBFNhvkzZQ10UcCsdKjhgDc42dR+N1gNUem5UXvsMV8JGv6rcK+AoXgIA6lB
Aby/E5dXc1YT5CJLs9NRGidWXW6ltJgoYORM/97GVNJeQRa758t+7A0rV/CaHJlg
HR8pjTnelOCQT99BmYknS2NhG0XrZsT4/rtCsUvJRrR3bPyd6M868jWmW443w0Fx
AYkvOQW2J7GDHjJRwJqhK2tDhTpl9Mtuv1Uv75UuPSP+sxcncjz4mGYR/A4vkjFD
WlZLDXH4RcS405llTQPI6Tf9ii0C5qFTVqj1yZUVnYAE49nqqXVFaRH7b+z68VMq
D61ThDEMvALeMNrMOuPK6czLqu7jpwbAFaJGsjrFAgfQ8C0VE1+ZcjWM9uP43msH
2CNaqPKu6rhZgbhNtlTMSzISOhJeTCK5LT7rGcOOCLDnM9yqosAZ/3Txq0xw5pKX
OtUsaCvyXOH1WGk0IJGA0W5k7Q/tV5zBuddtt8rVj8WbmV659SLU3TTZkGOp6SeA
FsoN3/w71djAYPJtNhHPqB+TICv7rs2JhhHbHvrHU16L6118UgSM2TUtxZEQ5CXd
CFGvyOzap2VHbUyiSdE9mGzvOLrnhR1IarQDYy6Raxha+5Efd87bhpCdluiT4oSw
8zsq2q00Yv9XyGDBgpZPRtZC2GJDyarXvnHWtqVvFoOHHyNk8GrOWfthhR7uINuP
xopCfRl7ijnBhVSjC/cdxpE4KItJkp5CkkRLxuy7polGvxzB1Y8EP62iyhP9Oz4o
AW6jwfvYaAa9bjX+B+QZYKjYZiKXbdu55h1WMGXng9yDhQONyQMPbCMprfu4tLr7
Tv/bFEak1TOahNORfVzioWE/Flig3JotDqB6wJE2EmXtjH426cn4orFNyai0fF47
PsoiGdUJvjKfWVe1X+71AD9+xe46JyJyrnvLY2y1gjYljVKFe4rhLfrCwU91xFoD
svrzv7LMSSJhuCdvcPq9OS6fw97upSYVlUWt4KIRtDOi1vxJpeR49VppMY4EXNpS
6+6mv2g4SWIfPCSw8C42q+sO6KUmqmCMcdXx37mrBy9DT1EjAbrq17WyVPmMQz9v
ehaCSiAAOZCXC2sX3pC6N6o2d56Z6tdFbPSgMBOFW1vuHUlMUtOkCXuxIjtucF/v
/vZVmtSATOv+tpDqcB2tWg5a6vq1/EHXV29XsSZ/Hty/1j/Gt4oirtmmajAVMevu
Upk9+WaDwWtJ44cWEOLnw5d1aiSupG1Xt2Qpo+QtSLFtYSoalZRenOvZcdEqMEMg
1ufw2oTq5uwGdoVbQP+CjdOhnbaIjqArj0BXMZ2dcxcluy0txz4kyRn72DvcpTiY
UaPFchqerEJ41wTAD5xeM6vfLpnUjnhHTuY8Z2muYlIAspCHaSuQbGbCvtkLsFVE
gM4U7W7xM37XoM5UNnuY5CROkBs4+RpKC9WxjL9b1u2mHSmHWg4h+bUNSG/OQvM4
jq58X2QVYE0MsHeCgUS+dWAaSsvi01YpeuWkf9LSH30jqrclgCM9cbrkpodCSrYr
xp7YJpa2OhUAB7zobQXNBavpxgOJSniV/NmTYSe+7B7qNPX6Hm3rq2ETH03JvWol
GOCcWlmhJfxwIKK2ddAasxiZ5h9+rOjE4YDxXOSFCUoTtHZvOAES+5MT5g0ZwMjK
tkmSx7uqngBbnYeo3lsnUIQXuwjbjymeD4sXNcGEFAB23EpJ6ewzdpX8NsNj4agp
Ubtj3qoXs+gvQjmAj9dI2AKhRuhpBAj4kb0CQyFLO8LJjnipsFI5Bjsxh4Ntc80W
w51Zb8QCaSEZlARJ0T7L6g/kjUd0q/cviMb5zCUdA2hq7m8zL8MhTIpehZgq2MIe
Fqc7nY5YyvKZDkIQF9Jza6bN/8HRSJLS2rYehVDOja6QOR5xVsV7EYoEvorBxg+e
4MutPpSDEgQFqGkFQuaKKT2cOIfv1j9FMyv55o+/puAebsnEBLOqeXGVY/1PWc2D
1YNQ0E0o1fQeSvvqdCOc54vbU1zsnOGdgcna0w6VgN93aNFmifAcUVoCG/QVGmfg
3yPGQh0/t2RjX2Df3b/oie0Vr37m7Wc9fTmlwPuaiB4WhBgzbkAnNKan5eFu2OrE
9NnaXTBGJPMRQ8/aNafl78a8L55rFRDJJ3d0MGdq8/Km+1u1P+ckJ0yZtX3ini58
D8q0o19JS8D6r8OFPyYpGbM4xA+EovnWiA8udN/C3VXfTPflOsIzQ7BxoiFKZJJ8
etGlINGRftBrCuP+sp5TfhfF/9wzLvryCT0wBXbWsqe9+rOuU4OyzSF5OX9tX/BZ
DrVrIn9lo2t5a5KVYz8gLJvTCDvjdLdE2wWAX5wnmqXZSvoN8vjC1rxOLpJaHH73
fNh2POpbonAfVj0eWXsdI3AH1nC+AsS2rDQguURUH6i/pFJM3iT23vBkFDVK1s46
SXrYIeUx0LNqoDlJak4hD7DV6JROMJ2CnXbMe1K8VUXNla80yoh2juCU33PG9DU3
3DN2pUMwUIO1p4hYatx6k2m+bB2cJhncW9ApK/seF4XvvS3HmWZ7yBZVv2OmgzOH
Swz4pIoLhJ7sHXUTRFdkF59D8Jho65gmGaoK+EJqtNZU9hPxRcHMw2yKW027oVw1
XCBATnASxDifgA5wIqtP4aK9fRPPI4zJu4voqK/qe40DVpjDF/4xnacbmB70q5X9
wgIiBWeZW9Yiu2Ssk2u6s0nfb+JpfqK6IniAtLtct2LUlcOh6uiWQq+B26UgG+Ik
EDKVriy7HEuzaaM2m4lmUy0bay1On3et+sdmbSg0oQOy0GQBP+TOUZl72y4FNGnq
edg8Dhd2rlIfKn8RHs52FudiEhbtxHfmKIapvj+SDPqN4FzpnUtrk8ul5t7ASdr+
XdOLqp0uAXlK3kDqEZc4eVmBKeQjet7aNb3goEEnbu6AxUbeB/8GQbv5aNeQUP0Z
/NPxh0rhtPRGkM7x/LgFw/nCqW7QU2fPQf/6jJE5/CpXUgo0ZuT3HZriSLFoIqfS
3iOls8MS3WhsaodETFNyLbalwyFvMqS64KlP+yWbCVm/G93ermWj4uoLZ3Jhbx/t
jPs1mKxGBXu8JhUrqOsBwMv58qTVYyNPKgxssPGohTdGiC9Du3nhEqj5vUVRfGDp
nD2IaQ8O/ugsIr3XIsaXU8p8QbORKaWAbmz3B5pt2vGRa36lyM/pirNUse6h8Xb8
KC2pHottzkt66qWz3Q+sbRjexeJdL/0qjx82QyPaDAfwT+A+8utjBrSy8rvHwFco
NYCfKhzq6SYnUSmo36p1wZae+CSP+ls+1zN3uPtXEzar81ULsvVYn5Sj6+sgZaoP
w5ROqExM8MFua/aab+kMjIVU6DYcAm4r+E4tv0P1Pf6FKstFSdVDCGVhHkmlpFu7
/lcjcXbOlcpMoGLkC0CdDoiScJ0D29jMaO8Fc0ifq6PCiJuAHKowqJS2H+VnUwoO
wdwPLiKDim6dSCzAVatzM2/SRB6mso4LjwCzGEukOChkbbDinC9+UoG6tV8xdovK
rx0i4ZZfkwiQd7P+cGs/CMdDYk+DYPWJi6w3n4MNvlLMkSTce+C99n/7CEAPU7Po
mizN5Us4y3bQ42pXJMZbPriedEplEAoTBcw90FZ8qvxuTfkZuyb75roe6lm4S7on
```

```
F/sn4T0YednconxhGorshMLRZ0aDQDwf602+8Nm3qyEY5gLfbe0JjdBnPomLo0rg
nYCi6MLwns0T9QhMQfAR6JOp3fHQ6rMe6ih9su73qqmsIkRrly4nSJL8LwhFdV8d
qPoEMFeKb+tnFmi7SOaT6m0oZRErа1iyiwpZPqkhA15LvcCDq1zcK3pd6M44hg+H
uk4SZ0aBGRY+WReNsmYDIT3WnS9uKJpMSx6pCWa4hhcmnOsp8xwZK1UEEKzNEc+O
ky+/WoYQlajv9vjRsQ8mVP2o3hpjAJg0HcvVn6BsJYS0fZykAZh8tA/MBGBzkmNj
Pm3awY31MM3MVhtFQmQtjIZYzsKKxLWb8k1N6bSs9tKFuZx0+FZSRvjwA6mSg6YK
BNHiZ3W4nf4HSc1EwhgHemDU//n30xAIvX8oSFf6YuxtPj6PZ8elBVvNYHflesLW
0S3o/nQVSEukU1z1aZUB70lnejzvGC5EEvnTHeohRrjHP88R0oz6K7HgsCw2GVS9
XT0XTjwIwmX7Q3rifjVxrju6sdmyTywLlwPWPMHFZbNWZMoaZdr1f2p6HoUJrIkK
Opk9QD34KpaH56pG0qJ3NxcsjF0AttISbfljn2FE7t/N6AXjwOWFKfMZyIMm/iSE
Yp1Jp7HKxw3owdFmB41P2FBHT/eehbfgLozSG/bhVj7pEuaY0XozKDu+0OqRxg+i
UJCfcngZP4nP5D6pG2ll3sFM+i37A2tGrGlGescgQk/SgWrnkDm+FZjIG9vLJMG4
/wBjVRqF639bUrc8qrhx/jRPxkgg4Ly7+UW3mwUnr3Erf3p6ZL1//Nd7f5BC8Rcc
YXY3dR+gAMpAFE62akhotTGVqUxcVU76KxI9geFg3e8pMHJ1ycygoM1b9Gt98IvB
59nId0bbvOm4iLuzs3cSsdboDlS/tWMqcETzrpIOqaqydrbTkwxGGv0/3vAV19+v
lFy9IQ8Z2mUF+S2CgJ9bTzTXh2QqIIugoBYT3TpUlq+Tbl9oFH3FBej1J3EKaxW8
s0mKvro8GmNxR2sbhBL1LnzLWs6vAstngAZmPlj1mYcbgNU998+27/+5Iln9IZ6X
/jrQhWtuKg2QgQV0gtraDqz6/lMGKeUidjg2C1IKXo/m87hJWFSj9TMr+/2K2OMr
XReM5ER2YFKsGqCNFkiTkl+T3SPw6qynf3S7lxtxmys8zOu7f/JFILKZarfWRyIE
2qyOWmBfu6/sEuVMGOWLpHbpGevp+SMT8J6187NH1NGO29jmGO9rjh4f0B8ZSmJW
FFnwQm1PalAzCPGxlgVbbERuRZ6tnPTFIBCpE4I/9d/lNbHeKgZRjhK9jsk2Fc7v
QCdpedO1qwysKFmC0otrromr6mTzEZepedKYuB1TDuZMBTwIQNWf4oGiBZlQ03z+
VuXgWhgWZJxspGZ8CgYBi9CoTgsu/fkjq0n+rd9LrlRhoLPR/iVdhtSvHp1u/BYf
OL9a2cqXRQfIze+cJfD2Ler8h627aW59SA8g566CSxPVw/GvO2Rk2mm/PCwep6lX
gpWu81riycD6VFUnSCDrw0aqpNfhNOBnx4bNqvGM2msMTJ46BgGv7gMHoUzjracz
tsP5Y8qS17FsxptAmPjP5GpFihHQv3JO2XgbaAudsKGMAf/bUZf5djDhmzZxWqrr
TW+abp6gKjktu1Ug2zYl9JYanABpb8/9oYI1AattVoAokUjlWca02bGqeMRpBtwj
oo5E22qyEkRIhfoHrWLoUg/bt2vEjKAdbe/Xp7zb1Mf6MDksa5/IIMhB1l6y0yV4
JKeRvxji3t7bNaYzTCtAcLMQRAoqrp/B97emRVQSx21ALE7puVLezZHTPDscyz7c
hijAssGK+6cb180XGxtM3VSZg3R8tGiETu6nFhTB4ojh7CG+szqAkWKupBPxOUkO
l5zIkutYJLpFhCbQ4cj6cF1faug6POMcww7iBkqRCU2Y0c4QcQ9z706+t67Sj3oy
g62KUvdvEiA+lm3MSTJASj76mi1hi1rdTNU2pdfT4JIzPAMI6RDN0Jike6Y/Vr7z
wuHcGe8inCjn0+14A5sdgRouC0v5tkId04pRewc3eUixnVvzsXTp1jvbMcCxTHYG
rM1GsyxHiB3j47De343GLJo3JUxt+X8e/Xfs/dwDbTppYa8J67/w74YRRvgGq/A2
/c/lyk/JOkuZcbnKGJa8UsflyXfEhbFDnA6ogWRxBHYTsOs27Du95SvrZwk4GL3j
pW4KkX80gGTY857dMJm8OEuxZbVDjhAyBgnC+pq4m4AyfIOzFcXKHSb6e581n0jE
Z07Agv5hPcO9phCHyn3pIE9snR0Jwn7vlGaMrv6uv6DDwWIx52yNrucgYCi3WRxc
XIwOTYWaGhkFJ/HDHd2gCmVbSsZPTEaU9IXxmvScOpfCl7sUe5baRYR5X4VS5Oh3
jNpFO5YYLwvN5CAnPRXa6vlKWZzyq34vgQhsHHiJJq40GdyKV0ODlWE6ZoyGenxE
rV0yLodGch/JAzig28oODwnw4D3IsCbu5hCVQLy6unZsxwWRjMT0onfFrnoO5ttl
XYq5LHaxkJKF9aBzSi/AcNWao3wEXVyKTT1P2DQcGCmVz+6fsR1AE22e094tULy4
mSAC10R8byELoQs+W4i8GdND86fG+mRQKoR8fYsrOF1CZpLXDFG4AnmiaBF5Ro7C
X20oNkEZ4yhYoiSOTp/yfWOphJ9iDxfXO0RVHSrO2Aw=
```

C.3.10.1. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIITfQYJKoZIhvcNAQcCoIITbjCCE2oCAQExDTALBglghkgBZQMEAgEwggmmBgkq
hkiG9w0BBwGgggmXBIIJk01JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUtbGVnYWN5DQpNZXNzYWdl
```

```
LUlEOg0KIDxzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUtbGVn
YWN5QGV4YW1wbGU+DQpGcm9tOiBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4N
ClRvOiBCb2IgPGJvYkBzbWltZS5leGFtcGxlPg0KRGF0ZTogU2F0LCAyMCBGZWIg
MjAyMSAxMjoxMDowMiAtMDUwMA0KVXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJz
aW9uIDEuMA0KSFAtT3V0ZXI6IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcjogTWVz
c2FnZS1JRDoNCiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5l
LWxlZ2FjeUBleGFtcGxlPg0KSFAtT3V0ZXI6IEZyb206IEFsaWNlIDxhbGljZUBz
bWltZS5leGFtcGxlPg0KSFAtT3V0ZXI6IFRvOiBCb2IgPGJvYkBzbWltZS5leGFt
cGxlPg0KSFAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTI6MTA6MDIg
LTA1MDANCkhQLU91dGVyOiBVc2VyLUFnZW50OiBTYW1wbGUgTVVBIFZlcnNpb24g
MS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9taXhlZDsgYm91bmRhcnk9IjNj
NSI7IGhwPSJjaXBoZXIiDQoNCi0tM2M1DQpNSU1FLVZlcnNpb246IDEuMA0KQ29u
dGVudC1UeXBlOiBtdWx0aXBhcnQvYWx0ZXJuYXRpdmU7IGJvdW5kYXJ5PSJhZjMi
DQoNCi0tYWYzDQpNSU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1UcmFuc2Zlci1F
bmNvZGluZzogN2JpdA0KQ29udGVudC1UeXBlOiB0ZXh0L3BsYWluOyBjaGFyc2V0
PSJ1cy1hc2NpaSI7DQogaHAtbGVnYWN5LWRpc3BsYXk9IjEiDQoNClN1YmplY3Q6
IHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1iYXNlbGluZS1sZWdhY3kNCg0K
VGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1iYXNlbGlu
ZS1sZWdhY3kNCm1lc3NhZ2UuDQoNClRoaXMgaXMgYSBzaWduZWQtYW5kLWVuY3J5
cHRlZCBTL01JTUUgbWVzc2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3BlZERhdGEg
YXJvdW5kIHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhDQptdWx0aXBhcnQv
YWx0ZXJuYXRpdmUgbWVzc2FnZSB3aXRoIGFuIGlubGluZSBpbWFnZS9wbmcNCmF0
dGFjaG1lbnQuIEl0IHVzZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBm
cm9tIFJGQyA5Nzg4DQp3aXRoIHRoZSBgaGNwX2Jhc2VsaW5lYCBIZWFkZXIgQ29u
ZmlkZW50aWFsaXR5IFBvbGljeSB3aXRoIGENCiJMZWdhY3kgRGlzcGxheSIgZWxl
bWVudC4NCg0KLS0gDQpBbGljZQ0KYWxpY2VAc21pbWUuZXhhbXBsZQ0KLS1hZjMN
Ck1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3
Yml0DQpDb250ZW50LVR5cGU6IHRleHQvaHRtbDsgY2hhcnNldD0idXMtYXNjaWki
Ow0KIGhwLWxlZ2FjeS1kaXNwbGF5PSIxIg0KDQo8aHRtbD48aGVhZD48dGl0bGU+
PC90aXRsZT48L2hlYWQ+PGJvZHk+DQo8ZGl2IGNsYXNzPSJoZWFkZXItcHJvdGVj
dGlvbi1sZWdhY3ktZGlzcGxheSI+DQo8cHJlPg0KU3ViamVjdDogc21pbWUtc2ln
bmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5lLWxlZ2FjeQ0KPC9wcmU+DQo8L2Rp
dj48cD5UaGlzIGlzIHRoZQ0KPGI+c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhw
LWJhc2VsaW5lLWxlZ2FjeTwvYj4NCm1lc3NhZ2UuPC9wPg0KPHA+VGhpcyBpcyBh
IHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBtZXNzYWdlIHVzaW5nIFBLQ1Mj
Nw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVkRGF0YS4gIFRoZSBwYXlsb2Fk
IGlzIGENCm11bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5s
aW5lIGltYWdlL3BuZw0KYXR0YWNobWVudC4gSXQgdXNlcyB0aGUgSGVhZGVyIFBy
b3RlY3Rpb24gc2NoZW1lIGZyb20gUkZDIDk3ODgNCndpdGggdGhlIGBoY3BfYmFz
ZWxpbmVgIEhlYWRlciBDb25maWRlbnRpYWxpdHkgUG9saWN5IHdpdGggYQ0KIkxl
Z2FjeSBEaXNwbGF5IiBlbGVtZW50LjwvcD4NCjxwPjxwPjx0dD4tLSA8YnI+QWxpY2U8
YnI+YWxpY2VAc21pbWUuZXhhbXBsZTwvdHQ+PC9wPjwvYm9keT48L2h0bWw+DQot
LWFmMy0tDQoNCi0tM2M1DQpDb250ZW50LVR5cGU6IGltYWdlL3BuZw0KQ29udGVu
dC1UcmFuc2Zlci1FbmNvZGluZzogYmFzZTY0DQpDb250ZW50LURpc3Bvc2l0aW9u
OiBpbmxpbmUNCg0KaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FBQUJRQUFBQVVDQVlB
QUFDTmlSME5BQUFBY0VsRVFWUjQydVZUT3hiQQ0KTUFnUzczOW5PM1RwUncyMGRx
cGJmQVJRWpPeXdpd1luQ3RrREtuYmNMazY2c3FsVCt6dDljaWRrRSs2S3drWg0K
c2dyemZjcVZNcEwyam8wNDQ3Z1lEcGVBcmsrT25KSGtJaEFmVFBSaWNpaEFmNVlK
cnc3dmp2MFpXUldNL3VsaQ0KdmRQZjFRWjJrREQ5eHBwZDh3QUFBQUJKUlU1RXJr
SmdnZz09DQoNCi0tM2M1LS0NCqCCB6YwggPPMIICt6ADAgECAhMPLSW9ETmXSs5C
VIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYxETAPBgNV
BAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmlj
YXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4
WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUGA1UEAxMO
QWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCa
lSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnelN41KImVaTC3D9zFCrS3i4Pa9ZgHy
A5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs165ernT9O5NLFflH
UjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZuTtMc1zy++MxQlqdn
```

```
9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCqlLqhBwDHdZ5qDTII2PVX1X3K
7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy6SCf58duq/AOEksC
AWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAE
EDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUuZXhhbXBs
ZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBSAwHQYDVR0OBBYE
FKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYa
ZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCBSXignLEynBakDKU68ro0RsyXWAPk
fXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9Ii6zyBZVjdaox644DsiLOQEP4YMS
7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz53PYDBh4zE4Nar2inC0D+VM6RGDy6
6K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eDOdu+F2MVtluLihne0Bp1GUTkr0
mJBolg6dSYal8Hw8/ANHpyExl56BJABb744gqoeuD9YSHjKK49+qYC9faFmQ+mK8
0lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzlEc2tUpAr4vRhZjVD6FYMIIDzzCC
AregAwIBAgITN0EFee11f0Kpolw69Phqzpqp1zANBgkqhkiG9w0BAQ0FADBVMQ0w
CwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxl
IExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAwNjU0
MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8GA1UECxMI
TEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/pdO/KLpZ
bJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY63PQWl+DILs7GxVwXurhYdZla
V5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TCNO12DRVBDpbP4JFD
9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtws1q7ktkNBR2wZX5ICjec
F1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR+peCrhJZwLSe
wbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90njlsJLOwIDAQABo4GvMIGsMAwG
A1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWB
E2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0P
AQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAfBgNVHSME
GDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAc4mi
NqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJOd64roAKHAp+c28
4VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27PmhKE1oAJKKh
DbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahiXRn/C9cy31wbqNsy9x0fjP
Qg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgkLD59fk4PGHnYxs1FhdO6zZk9
E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+uCDgNG/D0qyTbY4fg
KieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlm
aWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJcOvT4as6aqdcwCwYJYIZIAWUD
BAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkqhkiG9w0BCQUxDxcN
MjEwMjIwMTcxMDAyWjAvBgkqhkiG9w0BCQQxIgQgFPMLhnhgVYfwoQAWNtNbXfp6
/cWw0vajQObfIM2N1+0wDQYJKoZIhvcNAQEBBQAEggEADBKPOlAhmQvuL9r8u9eh
4V7q50gjztxHMFw2kcppxXNAEoy6iQ9LeHjSXSmVNIsNyD34OfqIWUOztwbva/xC
+qOC/4GwaG4nvqCmyT2FfN19X+2XHgaLtlgUSE5JhYifHm2cfFGH4YObujre1NS+
tZubVHdqf/Stlr1vFhpBYcsu0ZInwbeVbUJBMYd2iqG5sE702eQpMPeSdh4C1CB8
W+1n0eMlPiea/V2SZC3WCTpErF7llbYdc6jLAWsOeT8tlJ+DhfgBccCppbsCw2nlW
yAxju5U8wojwW5qTVdVdlerenMLyzVmaxnVKZU5b5PPq8WV27JVzEZtG9YUTZV3T
8g==
```

C.3.10.2. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-baseline-legacy
Message-ID:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
```

```
Date: Sat, 20 Feb 2021 12:10:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 12:10:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="3c5"; hp="cipher"

--3c5
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="af3"

--af3
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset="us-ascii";
 hp-legacy-display="1"

Subject: smime-signed-enc-complex-hp-baseline-legacy

This is the
smime-signed-enc-complex-hp-baseline-legacy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_baseline` Header Confidentiality Policy with a
"Legacy Display" element.

--
Alice
alice@smime.example
--af3
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/html; charset="us-ascii";
 hp-legacy-display="1"

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>
Subject: smime-signed-enc-complex-hp-baseline-legacy
</pre>
</div><p>This is the
<b>smime-signed-enc-complex-hp-baseline-legacy</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_baseline` Header Confidentiality Policy with a
"Legacy Display" element.</p>
<p><tt>-- <br>Alice<br>alice@smime.example</tt></p></body></html>
```

```
--af3--

--3c5
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--3c5--
```

C.3.11. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_shy

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from RFC 9788 with the `hcp_shy` Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 9945 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 6346 bytes
 ⇩(unwraps to)
  └┬ multipart/mixed 2005 bytes
   ├┬ multipart/alternative 1106 bytes
   │├─ text/plain 374 bytes
   │└─ text/html 469 bytes
   └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-shy@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 17:12:02 +0000
User-Agent: Sample MUA Version 1.0

MIIcrAYJKoZIhvcNAQcDoIIcnTCCHJkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAEYCnMa5cAMGlFedd4M7eVuZRV3TQlSwv6zq
HizrFLVHcw2IQIXHK5qbN2Gei2g4nukYK9jX/nlfLZcKwB2iyG3737Ga9ioiW3WG
9tJdD7gCDmqmuXW7uOfY2Y2czyJfxwygJ9rcYVF9J6bdq5yXxiuPCpIQEYZY2d6O
HZKvDTHpCbDksSrj7YHAc7vzWFSGDvJ3qZ0Pax0782/oPI4e0I7IhpSJyi0kSJyw
```

```
4ibrBeMXcSokx6wn80hdJK3gb2txJIbAIKCQ4cdTTsni5kYZ1eU+si0eXLLADGoQ
g1dcw0Lcniv/iElqQEeIqitEjrgcMOGa+7NfUt8pl2ql3/SgyGgwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAdhLP26FYAU8560yDWy0tAg0k
r9TR3H8R9QxKI604FXSK3bmOXqq7mWT58NTkquiB4ZEycB+eC44YS3CpPq0oUxlv
KO1x9vjGq8ksFQwaZ+CRLlK+pJWPOkcfLd2m3vYbj5arKGNdJe+cqqxoX+GXJlY3
7TUYptqU7VRj/oe7IfawjmORo8PUtcftFmNNTrd+ohS01RTw+czmu8OS4SDEVQZf
mgLFHTVqj0BfTGUJDqA917N04GYBRXSYUVL3oNjBBRRS3aWTRZYUW9lp8XRl3LJQ
berrHomKqkY1aLBn6m6bY9/RkyACqmcsar5HuinbuNS+v7WNuQKeFgWPDDdiNTCC
GX4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEDkYoCBUV2kALKjvqgmyJIeAghlQ
4G3n7gBTsLWMtbnseEYMFqoVDK2AtaC6iq1AEi7qVHvCueAQQzmiFDD39N13w6+W
MnMkUG9BSN3Bpt99HaHITGsfnzkD+Cv17da/1WfWPIDI8yClA2OzUKOTdyBUvrBz
wZKrCMrfzGQEgzcsjzHTP7aHezlCKU7aNc3GIvY6V+y7OYARPAD+xlsdNEBLdO/r
iZCtxCe5RaK2DBQxu4wOCHiWHGBx5wl2iR7uPHi+dXyhRYb4PKh/8uxBo0WzBYmt
kNdkYIcNeK1u7lHFCzD8S5Il/wB9jAJK4BnzKz0Z5aISDtrsIeOv4khtJB54KVf9
Ho829bIUYuPX77MWyoR8ce/+HD0xXxrorm6f9qIk4chBTC2m1AVDtTiRvPWG4eCA
NQfg47pEwgz3cVeGCHExyGwVVl3BsOZ3azeh2IXM26oqOCrxeEmYcuK5Kletg8e+
iNecpmOUBcNtBB3ivdG1kUvlSeBmF3NIkDup3G75lFMuCQUUYmMTOofzMA1pcKMq
jPaQmzydKZhe2UrhYtr6Xzqxnj+WBli2iLX3VDBaQHWCUI6NgB5P3vS+3/qRUc7E
1PjQ1jzwwfmNCZQQBGrzfAdqMCAJEqgaWj0VNrQ2O8pRecynNqavlpO5pn4K2Jjr
nIV4xmillWypRkAT2cl+Vow+DeN+HImKhZPN/kRQvs6iRx0OuZ0uTe6wE+F4LoyV
REg0O4lJQeUnATzXIyHz/QENOnmkMa+k8OQYI+FihUkFIOLzvQw3CBG4vmO3sei3
mxCb0Ciy6GCVMXxk3BzeaUMifd8YeAfwO9aNHnVsZ5oEzTEfIGUuVt8P3UA+83j/
VXyogQznyhlvnu81J2cj8k0qfH+yyIqAqEDjx1a3toNRcutfdCGURuIGbbF6p7l5
rWE3rgPOYvyDGkRx6CdvnCUG/kiOX3XSP/e1R6QUO8+NR9ZfgMwBHmnfBgD24RGW
ucLTRaKwD5tQrPxp0KnKrdoQ5qTcfWEYirBtYzI/cDsONkmt55fL/efSdVsUZZ6W
oThl95axTiOrW+EeZkkOhYFFWGaPV1ZhJbyzYgFHjumLlSMB2dENEo1XtjHwlggM
+RhIMxfTcWr5bk34VxtbgGCcszTGPJpUZhf+lSIvVoIeyVN7YQ+VT2JsgDd2oikl
Z5YZ/pS7z1oIDas2cgguRuAHyz3WUT9heB5+fjx1Uw14K4iFRq+RBwFulCOqCBgx
YUnEwj2C4c62qloS7kfLQU95Z/q265wbf1sYl+ZHwdYby4UPcvcqXgGCwSGZTJvD
xMHXmfkKB596UAlXefx1qb5tdlJdss18fXMwCrmbb4O/XxcOzoa8eeNs7urHP7jY
fNLEjpyAD/soGAdJcxP6o1IqItjXtZqPCRnRE1QSqU3RaLQngI+B1QSM8lJjsQx9
qZMVznL+ROEUbAAdVR83oDpbA9qi9Xq07QLOcoUekYLdND0Pup+zPgjQ39fDtJLA
+loFvZGrTUhTQi9On1d4ZrdJziTwBw/l3lVuFjvBfVbYeGhdsVyQgxP1MHlGiBA2
DdHcD3EE0MRoiqgV9rqwspp4ar2OqOc/kVvh3VcA6fTASYL/d5254WWnxq9sc2HR
0GH79c/4fdjmEPvE5iwc3USMWsVO2/2dOjNurBWdPRqHIkSSVSnf9xkRfWFY2p7U
DTSzkQOKQ/3mG06ke2nV33tna4EnVB8tZaL0bcoUXwGtclkCxCMftHikU8M4tbay
RA9bzhse0/WVHqtDWeoQvifls/IkdYmlRCHRcc3wDCi5VVaX9BOpCDKaFxfatb40
RTBfSYSoeFaUkhTjPBEoZUPuE6qXWGMvS4tbTuqGK7u8WAkVC71lc3zqisz2q7Vs
qBJxqnIZRFbJuxRuOlIoQPEUPsNJgTqOAtWzWcFQwG6hJ9CBR4uQRVmr1bRJsik3
jSvcVjbLeTTINDxRRVtPa9preDrr494Nykt7+5D2qhGh+CiAQME9P+Wbf0fwhotn
M/1X/GGPmT5XZA27ia1OJ3+/MRLqP1m3dR5VXDRZBtXqxPiB72aP6TsXLcSdlky+
n3mmEB4aplUu+F9ZKDgDXImP3cFSqqqMkkOKNKi/J0omabZfXOnAx/vYOtjjSl6K
KJc/j7/bo5q75WaiRUzVbFc8RmnDCVF0ceICrATgHAtsbDBD1BM2SC72w63Ic6rg
TNy4wecyaQeyP5qJFeMLENGA73a2xPCFh4Xg3RgyxLR3xUJ+1NJO7iE8EF7T2peH
AzL6+3ZAfKg0Q9uoxr748cs9p5s8r3RAaaFAjk8ZVrn2mljrOqMatAfIQ9TY7+Vh
AMpfa4PFLcm1bHlIeRD4g0jdJ4ozJlDHrb/xAyW+IIwlm7W7AirdNldCw8B7rdmy
NbiYtlEd99MsmKOK1fpYmke0i4BVsFFGaj9OuAynIBl0yUaSQ284l9ejaTUlQ+YJ
FeJjDZ1o1WBbFb6j1LuZ9k3vDye55ZphlykGo31f1LtSmZ8daBHp64h2f+BrylRv
cHdszK1TwhBg2TCVM9+MJ4jplf/ls8pSVtoHZQUVJkm1T7lm/tA6CPSRvCjjtuR6
3YwTHOvx6NfQr0vr7LSaG0sSBugTgMepBja2uh6qR2QkJaCQgFeUFEjDtPzkQ9k4
UZTm0u4g+FW61XN6T/BFC7euKLXzhI6htv1foyWcOSEO0+wz3vRYXVmsYOotVHSe
iK7TA/oUSyu+dADbShFimJ295RZIALW3nMx2H/f6amg+n8NA9uEn33er74g+JRbA
OE78tRz/190+ub4v0lspkb3osm1Wf5TKVFKpCbQpTEac422pjpBeO4iekCkW+qJB
v1s2kd45S9Fke+s5o6d+lapwL4finUNOiga6yh70vjm2l7MxGtS1D6ZnsLPFgb7Y
uSUMeNJ5UvSwrM/uOReWmZUX7pETCt28U+3dqnR44VYJ15M2CpWgB2IxoLph0D8G
exKvxXFYpF3xS8w7cmHpYsBkiaAWMfQvYop+huEdQLNtFT4QfVLOtxVkJKZXS781
```

```
0ylhG9Zl25+c/mwJj7+i5OOQz5Idl3yeqrtTbk0P4Olo9Q274ZlkeonxfWcI4qeQ
Zc8vswWpCbyHneoYrhMREexO02ikGYuK0fYhGfySTaYbQPDX6+altrboUmXoCIth
13vbZ3KD/2JMKvctah/2Cb/2ZeQimCrvYtehTlJiwl0qkS3AcSTHlp/5juh3oxVn
eQpFKYo3chZ9s6xd6Nsae71rpZ24olpkZtAbrEC78ao0gmULuxvXgzzll984KclC
aTYoSbk+ayOEORUgrvEwJEWf6MP1wRIcx1b9r+GBjtogYvJrLFJ7OZDpkigkLKYd
nWrztRgvfWpn5S77S/ZFPUK8Ija8G8zBdOz61Bhbl5tLBOTedDiC5NMVUGAVknHl
R5PtQE2NkVe/kfvn7w/Vy7AnyDIkepsI4rZUIbXqkId8xUKq1Y+r6BgaSqtztXu0
aUnr5qKU2K9F6/2AM9mZPo0VhBJU5qWiMZeev53vKGvrXCd7PodPWg0CKOMP4f9X
fBl+HlsKkdOgcMMiiazq/xoG0OThczQhpARNXaMDxzZmrO9K4+tG5NxVVlF7INfZ
ADFunqox8hpk2HW2sas/8wQ3FqoGU774go1g7ldkBed2vOETee211rXDyf7DIiTH
g1/Ty20q+qc33dR8fVgLRB4wZbuKiwb7mvOaUDXQCHxMK26w9uS/7OmQGoOTJs+R
jxGhy7sL20fn8LlCLLRm/RKcc1EPIWR2pFi/dvbUHLCYcqtl6EAwtUSXXXJ3q7NH
si4VPnVxjF6b/iKaBuWsXzGmSfws5PmriK3JfXK9N8SippZwwdhqGX3JavUoFH6F
swEWrsWTGnalU6l9B1/yYTrlB3+XDFtkGuBULENI/BJoXPA50BZpkvOF6d2Q2CRY
aUFGIFthgqnMLJJYozxmblkM6f2teCwgw1zD1Hs6emQ5Bf6eBOiNnvFHYA/wT2c6
yBoXiGjJ9HOrxuKGpoD6LekD2dAzSzZVkla5IwnzfCd8Nby2260LJP4TAxZvkVne
1cK+/Hsa9fNvR9rh4VprQpKTcqLH7TXAy9HayqCpeggbMbxRbXGsxgC/szMjKHoF
qjrfU17kXdo5hp4LowHlpl0+4FsSYXvl/zFRNFUSj/EyTrfwPGcC2WPY8JaPLYxM
KUjeKKlvH3PQ0QDgeU/0GoCTwekBa2mwfwdGtQfmNPeP/usTiWN5K5ymeeLbgwbE
JNtN+QqZynBqUAuVBv8JOyHv8SzCgEWLK0WEK3zQUrj79lQ62p5sFSd5fWpOv4tg
e9n65e9O1yyu/olkhEW+yc4SKz/V42knHifYIfVGsQ9Gjq26m578QAn4wtylNKWf
4m7bg8jLP87k0eDB5Lkr+bzFiO9UdYYE2sSO/Cn/WCeU0UNaOsDRB0tGA2bJVDcW
5GhHt/qR7OzOc/h5HR7JIY/JR2ekN43juTCsPypLfZthgUbHTxWj9H9/3rQNfniX
lIooLIDXTi/MotzcZwFqMVyQhzd9jgHOY4dOlET77rpGHJv69UmjwHYqfoeiDdz7
OWHXTCDelVKT6IFlqxjpfrh/EUWjBUE1/Dzx4/ZQIoLieOYvqMaELjjedwOpEoIx
hcK1rsvBDiU7XR9VTvA7VTI1egqmculyeBON/d+MlPtylFYRZtw9m7837EMPuAwD
JawBJdw1M8DaznEiLm8K1PKH0MqQHjXnXSgQz9BjX6JBaQZYEMyaH3XtS0LMN/As
Ga1DIS5VMxCFPNkP3IJKEz9+JeQpUKA06uYxcHIQEaIr171wJ55JbxJnQef0klSN
xFNZbJ8HrMp7ebfsezsX0qL86HpmAqamzJblXjpBWdujxF7haTG5JJOvfDWVAIeo
2L1JJxn4PlvwHQ8aCFDfdhtSGUm0ht3dAdcdxvKSBXtn51b6vr8Jk4GEX7Qt4MZN
Q6ioS/i77KNflKUcGsH7Vs7g8L+d5Gix9yuGln39tUF6NvdKeCpeLIJR0wq7BiD5
FViBa/K4dymxQl+3zXcgvCZ4f07LOHMTkwONtyXKxmx3/NgOgsXEE5o0ynFp36wO
/bfA4t0gHQF/t0XjF9QwNYNcL9Zl/ih440TuElOsIAiWGp/dUYVfHGtx7iri7ZwB
eOWV8An9oy6w3U/6d5gZhWOLU1tL8h2LiXqFOLFMMT9F+3ozCyxEFSIg+8lmrUqG
D6Y0XX7Fzb29bsaSqYAzBAHJw5XWgqFSI/tnbR3ciitWNGj1bBUzjzRzoUKumW/o
Zt3MvbdtFwxM+lzRQyYoNZi8or/qQWls1pF4GNdTUKDROJvOzyLP3b59Eo3tLUPm
IH9f2dX3XnDCncAf1zmtyXy+dIJcO2FD6Jzz8E9G2bMNR/6zB9u1r+pYDAjJnmi+
V1W7vfw5jPFT1xWKype4RiYXa6uSV0wl9QvEz1GNnwXeC1P7ZDALQ36v1v7pmDSm
OldaIZQdbCONLwWjZnLMB67OR0r6AbiTn1k/CgLGTJ+GQ8TsmZ/eAKPo00miDKaH
ggRpeofpLOSk69vJtgXYkaWh1YdaadHW1t6SWMy2CRe2HHIZ9g7jxDKOC5lgpDlo
FP1CRmJe3ZcCWFUYrabiEJtyL9NCw+jcjBejA2sM/CWEEkx/dEOwZFCu51U92dgz
jGoHPlpiMqHAQYL2xt3xbZfc1Z/O93Wv2huB2/eu8J3bk1+BSLENr63NUwK+PbK6
tcCF5jtrDsLowOnAYeXdj0EnxaV9LwequsKiVJxfik2H1QGed7MRYC8Tx4aCrqx5
pdMNm78438mie5/PgRpQ8AJJ78A4AWHaOOXbg/sWUXF1bBgSj+mcdyAEmbJUZ0zM
v++vJw33nNmum2hoUfgfq8SvPT5LizVnzzuN/Xd36+I1W0dsWVMBwgTH9m0IrGKI
K4Ddx1AlntqZCCeFetwP1Jpec3X7HW9GVUTIjMel3TbCOgNt/qmd6GxKHZGfN0v+
iqm9icPZjHfoWkh2NXbHEA1qjiiXl9bmYdKBX7pBrlukr6sEc0nknQiU1aCFzbD0
Z92j40Q5ZGAFZqFIeHXGRR5tlOQXeA9r1xdnKocsC8mAnXRzLIyqgW1y0IxoGZ9A
wMXTSsG97A+JvqZYOjQFqFNJNEpIkmYmQbEIwkTu+xuUJ7X4Z3trCc2AzdPsBh/s
w70m7dm8++WmQXYfWRxEy67fqCRte8OQFuhOzBksVeEdisdWcAtoft3pX/Qwr4vf
/M7HR+av5lUvDsNtXA2tjK/SFfHN4VkZf+jyuzb/U8zAM+WixSAachsLIDxYVCaJ
q9E/OU8XbDOUDIhlGxA1NcktIaDrYdGwTYb5rQEmekzbjk6Fm6lCW4IlefBKd5dR
GUx64ootY21qqxJCUiffYQtLBi/tZVbIJpsLH8zn5OoRNMkkwGNprkNQpOM3NaQl
+HlICbPfPHv6FygLYU26SaBt8fCsBSIvGSKmvOMRVHuIeuavoqhj/K1z2avC7R72
5PaUJMitj+8fE6iAVkxV6vqh3EqKcF4570J77pp0j71PR3D8VQkn93qkLfWLJIgN
Z9DGCnlWfcRLaG3MjKait9PikUosTeA3XSA4tdDyF/AaaDUSfbqseFQuOW15lz8h
EhiR1wMlwcRkanCGxpJdYW3wfCrv3nNMa2Ehzw1fxoBXqrUKbtY+/3LjUAy3DmeF
3YjunYL5Ij+6Jvvs1vDnmleE5DRsU0Qsygfjuwmds JZ3JXUD2fRaZJLNqc1s4im6
```

```
R++Mh1jrmRrazBsgTWanqdxPLwRAq9V3JyjxjU/wAirCX5pCAXzAHIiFHdJnlliD
21SPK2RPbrJ/G64KMLAWK8r4SfbmfiifOCJH+8F/YLiKB2W1oHNdaF4MagvgKzIy
bYDy85kUGgaRy6IhCgp4gqd8Of4N3YHQhhQkl4/vYHEzaaBZMTU5TU+q7jzSDH0w
T2UoXjO5wlJgZy6UYCAOzN1wY0M89OYU7pUXacjNaXUEhajY2zSHIKZva/lTW1Ug
1111xYHLqZ/93d68Jb75nszdbLcwnHtyUuMtiQVSVyXzIYgmTjjRZ8WLeS1rIku/
a3y1HLT+3m383l8p8S5HKwAEehz1zhxN7Oy/A/sFYZ/iQyDkBivOoyHTkM2596uC
GdrrSfrGw0aFGyi5Zk3QxKwhunul/0rZcrFu9VPYr5UrBcB3TQC2hCc0MyfLaDxB
Lo3JaKr1K7dfeBoyAXKSSv6K7eUYpWP0GBEmmLeb3xHMEQInpwYBuDgFX4dOzNck
wYUOukJHh6TJeX+FynigAs91Ai1sNgwKVEQ7MZKv12MPfScL2IXs238oDxOO9zAH
zXNjf4iLH7fYj8k97/8CLLFncbdoGKaR1yItKcxjTxSkXtimZk5uY6yQqnyV7mf6
JHKCQ6Nvgq8NWAVUOkLeRrifhRHy1AjFMpp7o/AuWy5mvx92LhYB+uWfRhoBZWee
fmw4xcQCe5+Sp+Z3XP5r4c+h5rXXaGdmXFNb72eOEY7AOabo9gi1Vj4LgJPLg7L7
qDYpcz8FCeSgIQ6iSttk6Lhg0AZ2cv7fcMWQcO3cjTU8HgRET4doy2AznzP9G3a4
jYKuQoElzfjYycYR06qCoyCCCw0IF2LfmwxF3XUbIMjEwvI0iiK/epN6izO3mxMx
Zf4MmRMe6p+XallW3R3AozDJuUWw1GoQ/tokMN/HNK8sE3v8Jf39xQAf6uTA6qAt
Y5BpK1lXCRyYg0YLUIhBRz0zSkBA94GGK687z6PSDVlkY/pqGFhThTcR0h1lbbvO
eOT+9xqi9WckQqEVPklD76g8x2xNxw+AYObCjvPYNCfK4q0RAKm7Js7OFhpJS9px
Ns2vGaZ7y3w6f7AFa3KSbyiYmbW3nj8g9Ew0yNEDM/3C/mGEQWfYk8Ay3QH/TynW
ogsx3K1kn1+LY4WpaUiZjYVXKNNVE8+eiyykZ06P+fcOTZak42ARyO2+q6H/yXoV
s6C+H4xPHdq2WE7z0BrC4dmL5ihnQ3tPhfU2gU7+sYI4q0uUpuVNOs2yHzwMbAeC
TctqNj7ZEDdz/D7uYhdJFEbBYxi86pBCWtOCuaEckRQuqgy6lYGcyoFkxJMhEDKL
hj3I9t3dqwaIWTKITodE8AL89Vc1GSu6SDPQKrHj6hlDPtXhIrh1uF35C9uwKNUI
01JDhzsbX7yjIVdF7FI2sKCJWb/OARZ5sm9F5sOn8c0+ZVBvOpA2m5j0BA8mP+Jt
XcGg7SerRK6wxxkyFyF0DMcyrHs++Gr+8lY+RrPCbZYDWOsCib4nqqb70htn2bcg
C4EO+40JuW4MpLrxtIjMkQPjmynj9REM6qkJwOveYbEtJyaIaaHo/ZJ7mCaTP0xD
2ha5HLtyw458elqQEDy/JcMiS35az5arnYr1jF1ceqGyuaKYwwlKwB9+Mr9gzvKA
fqwNhON1LL0u/RjnvmVoahWqTreTg6lTEYxx3K9ufl66QFkIP0lQP7sHjQy5ksd3
xPEgMKw15xgyB+k7QuZoQi8QMjMxnmI1ecc7itvO9yG8YKAIkI87O0hVtNwYkSat
xPc2w/eJlU2EiVYo5V2c35zQagOjZ/1qSkXOZU1hPifl5V7LD8hr1wpJMJkrk+of
rrjZ1VE1bios7wIFyB8g2Imk9c84Rk8k6SjUYa82mkjkvHytn0SSq48aPsJXiHw6
```

C.3.11.1. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_shy, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIISAAYJKoZIhvcNAQcCoIIR8TCCEe0CAQExDTALBglghkgBZQMEAgEwgggpBgkq
hkiG9w0BBwGggggaBIIIFk1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5DQpNZXNzYWdlUlEOiA8c21pbWUt
c2lnbmVkLWVuYy1jb21wbGV4LWhwLXNoeUBleGFtcGxlPg0KRnJvbTogQWxpY2Ug
PGFsaWNlQHNtaW1lLmV4YW1wbGU+DQpUbzogQm9iIDxib2JAc21pbWUuZXhhbXBs
ZT4NCkRhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTI6MTI6MDIgLTA1MDANClVzZXIt
QWdlbnQ6IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjANCkhQLU91dGVyOiBTdWJqZWN0
OiBbLi4uXQ0KSFAtT3V0ZXI6IE1lc3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtZW5j
LWNvbXBsZXgtaHAtc2h5QGV4YW1wbGU+DQpIUC1PdXRlcjogRnJvbTogYWxpY2VA
c21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6IFRvOiBib2JAc21pbWUuZXhhbXBsZQ0K
SFAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTc6MTI6MDIgKzAwMDAN
CkhQLU91dGVyOiBVc2VyLUFnZW50OiBTYW1wbGUgTVVBIFZlcnNpb24gMS4wDQpD
b250ZW50LVR5cGU6IG11bHRpcGFydC9taXhlZDsgYm91bmRhcnk9ImViNCI7IGhw
PSJjaXBoZXIiDQoNCi0tZWI0DQpNSU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1U
eXBlOiBtdWx0aXBhcnQvYWx0ZXJuYXRpdmU7IGJvdW5kYXJ5PSJhYWIiDQoNCi0t
YWFiDQpDb250ZW50LVR5cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InVzLWFzY2lp
```

```
Ig0KTUlNRS1WZXJzaW9uOiAxLjANCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6
IDdiaXQNCg0KVGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1o
cC1zaHkNCm1lc3NhZ2UuDQoNClRoaXMgaXMgYSBzaWduZWQtYW5kLWVuY3J5cHRl
ZCBTL01JTUUgbWVzc2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3BlZERhdGEgYXJv
dW5kIHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhDQptdWx0aXBhcnQvYWx0
ZXJuYXRpdmUgbWVzc2FnZSB3aXRoIGFuIGlubGluZSBpbWFnZS9wbmcNCmF0dGFj
aG1lbnQuIEl0IHVzZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBmcm9t
IFJGQyA5Nzg4DQp3aXRoIHRoZSBgaGNwX3NoeWAgSGVhZGVyIENvbmZpZGVudGlh
bGl0eSBQb2xpY3kuDQoNCi0tIA0KQWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUN
Ci0tYWFiDQpDb250ZW50LVR5cGU6IHRleHQvaHRtbDsgY2hhcnNldD0idXMtYXNj
aWkiDQpNSU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGlu
ZzogN2JpdA0KDQo8aHRtbD48aGVhZD48dGl0bGU+PC90aXRsZT48L2hlYWQ+PGJv
ZHk+DQo8cD5UaGlzIGlzIHRoZQ0KPGI+c21pbWUtc2lnbmVkLWVuY1jb21wbGV4
LWhwLXNoeTwvYj4NCm1lc3NhZ2UuPC9wPg0KPHA+VGhpcyBpcyBhIHNpZ25lZC1h
bmQtZW5jcnlwdGVkIFMvTUlNRSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxv
cGVkRGF0YSBhcm91bmQgc2lnbmVkRGF0YS4gIFRoZSBwYXlsb2FkIGlzIGENCm11
bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5lIGltYWdl
L3BuZw0KYXR0YWNobWVudC4gSXQgdXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24g
c2NoZW1lIGZyb20gUkZDIDk3ODgNCndpdGggdGhlIGBoY3Bfc2h5YCBIZWFkZXIg
Q29uZmlkZW50aWFsaXR5IFBvbGljeS48L3A+PGJyLz5BbGlj
ZTxici8+YWxpY2VAc21pbWUuZXhhbXBsZTwvdHQ+PC90aXRsZT48L2hlYWQ+PGJv
DQotLWFhYi0tDQoNCi0tZWI0DQpDb250ZW50LVR5cGU6IGltYWdlL3BuZw0KQ29u
dGVudC1UcmFuc2Zlci1FbmNvZGluZzogYmFzZTY0DQpDb250ZW50LURpc3Bvc2l0
aW9uOiBpbmxpbmUNCg0KaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FBQUJRQUFBQVVD
QVlBQUFDTmlSME5BQUFBY0VsRVFWUjQydVZUT3hiQQ0KTUFnUzczOW5PM1RwUncy
MGRxcGJmQVJRRWpPeXdpd1luQ3RrREtuYmNMazY2c3FsVCt6dDljaWRrRSs2S3dr
Wg0Kc2dyemZjcVZNcEwyam8wNDQ3Z1lEcGVBcmsrT25KSGtJaEFmVFBSaWNpaEFm
NVlKcnc3dmp2MFpXUldNL3VsaQ0KdmRQZjFRWjJrREQ5eHBwZDh3QUFBQUJKUlU1
RXJrSmdnZz09DQoNCi0tZWI0LS0NCqCCB6YwggPPMIICt6ADAgECAhMPLSW9ETmX
Ss5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYxETAP
BgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1
NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUGA1UE
AxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnelN41KImVaTC3D9zFCrS3i4Pa9
ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs165ernT9O5NL
FflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZuTtMc1zy++MxQ
lqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCqlLqhBwDHdZ5qDTII2PVX
1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy6SCf58duq/AO
EksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNV
HSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUuZXhh
bXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBSAwHQYDVR0O
BBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEwjnwHFwyn8Qko
ZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCBSXignLEynBakDKU68ro0RsyX
WAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9Ii6zyBZVjdaox644DsiLOQEP
4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz53PYDBh4zE4Nar2inC0D+VM6R
GDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eDOdu+F2MVtluLihne0Bp1GU
Tkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb744gqoeuD9YSHjKK49+qYC9faFmQ
+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzlEc2tUpAr4vRhZjVD6FYMIID
zzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpqp1zANBgkqhkiG9w0BAQ0FADBV
MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2Ft
cGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAw
NjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8GA1UE
CxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/pdO/
KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY63PQWl+DILs7GxVwXurhY
dZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TCNO12DRVBDpbP
4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtws1q7ktkNBR2wZX5I
```

```
CjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR+peCrhJZ
wLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90njlsJLOwIDAQABo4GvMIGs
MAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQX
MBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYD
VR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAfBgNV
HSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEA
c4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJOd64roAKHAp
+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27PmhKE1oA
JKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahiXRn/C9cy31wbqNsy9x
0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgkLD59fk4PGHnYxs1FhdO6
zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+uCDgNG/D0qyTb
Y4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMAsGA1UEChMESUVURjER
MA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2Vy
dGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJcOvT4as6aqdcwCwYJYIZI
AWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkqhkiG9w0BCQUx
DxcNMjEwMjIwMTcxMjAyWjAvBgkqhkiG9w0BCQQxIgQg//G1y8IBZR2ZHaxvjng5
wsDzqScPZmGqfXdsuHb7bBYwDQYJKoZIhvcNAQEBBQAEggEAgNAXRpWDJX8taLEv
apUOax4C3CeJQgG2loke7SrgSqmJrNeCSuu80jFOxNY9YGiz8jUKOfk5lBiiO8p8
bq5MpX8NraGtWaL79iK++2nZ4D0D4C4VXYi6lVEio8cvChUS/HURa8ehtmOxwHFK
q0+Qw5OA0LvYNNu62oThBLdJzfbirxlQL+q5/xLndvEZkz1ljmiATIEtJ1vvsEdG
0vXeLi0Ppa8M50VOVpzK6DQ2Ay7Gu2ebfq99jLY22Cfe3GHab/WrUeJZ7mFmaqBG
WM5HN/DtOsBA0zgDBSymieKaXbzfFAzNcgm441xlPMWCWH1ceqgzrq20KHTts6yv
pm6/ag==
```

C.3.11.2. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_shy, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-shy
Message-ID: <smime-signed-enc-complex-hp-shy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:12:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-complex-hp-shy@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 17:12:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="eb4"; hp="cipher"

--eb4
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="aab"

--aab
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex-hp-shy
message.
```

```
This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_shy` Header Confidentiality Policy.

--
Alice
alice@smime.example
--aab
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex-hp-shy</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_shy` Header Confidentiality Policy.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--aab--

--eb4
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--eb4--
```

C.3.12. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_shy (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from RFC 9788 with the `hcp_shy` Header Confidentiality Policy with a "Legacy Display" element.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 10945 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 7084 bytes
 ⇩(unwraps to)
  └┬ multipart/mixed 2525 bytes
   ├┬ multipart/alternative 1605 bytes
   │├─ text/plain 568 bytes
   │└─ text/html 740 bytes
   └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-shy-legacy@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 17:13:02 +0000
User-Agent: Sample MUA Version 1.0

MIIfjAYJKoZIhvcNAQcDoIIffTCCH3kCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAEBXJpGHO8AJVfwKb9Juhai3fwEaeyt576LQ
wqs5p3GhRIBPkKrkjOmtlZbO46vl1BvR6FkjXzBpMTkD+atUlAgwcR6v904kwV/J
8Lab/rxrhuyIYWXtip9z1gJZLq+2YVW5VwafpPyn1rP8Bv7nzzW8J6ewu3RWRs1g
XdALRlUG2vgMLUGld8Ztvztz4idD1ixj3Gebv2YwOcPPNxT8jLe+L0XvNtRqAdHs
f7PtLnorVWLwiZmTj5lFBy8sEUxCgY/ZOtj12iVgudsxiaMecZwN2GWe469I4pOF
uEqpKOwOkiosPbeCFrFYYOgo01v8myLHEHy99OTiEQNn68tY2qcwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAoHffD4M7tWWdVj25qIu8/aMz
Gpu5MIUOI2Sz/64AOTmvrQRU4RXMR4SYBqaGiCrL/O3Y8EMFnLvUNP/6fE7EQBS0
fu/bsALlL+eLVQv9HdN/2SxCxzC6GHlXCwOfwCk+QgzVcbbct3ZLkeP4OILmTQoB
ar3ZQQEGRO976398AdChG9t+8tlGPAWeR9QWnoS3IBZQtqLiHzZAWobHgYz+iKSf
5qfCdByCZ4jyJooEOeFTVWSHFyOZhdnRFlJQU0X7QlhG2Np75WDG4N+A6kEuKrr2
SK/4va7JtDE9hWCdMOf9ZSRrMss0tpGromCoOWleWujL9XIW3jvuEkyInx+CYDCC
HF4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEDR63F3Ex9ZJaqBncRdFmSCAghww
DyQUVu2Oxy7BDRXBlsAlBK363lgVpACqFnCDi+oR9dHUUqJ8zsO9AhjeROI/RxNo
YVx0Jy4sWw7QpFWQ+qy0tHpjfgTmr+qcMsmxxkTihbD+vn2dWMKjb07wchVOuN97
6WTJcoKz6f8WRc+2skkXioKJW2SRc/n0Ii4Frf95JN7Yy+taMKSgb1gQVGZBG+E2
zhEkug1fBodQlUNOYtqy0gs5YGUxXKHnIUAX43F/e9xYcNDXelHZk2mRIUiygW7A
OETb5DIbY/EtphHfa7WMnHhgRVK8EpKqrfKYUxWtJ2VFkS0hat+hbzQlUKcOtOig
QbdZGYU6RCuNdvVS2tS6BJ2K4guWkK2XHPTZWFGMPR3RiAGisySNxvo585mHrwKr
hG79/caPmlcHCopZKikPXAYrNeOqlcaObsfasZ3TIFiwD9JSJik5UnStdrsz7R/S
D1GNWUwETvcRKtqp2vrMhvHmuNp0C9dN3biCmzLc2fB/1vKAGLglRP6LR14nQJlS
CAPHiA0af3SGxt5Wy2mU2vWLEb1D0pIXOsQ/Easx2htl+fHC+CiO7HRFgmp+Sah6
NoE0Mt/LZAYvjEl+BpzChTY9RThaa2igmMeqRyy3PdQtR7GMylfpObsayqy+Me8s
wR6DyIXa5tF3AxjxL8o+5hrYieL8D8N/04aJHroJI/Mf6iotFxzpzl34jcw4g0hv
VElBYHti7+YL4wvslb74f6ba5CHP8QjQ/eGw9U2ZIB/KpWiMmUqgxm2ANmCEwT8z
3tAfpglE3V+Sxp89YySC+tYXtEYwf8GhNO7Es0V+qx4yD60mC7NGS5kpjT2gUJON
/wiMgx8w8vzvrwRM/QR5vzVuWRchwT7Jg/NRFaNydMz3y1TxWkHlEuqE6WoTe+XZ
ZLDhSeCi+NLcYDVtYZ0Y+D2PoBZLJvpWtJkr9mxTdGIdXVG5mibxKW2YyGpJKUPh
```

```
AXUGqf7xwrXwfifEwpVqWbUDm1U/69xW1Mrrk+TJj9C+tdb7Txwu0MEVNl8oHFEU
CbUIUlOee0/H2/ENA4cgswSUvJLDojB29sfUvcYOW+EJbIpOf1UfDe3R3XVH/iEy
c7SzK6Df/nxlGUGvIMMMMuCjzrZm9FKAFwgJKHriTIdrWQMCUEhxQdkTPoMifyX+
3YuzZ+7f0VWFlfuoK5esvGOl31DrnvffO2WcY6Dx48RhQDiRlm0rGL7tM9N3ii3v
Q27dUcrUQDVaEoEJB4qgh4RBAzHwkw4xOanzo/gBQIGo9cW1XP3a8IpTFfkhVrNg
8Z9I/VsjYfxgwNDnMO2VRgV3lGpGKNVhWz9SzcjmOEyjwwNw0l9uBLxseSrgaGiP
zARiqLV/SWK+E7FwR+INQtrncRs2yvMPCqayZdOn1TN+F+ASIfbWm5yaIMt0plN+
7o/CfzXBc0M2N7HnveJXKhCysZOosrrTaSWPT3SS/gGLxQ2dXMHmHAaZvEkFVjlX
xzg6FTTPt4xVLKDxJrK7U8xj4PF77YxuX62vlvD9cdqSb2sri2c2+SF+VBCTF1r4
/dOj35AhSFLqunWR0A114tXeoP4PN2Y/0u1Vq0Vi/uQZHQG8Xqzpztj/kHYJM9V6
yKu8NbGtxjunBW0t57QeB+xycD8EK1gDDyswUpTENzI9T4dhijv9zVHlEWrwQ6ov
u+rKgtP1o04h1+hSeUjhCLGijYEXsT4MWKJuiRKnmbh9sFSa024dB24x+AQJvZ7k
t3lNC3Y2cMop2mpK6rMjruh8FXH4q1Bwn1CyWMzLYrjD7uld5UsyL7o2rhR7mKVZ
FeosAcyN27WI+peHi4L+bkeBHulwxwrXib53HYZrISLFPuGtOwvVhY1WuX6yiFWf
l30jQ4FqNY1/qgOpq3HkWMzVn955A5H2YYegGbsVDed2lJ4UIQR1sMBkJHLR0TCW
jcTK/OqEz3XScJuXHjgAwYgagUGb+Voc8LQO174iwoVXvdaBE3+mGFWcA1x1UOOZ
Or/vty7I13Yqb/GtBj2l4t0pF9THeqsDgIlP8IJWLwKSKSUmCyyoN0xxC//A38rG
zXxE186ri/ZLkFd1aCg9Mw0RHEdUOSg1K79BFHNFJdkxWgUuAT7CX7q25u0R3PKN
qSNZRyUrwRah6MAV8XRCHNvtuKk8UUqbyIy7NNcO2PwAduqtdM9P4u5AgAuzNuv+
v8Sy168YT6854/52dHcgYScWLxHCnYroRnjY2DUNkM85clpUBkX/QlB0yiLiE/w0
VhmT/X7iOI5uFl/eW0jU5oD5dWSmD5DCuY+qz0JKvDQKqEEwMHtKjkkyQBt6vnOO
qBCBqoW0+aJEWjzhHaOM/wE7U6H1NSaORP0tPKy7Jt+K8MajdUuU3s0nRJfgNNac
rTEnReJxC7B4dV2qtzs/SDQryQPTuVlR/2+KkgAUqiDYMZvQfdRlbJY6rid3Evdb
bLPN1w6c8J5qV/+W9uDWTofx9fs9uK0wZlIwfc1ac8Fke2aZSpG1OTs1dP6BWcga
h88avKEV/pLt5I5iigj1u9q5A2PwdWoxdlvSyhL6kOj618+B8Pun4NBdVmvNIp5A
wp/ACatR0AFoPCh1Gdf+39P7STfkBB+5v7+OKtajL+rMR7AFwGHxg5NIQ+jc6dPf
I27AW8D1kDLH5SuugDzDy+S33y0j9vY754x1YrKYoUwf/aRvG2EfGCdrwxjH5bsw
ukMntuWpQMhBEy94vdTNWo5xplNvCkiJCGfY7AMhWfHgacae+uY0WqxgUxpJPBaF
c5rvZaKD5QS6udPyyrQ2xPdKPJ3Ky3Xh7NREeDYHWq/fJXIbq/AM5LqhijWtcwH0
4YkjsYJ2DcWnrj2grNxOAVD3bK4HRgtl1nSUBop5kn39zpK5ZgRPqOfRKxZbFCPm
1cQ1avhCXwpYaFDa8Q0vBA8n8fQ+GdBJrjEtyUC31M5w4spY8d9uEwNtLaJc9okm
B+TsRIbmRLaGkwfUh2jlQj6X2Jj2dldfT9uwMkxBzEg6H0jfH1EyJ/xWbeLrGgkK
rIJ9CjbbdNXgsBVT892yvRczix7z/vhCKomUXmKQzEKv/vOl+UVyCtdcPqUMblns
Buj7wxQHBH7kYTIAmPMIKMAcpLhpYecD+6AebpX2Bjq+i/kM+1Xr02czQTBbJYn6
jaYWDoGM84S64TJYXgsGffyysh/aBbB3rhN071BjMIwIPgtC9sD06TUNIVwr0+bM
QNajsnpZ09qlLM3izMgXzYB8DFTL/UW+aGnwQN4fQiStPPQlo0JwqVtUbB4qr23n
cnp5n9gPb7iLeCOZ5Je9qqta/Uj90BPM714qXbMZpkICPSJI6VSvkBG/WMnnHjCF
+x9ek55H6XPD8e5LWWSVrqK26LY/VKtYQVtIhPP4RsZluSl8Yk9TwGx7ZBOzwyuB
ZySeTTF1Ao7MYzk2wMOhcwBexcsPC5W5voWIQy/hXc+Q/K9Zm2ewbqC7q06hH1L/
bX8wjbjVYm9OOLSfUvtHSzyShG0tchXh9aCpoVKLybARfaiJqAKvsUMXNTiFiXzF
85NUAWGqBHtKyJ+R75Ud+OiZlBjplDYo+j177iXqw0E+0YmPRC815f7x25eOz0sT
ry1xRxlQEweP9ooT5e+2XdUYQSi1QuZJb2h2LX7rDA/IDD2TtTTYg1UbRfROayzg
JUQb+2kbyHArQJdIoCeOYGOnpFboS6ssOlgTmp7zIkh5M/PLQraASzQmXZMVJ9SR
9iOrVBdZN1A0DDJq3cM/iDrTQYjfigL8lP5xz4CA8uMD8FLQaIpwL6SCby50RFXX
RKldybjfn2LD1nquQmA6yqI9d32CucawMyASf+70qrmtW9PNzfgeAhIaFMuK0ah2
AymtgrFrH4U4qxJVweAvwrcyWtpNx1yASrYlrz0MbV8qhdLdpsAENlltYzPWtyqF
buYEMKkMFTdNlzKCJnXFw3ui1gHoALM1mRJENzAPx3nQ7f7npmnzG3xBsjmwuXQD
ROQlVIu9PLi4NWE/51NGgvw1PCJvYIqTW5OfkkeHnmnxtzH7L8mKHYJYKWMtxGoa
N0g+CxXwwOmoe84EBtSlw/Tz3lRtfo3wm5Haja6PMAE2oFEReXlMupow3jrZs0/R
1JGUzudUKsneDa1N9cdG7IZdFgImxZFQU+Ensp1Jh6zWOM5eYjJEohoL+XlTi9YZ
pHGoWDecs+UA54mNVbhQrQnynY3T0/qmE+lMAortbCNjCZ2TiHSxdf5ORqdMxjoH
DzKpqmIcBnQTTcEfx7Mzg7WRzAMWfAy4ZgA1K/En905C3MH3+j3gX4lS0xa2mpJj
EMS1Z7Iuu+dM8E7ZSAFdNWoGJTV1ekoKMaHbfMe4OiKzx7NqFTmbLAcMqmgx/s0x
tZYqsYjUTornbzK8/F48VlyGzJKbvSA2UVXggcdI881iaCuyJIDy3Pv7A7Bh8sA/
lthTkn9VWI+iDcKgzQanoh/JSfAcdXhcRDbpJrQvMMnEzvJk+c58aiHnDcDgA7Mm
6hCqq3rSdd/POhFBgeCMLYEvWu6OtrM45Lfte52/EmYsdBorniMbuN0G0KJrQgQb
lMmx34vZuT/cYdJvoeYZXGniZodNs++ziupzrfB2GIQIFqCLhDhw/pFsrMPOjcZy
zl+iKT+P/ZWg5yMB5cWPOzZs/0IXrKpbkhAquFgv7AkBAlDMORyBDSKSmA6bu9Xc
```

```
cVm926zeoo6pNFgz4WDHLeMieAN/O+NUZnK/P1SBjIfksvTyHQY8DdPjgqrK47Tm
NjKL8k+jJh76Gcs47DbcFOKsDjDPRRDZyl1LB5c/iA9V3aESjEpZ+0lYnHcDFt3f
b6hsO8vB5caby0QBHBk8+13xnoM1/lCbUKmforcjF+I1R8vJhUFBoxVCIZVoPwjt
kQOuBf2IijAJavog5Agf4Y9SHcQhnbaeuBAzBY9jBx98mhZj9HGdAUhuBGTvUO9r
kqHIrCyiyjUX24RqiGSF7517Nr6TVj2JZlosIuqcEtpFFoAjGZ6yvTE185toj42t
n8KISHFu1J1LdkQgUdVBc2Hn9VTF3wfVBXNvoIV6gZckzVQM7VT8CEOoEMdkt2RC
+xoTOIKIzER0+OQJxTG3Zgga+NPzEC6C4gohaOT5jaJmDURWnjeewkA0uWsWVzhN
6e+oVUirLt1ml/biJ8opoKdcxwHA7hwY5V/G+u05Ezr9HqXm0530gTOCRi4strmz
XQghJ+We5XcL/TXDrkU+GGCD2+rrtCMoa27qY7WUS5B9AOtmWjoZnvs5BeqDkXHw
xDnMbRvHKMmCaUwHoeBAJobT0PKqOxHzeC1N+Q4E4yIN4guOfjoCxsEVEHB2H/Ke
BfaxLY5dHr6NMWWR5FAZm+AYind4/pimQc6OX6VgSRBnwgvLJdu5RkzpnpAsrXxJ
NcAgR0m6UFB3Lmz/DScPeQIL/OD1E7FyDsL384AqIP8xPkiKxgs/TrVzTTLJmGuz
P46qPFb8cmNJ8jj2dEjMfSlGZ8gGIXDT08CpU622QaA365L+w77gH9KEWDDs+CtP
3HS2GPL3jO531a9w9azTPxYmuEGM3fJNCXx9Z9du367DSzylA3f+yjwR8wHnLiXn
JGTe0Pfsm/KD4KW2jk4EAWbAts/Msm6rebnFLWltEFbHQAFRixv6L4AS0zhFVCs3
CJj1yYwgdYJvl5wlw3iuf+1oup1Q3cij+S6b0/QqG7uk6FpboQhTpOVGnw9xcV1y
SACx+7/AHQfIVgfODNln0T56wGsOs4hOp4YTuzL7nRpaMCr3u3f+OA+DH1c64bC7
pUSHZjlTcwXkVR80C79Xwy5RTxg/dJHgcQ4IsPfdSV95J+FwkHAZtn00Ig2/nyTO
0NQahYFrg8gcei1OpSCU8b/1cU4YD50WJfuGuFyFsKVKWFQrdfUZ1JyGBxnrOPIy
/kf1n1jELO4TpWDg0G41Awd3O78bacC5zjPWp0fgCeSTKJFqXnG4AIo7hD3SXiSr
Kj5nKLz1JePRwd4rf9I82cyl7RaiVDIog0vMLVxvewecUjWqKa9mdKDUcvEGMyt2
gzcd7171pdr7NV9/1mAHTeoWSpg/iIW/Cd9T0BeLMHiLNc9eujy21E6zwSXkKEBr
YP+33rFKeSGa1l/8ypUJIFLOmz3tDCZRYBO/uFSDEKZ2VGEy1fFSS8qemCHNmlCP
1yP2e3V1fJh0z6Cl0MSf1AbRQ+J6OFpbeMZS4U1wIs/AVdsirMcuT9pnHrkYH6W8
DBLIdoUttGTfH+54ipKUg1WrkJLxUmR6CCJd095jyzB/p1iYhNWz7etGSNd5/mrZ
6sgGGXPnI7LCwGSWtEPazcPBqfHEy8nsbXoYzlXNqxcldCGmi1RJsyxqcY4izgu4
0TXlhDDJZ6hoPU/bFXVtds3btPwNy0uFGX06fu/t0pznWGRalANSp/21n8j0d7ns
wjbO0u0AZuewj43FgJWWKgfi7tSMbAQl4Lth6XF2bf4cFHvegg+AUnvC8cmL+Iyd
Y1RURBUJBVln3OiD0q7KzO/OQntLUcrt02wG+FbW5Zp1deXMMY9Y12yxccxAgVeN
RJxaZfsPPJobn39ZI8ilEU/W/6NZFXUSk30vbBMb/dlGrP60n3ig3DeDR0flvqS/
2hLZb9ER0CzLfimZ35TxbUoPm43OH3QWoIM28+mr2srObrCeJQeO6SFumif5iXel
jOcDRbm+jjUVC7Jdwng79npdt71Q3jUPp8ge15uiKr329S6qwYtmG1phsACYRCaX
hxv8yzb9ZjFykp3VaVW9GK3AJF57HIIC33LF2YmEBWwa7HAs46k841o/HtNZhAn4
ti4ogWH2YJTiBzfQQVYv7L7BAnrcEmsdONEEYdaHKHA1/jR09so+5sxEiyRTNLta
f9Qco4NR2AFYYRfMgxPKpR5pL1hpmcAsKIrUvZBElXvmDTwoZFtQR3/DWQaFUMnE
xXLTglkLBtB6z2FJfy1RFJkjLm3Cr8Q0VitUbByDtBYkK668SLEU7r5gKcvtHlcF
ih/QwMiAXygCU0k7pxUK0qHa1yNyiVxeBAvUtTEr+S/hkO70iwSliILbKOef+8pL
RLZucZXDC5TWn3TCTSjeSI9XjERRF3P7ueM1jsfhgVzdtCxaXqgDyNeZDbTHM9Zu
KYIwJgrpRK/UQGl7uKx1IBMECo5UrVOhT4WwxH68GlOOilENsatV2oBjNz9LhCnh
aqb9YAqBb+OEopDuXhIhc75P5CBOccn+u6S+PU7myWbLOnQVVXh/d1GJSZEsDnie
tW0Pbw9o/5hXTOupX4uFAvbgkkQ0D016jc+5Wqn665cEfm60OehNQmToSr0ODF8T
UbV9QWvzOc/6rvjm1ymIRkHUblC/9lJzjJTpw3gBzfXmpKEnyPniBVAiKa1NtWrf
K22LNDDI8mdmSSoIyTrD/2Y9Z0OVCbxlLkXBsnKHNmUUDHCSDqZe7DPONQEY9Quu
a3qtEU1mcOGk3HIKQR8XeaUDnlvs9gG5P2AxQEZs3dP1M3OJ9AIwKjpwHy1jfPuK
qh6mJTvBYkJC3zY0rfhJwkabIBAqjdTUbdUokVUOIE/wMA2PJZxbG9SFsQPU+mBv
GQv3siLE0iuPYUw4ICox7IhMDetWP69iaI03jGQbuEmOdd9yvI8fjCcroUbw9PbB
3gUHSSqm+sqqfb02LCWdpv1d85uZC+VE21Ch2LQIrINhinhH9ZJiX+iLAjthx55m
GMCORoWUmNMBl5aACuaVf6wvm33GxciQDMWWbL69IAUmSu2g85FrBpuUhe8IFOkk
VF7053IBFw/LF083OrDzE6w5tEr3NM2I1gLQsvqL+bpgGkixVthBh35I54shZzyk
wUJSTlQDrxQRrm2HTuCj5JNkSnm3W03DHdmiKMlDOLIyAuRIRuTLMUEtlgqz328M
o/6k73SPFuAwpVokN2kC1xDtHS82PyvwO1m3a9WFiSoVG576XPDDTfGtyx2KYZdx
YbE9WNd9euMYYGQdaGheQ9SF2U3+rQXaFr89GUAe1XhU/24npcutZsA68o6e+NU4
e8pThbPtgWhXyX+NHuWjArbnuSoltWcwaNXcReHaKfdoE9Z0Uixr+XYuHfgYDgyE
O/U+Nl1UGys/89wbEK1B/08JxW5TFzEQ/EER/Q9ZB3/RB99pL8sqq1LJq30al+NI
i0P8KeMrOSjGmXu3ZH6CHFcPXj/uTTT356mWiGr+SJAYN7DvjYuWf1MA9S0p1V20
rcZN96+yt9c9CubQSUdU0yUh+Xbzq9HTM5JaHACxjsc3RQB4CDaAp/67toJQcCSF
tHHwXf88Sc3WPpXAJAnaSHxgsJu1nlo7wPj+jiJ7kMwD19Bl/BPrHGc+aeUTvIVW
D8Fu+XVtFPnywenrYnooqkyOFkTbck08MYDxOiiyXhVWKLlCnSYwfIQvDtEN/bq+
```

```
ObXlYQZKiwLcQAjx0o1Dr1gEEUMDlUNYo66MjRfnxgtetDgOjAZNWNB1lwVv44tH
Z15bb2QdMEBL5cSaEQzO3CtuLNUnPJHb3NiJV3YuWuLeBtcwJNzTup4GLD8kbwqz
IJD4aG+bCywKs6epTifI9zhLorDJUrmxaxy5sxHDrzufAMNfZTV+nTGGQ6iVsLVc
RmfiQ7b8varVDVtrBHX8vzI2Quier/gNLxn4AYnFtXQjbalYOp5ySOG7Fx8GGZvW
+NxHLedmmASlubNLYBre42wV6OnGZ/eZJtkoH+c3spaq6Ujsp8pZiwE60jfwnrB6
qHRxP98ftbEdcB586TvOx2zYNbd6MRMgQMxo/8k6YRvJTeHfAdJ69TsUI3OLVu6Y
drxpGcDKK84JEt7W7h+6vlPfG8RzK0X/M3U2EEZ8CHL73caVcPTQ5FSm/rGj1smU
ZBja96TPY2JYv4YB69drCTjhH+nR9JAuhbna82e/HKN3Od0fU54JjN3C1FUrhiAh
1k8oFabzoF96YVdg/mSttI1zH3Sw010NmyuagwYNcoLELq1mgWM7Kd2989KkX2j8
/bQRsJxO2Bz2IdNbD7E+hBjedywDaqvxftqQBcoQePfMnAhhzVCrAB6z+UfjS9Qh
us+CcqS4z+3YXun2a+Mv+qayDqVjWcZy5sDmXXtS7rxHcOdE5CwDOoH9quLS9N4k
aoZHzN2jc1ksQ9v32jimBKQfmoMohIvAwVkRgzCBxGRJj1xJsROMK4bmAaCiY1pX
eGbbwfTenscaZVy5OIa+pEmFIjlQ1UvX10D4nhQGGskAJkzz1u3FD6mH7MmtDJVl
pfOdegJt1w63DyKRB7zXAY4KP5nCdV+PGiJa8KCyVfDyrm0+/UlLIvpmUJP/akFz
H8g5VEv4CP/Wa69P72w+xZcbRaEwvg2ZZ9fdQ3EWNi14yyB7utbf8kdJPPBNGutH
/Fl9XyOtzTlkOHUETcZ+jE8LBCSjVmLU2ELMKFmWNsST9cM1nmA/NN8ba9ijvVA/
cMTAloqLf0OdXnzUNrdabQ4rxvQaIeW2iyQjyjQEFKLOOKcqwvtu4Wy9w4DibfP4
U2IY6QVehXNXveg5x0wvfxH/gMT9Vp0N3xCBwx89Bh3OS1x9ViXVObJDLWwO/ZxC
BGbFvqM/RNJ0ew6MUYDU6Tre6LAvPcLgYL2dlywZGWG2OJC1MOajDnRH9iRgBZdT
6yI9K5QPEcFa9AErInwKFQ==
```

C.3.12.1. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_shy (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIUGgYJKoZIhvcNAQcCoIIUCzCCFAcCAQExDTALBglghkgBZQMEAgEwggpDBgkq
hkiG9w0BBwGgggo0BIIKME1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LWxlZ2FjeQ0KTWVzc2FnZS1JRDog
PHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHktbGVnYWN5QGV4YW1wbGU+
DQpGcm9tOiBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NClRvOiBCb2IgPGJv
YkBzbWltZS5leGFtcGxlPg0KRGF0ZTogU2F0LCAyMCBGZWIgMjAyMSAxMjoxMzow
MiAtMDUwMA0KVXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0KSFAt
T3V0ZXI6IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcjoNCiBNZXNzYWdlLUlEOiA8
c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNoeS1sZWdhY3lAZXhhbXBsZT4N
CkhQLU91dGVyOiBGcm9tOiBhbGljZUBzbWltZS5leGFtcGxlDQpIUC1PdXRlcjog
VG86IGJvYkBzbWltZS5leGFtcGxlDQpIUC1PdXRlcjogRGF0ZTogU2F0LCAyMCBG
ZWIgMjAyMSAxNzoxMzowMiArMDAwMA0KSFAtT3V0ZXI6IFVzZXItQWdlbnQ6IFNh
bXBsZSBNVUEgVmVyc2lvbiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L21p
eGVkOyBib3VuZGFyeT0iODhiIjsgaHA9ImNpcGhlciINCg0KLS04OGINCk1JTUUt
VmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9hbHRlcm5hdGl2
ZTsgYm91bmRhcnk9IjZiZCINCg0KLS02YmQNCk1JTUUtVmVyc2lvbjogMS4wDQpD
b250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0DQpDb250ZW50LVR5cGU6IHRl
eHQvcGxhaW47IGNoYXJzZXQ9InVzLWFzY2lpIjsNCiBocC1sZWdhY3ktZGlzcGxh
eT0iMSINCg0KU3ViamVjdDogc21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNo
eS1sZWdhY3kNCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFtcGxlPg0KVG86
IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIwIEZlYiAyMDIx
IDEyOjEzOjAyIC0wNTAwDQoNClRoaXMgaXMgdGhlDQpzbWltZS1zaWduZWQtZW5j
LWNvbXBsZXgtaHAtc2h5LWxlZ2FjeQ0KbWVzc2FnZS4NCg0KVGhpcyBpcyBhIHNp
Z25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0K
ZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVkRGF0YS4gIFRoZSBwYXlsb2FkIGlz
IGENCm11bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5l
```

```
IGltYWdlL3BuZw0KYXR0YWNobWVudC4gSXQgdXNlcyB0aGUgSGVhZGVyIFByb3Rl
Y3Rpb24gc2NoZW1lIGZyb20gUkZDIDk3ODgNCndpdGggdGhlIGBoY3Bfc2h5YCBI
ZWFkZXIgQ29uZmlkZW50aWFsaXR5IFBvbGljeSB3aXRoIGEgIkxlZ2FjeQ0KRGlz
cGxheSIgZWxlbWVudC4NCg0KLS0gDQpBbGljZQ0KYWxpY2VAc21pbWUuZXhhbXBs
ZQ0KLS02YmQNCk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5zZmVyLUVu
Y29kaW5nOiA3Yml0DQpDb250ZW50LVR5cGU6IHRleHQvaHRtbDsgY2hhcnNldD0i
dXMtYXNjaWkiOw0KIGhwLWxlZ2FjeS1kaXNwbGF5PSIxIg0KDQo8aHRtbD48aGVh
ZD48dGl0bGU+PC90aXRsZT48L2hlYWQ+PGJvZHk+DQo8ZGl2IGNsYXNzPSJoZWFk
ZXItcHJvdGVjdGlvbi1sZWdhY3ktZGlzcGxheSI+DQo8cHJlPg0KU3ViamVjdDog
c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNoeS1sZWdhY3kNCkZyb206IEFs
aWNlICZsdDthbGljZUBzbWltZS5leGFtcGxlJmd0Ow0KVG86IEJvYiAmbHQ7Ym9i
QHNtaW1lLmV4YW1wbGUmZ3Q7DQpEYXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEyOjEz
OjAyIC0wNTAwDQo8L3ByZT4NCjwvZGl2PjxwPlRoaXMgaXMgdGhlDQo8Yj5zbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LWxlZ2FjeTwvYj4NCm1lc3NhZ2Uu
PC9wPg0KPHA+VGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBt
ZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVk
RGF0YS4gIFRoZSBwYXlsb2FkIGlzIGENCm11bHRpcGFydC9hbHRlcm5hdGl2ZSBt
ZXNzYWdlIHdpdGggYW4gaW5saW5lIGltYWdlL3BuZw0KYXR0YWNobWVudC4gSXQg
dXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gUkZDIDk3ODgN
CndpdGggdGhlIGBoY3Bfc2h5YCBIZWFkZXIgQ29uZmlkZW50aWFsaXR5IFBvbGlj
eSB3aXRoIGEgIkxlZ2FjeQ0KRGlzcGxheSIgZWxlbWVudC48L3A+DQo8cD48dHQ+
LS0gPGJyPkFsaWNlPGJyPmFsaWNlQHNtaW1lLmV4YW1wbGU8L3R0PjwvcD48L2Jv
ZHk+PC9odG1sPg0KLS02YmQtLQ0KDQotLTg4Yg0KQ29udGVudC1UeXBlOiBpbWFn
ZS9wbmcNCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IGJhc2U2NA0KQ29udGVu
dC1EaXNwb3NpdGlvbjogaW5saW5lDQoNCmlWQk9SdzBLR2dvQUFBQU5TVWhFVWdB
QUFCUUFBQUFVQ0FZQUFBQ05pUjBOQUFBQWNFbEVRVlI0MnVWVE94YkENCk1BZ1M3
MzluTzNUcFJ3MjBkcXBiZkFSUUVqT3l3aXdZbkN0a0RLbmJjTGs2NnNxbFQrenQ5
Y2lka0UrNkt3a1oNCnNncnpmY3FWTXBMMmpvMDQ0N2dZRHBlQXJrK09uSkhrSWhB
ZlRQUmljaWhBZjVZSnJ3N3ZqdjBaV1JXTS91bGkNCnZkUGYxUVoya0REOXhwcGQ4
d0FBQUFCSlJVNUVya0pnZ2c9PQ0KDQotLTg4Yi0tDQqgggemMIIDzzCCAregAwIB
AgITDy0lvRE5l0rOQlSHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQK
EwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBT
IFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8y
MDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMg
V0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQJ+RpwpODxxzY60n1lJ53pTeNSiJlWkwt
w/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6
rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXm
bk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmSwqpS6oQcA
x3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnl
sukgn+fHbqvwDhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB
/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNl
QHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQD
AgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSR
MI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAgUl4oJyxMpwW
pAylOvK6NEbMl1gD5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LDsfx7fSIus8gWVY3W
qMeuOA7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxOD
Wq9opwtA/lTOkRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFb
Zbi4oZ3tAadRlE5K9JiQaJYOnUmGpfB8PPwDR6chMZeegSQAW++OIKqHrg/WEh4y
iuPfqmAvX2hZkPpivNJYdTPUXTSO7K459CyqbqG+sNOo2kc1nTXl85RHNrVKQK+L
0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJcOvT4as6aqdcwDQYJKoZI
hvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAv
BgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkw
IBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElF
VEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0iehYOBY+TZp/T5K2KNI0
5Hwr+E3wP6XTvyi6WWyTgBK9LCOwI2juwdRrjFBSXkk7pWpjXwsA3A5GOtz0Fpfg
yC7OxsVcF7q4WHWZWleYXFKlQHJD73nQwXP968+A/3rBX7PhO0DBbZnfitOLPgPE
```

```
wjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZO63dKvIKp4cQVtkWQHi6syTjGsgkLcLNa
u5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0
zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsC
AwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEw
ATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsG
AQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQUu/bMsi0dBhIcl64papAQ
0yBmZnMwHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcN
AQENBQADggEBAHOJojanzqmgaSN3/gqSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNw
YyTneuK6AChwKfnNvOFb8lV1iffRTF/KtmVEDMR/sYeqAH83KM5p3el2lVh4OHhy
I0qNuz5oShNaACSioQ23WxHGVy9vsdVfnbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/w
vXMt9cG6jbMvcdH4z0IOvg6mrYkKTM/RCGnumghxwYToj1OyD5Gs4D2IJCw+fX5O
Dxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDd6hnoQ9rNeozIcBVyybQYjf
rgg4DRvw9Ksk22OH4ConlB8f7R7s1LM2cSYxggIAMIIB/AIBATBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrO
mqnXMAsGCWCGSAFlAwQCAaBpMBgGCSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJ
KoZIhvcNAQkFMQ8XDTIxMDIyMDE3MTMwMlowLwYJKoZIhvcNAQkEMSIEIFT1fYL9
gAEHvzGwOrKYPQPsCdQ+Dvgh0flzrEz5H3UXMA0GCSqGSIb3DQEBAQUABIIBAIaD
09L9rNPSxDuaCb1sGOVYYWZmZ17BoLp28exTLU4Z2peJZiipmAZUAuKGeZ1CdLEC
VqQ+t2snrG6EbfDad8TT0xmP3BXbQdeIO+hftHNyM9B6MkRlaWIcMHzuW3q62w6d
9dMRg4G/PxUWWP7L9c4M3t5zsf3S88JcWA5zLyXxScvYtT6Qccu43HSXciTWb9rQ
vkEwATVblSzmhVA2KFICXRw8s6OdiLy9q0l/8OdXZ8oZBpRgPbn0s8Zp0yX2bldF
w/7Rag0W1j+d3uefP3kxLm62jnd17H3TLlpqNqKo86Ho0TG/Tuwqi3OsBVnOqrBD
RzEIRwi/BymNcaR2Bac=
```

C.3.12.2. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_shy (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-shy-legacy
Message-ID: <smime-signed-enc-complex-hp-shy-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:13:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-complex-hp-shy-legacy@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 17:13:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="88b"; hp="cipher"

--88b
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="6bd"

--6bd
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset="us-ascii";
 hp-legacy-display="1"
```

```
Subject: smime-signed-enc-complex-hp-shy-legacy
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:13:02 -0500

This is the
smime-signed-enc-complex-hp-shy-legacy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_shy` Header Confidentiality Policy with a "Legacy
Display" element.

--
Alice
alice@smime.example
--6bd
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/html; charset="us-ascii";
 hp-legacy-display="1"

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>
Subject: smime-signed-enc-complex-hp-shy-legacy
From: Alice &lt;alice@smime.example&gt;
To: Bob &lt;bob@smime.example&gt;
Date: Sat, 20 Feb 2021 12:13:02 -0500
</pre>
</div><p>This is the
<b>smime-signed-enc-complex-hp-shy-legacy</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_shy` Header Confidentiality Policy with a "Legacy
Display" element.</p>
<p><tt>-- <br>Alice<br>alice@smime.example</tt></p></body></html>
--6bd--

--88b
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--88b--
```

C.3.13. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from RFC 9788 with the `hcp_baseline` Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 10575 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 6820 bytes
 ⇩(unwraps to)
  └┬ multipart/mixed 2343 bytes
   ├┬ multipart/alternative 1138 bytes
   │├─ text/plain 390 bytes
   │└─ text/html 485 bytes
   └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-baseline-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:15:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-baseline@example>
References: <smime-signed-enc-complex-hp-baseline@example>

MIIefAYJKoZIhvcNAQcDoIIebTCCHmkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAAh8BW90JuemYqxwwiLjK0/1puC5akUSDDzw
nwIP1+zCjV+RBTnuJbc1Yt80deysj0WOADJQxHdjGLqhqwy7tYChAopgpvEmZIFN
9GOioUSRxGHbRc9fG+OPKYhTqxy/sPWY2E69RjE08wgh3+g1NLGW968F2hQ8T955
aWD6gffqhVHgUg7ZyBV45TwaqJhtKU0NykP8fM7QMTLfAleXwhfC0XDg/edowQSZ
+8Akm+Q6Z0Wc+f19QSNVUhs57E3Aj0RXeUzVND+uaajAyWEv5IrkIZsYyqoA3346
1bGfkgqa1rZwCr0nd47+L/JSIEigsEs4BO4HCL/3152nd+ujEiwwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAY/JjLXmn6NbOt3TjrWIQyj7z
UqVUsuGDTnOvGzlmr3aX7MAGb9gcbiJvbEi1qBddKbc5hBy5MOAaa2eahJW32e66
Q2YcvCrj56tjKGHnKCKNhEyQaBIJwa586dT87MAlhCgSAOlPRWInWkH8yjHkxgF5
VXw2UuH1zk2momhA0c9dkX2vAXihIaldSQXrhAKcaUYH23VcelUtFitlyo3jbs4V
sSdYOhfEU7agSSCuUghB2SYTMe88nrh/PUuL9BCx2Yfmu/UOq6enkK6zhGGw2hY0
zMACnCBtdAcaXBCsdXDd0rJQdD8lvXE8GlR0VIdUAo2KVmww6dD0XpyChiJccDCC
G04GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEML/LZyVd/Cgei/l+M1kHF2Aghsg
```

```
1TX6aXgTAJEAbBbbnV1Af5NLxsxal9GZ9AKi4pWk+1lOjzvfxxAOpeMH5z4jH+3r
+mss2RN+DVdfItsa72lXat6FdC6+RFU5RziCGJdbHIvRzw29BWRQW/eem+RXhi4t
VST7l6ND87C+BbWwVZ0JDj3yHXWxYGSgzNNHb2Ix4wnf2DWbWqtHl+7SNiAh7QgE
8wlv9KM6Qi4OEwyAEPBxtkGnrGYgChBrchvcjsV/TtQx8WeK/0z1uNDwbVtUPaep
UIMOuIf2vCcp27FkWyh6OJdwWVeRg3af81vxfaStN2GbKATt9fh8RwNACtGfVc+u
NpjL4Qf8FMGbfuextkmlq0U1nsGZP3O1JO+VDrpkLRPoLk4bjh6Wk0mEbvjRFeNX
ZUVMWVbnDH4Z5+t0IXNV3T59fsJ7QqnHOKqGL1y09fZTIc6lNA3bELXM0nSgDP5Z
iDQLyTcs0nk7YooEIUXOlUMt3FBS1SR+ieABPj7lzCn/6bg43QS6tbtvx/12bJxC
C8ZE+dq08TDiWGSn3vPfADBt+7reZaKXNAH+tFVcW9Q6GbgAVwvwNynjRySTfzK8
HearG5r9F8ZtgV/Fmedod4s8/VxGdq9gl+zOR0nmE8P3k2PY6pAWbBRb1DGfDMwm
A62aiLzM5cc4Ikri1jexndSQDowQpnllD+RYLWYEni0NhE8ueM0iN7Vfv4b8Bxts
iisQ7M/lcbrCTQQjR2GNpq3WD756ARlaCIO5zqXMkE6I1HxsJFYGjQWYo/bRqdK1
8nzEbRL0vcNSIr0jcH6lbizm1otU3bDdqBXlteKW/4CONB61hXYwMaoG59z3YVaE
GoazwiiAXaFZDIZ/so1sQAHuy7Liwodd0MY/FxOrgCQkN4E0CMYxhW+3Zv/lSpli
2IDnyaMZOBoIIzLw8uJvHw5XeI6B7vr0LKgd/JyEuhqtHNU+q4fW1hUWF6rFmP+5
88I5LlTmKYHAs5wNdI4RnhZ96nFdjz2sG2Mxv3aChuzrfYmCM+/88NSB8QdZB5Xd
H5FTwjizYdFoAaobAIyme8x5HRqjd+GTY/sqq5aUgs388CCQE22F8qExCE74bL0Y
YT2NX28Sp6C4i9ULMxV1YnlBy5WFdBz+3kd0vI/+c7nkxjgfmDCZeOVlrzlJM9yJ
aDvcOIRrPjn7XlPYOaquxzBgE9wz4zrS7IUcnezipoNiunEYHpVIj7LU0T6zuE0o
Fu/dcXmeb7njOs/R09hm7kipEpM75kz00cYEvlNBfsH7llPMoKpqoTK3K+c9GXyA
wBbXL++MzgRfNubhSqOOuaaXRLYiqkpGfmvFkUYzNGsgyq6+Bkwjit0XG1WgySo1
3uoQ7GDzmxE9VNlSVKPDSPiuDPQccdfN+BlD2lVjrSS5Koon+vl3McJm8zlX+UaR
wAOdhVjsOJJvpyoMI6Vvlh26oYMqpPdwvp/eBBiZREuDpDdIyefd9aMnYokY7iua
KucdGoryEc+wnBTsnTryfOtU6UwmjqQexZFeLrce9FJ65SAr0zlln9plNjloUauE
YpIQWtwfwlNHG7VEwjvKdO7llfc7zJCfUZUCHogMoo3rl6WsK6QSKNf/kl8/FUjO
/iccHsKVWRWcNn9MuXchhEwR+QvI26f5/CD5ErXSy/wxk0mm6V2fbd5Oei+HlTz9
hIDYGHxJPjAq83YVPQ4r1Ndy682QNDL9oNz4ENFgYRj8Q8G2OF4IDG6MDOxSBNuu
uRcjTvE5bl8OhZvqOF45NyKQZh47XtF6ESrYI45DkqpHDxNeIQG5Fowfzz25SCy4
CNQcibLe4cYNylTqfAHa9FHDMBW3kJJDHtmaX17Zbtyz126S9QvJiIR8x7W81lSB
IEbOMmZ6rNCok+7P5JB565//+T18y8dNxZPLtSbBx7XO3b9REiTR2s7M8jYOjKja
/7CWWX/fAQeivjy+9jFk/fD5x3w/Sn1uFQCBUmf5YflkzEqqr0jq0ZjxbzawgNkx
QmtG4GtUr3K49MaC/XJ13/iOONRng4Y3q1h+4mdE6c1n+CpG/BrRBb5bxZrGcqJJ
swlvoUelHwyKXoXloc/RholYC1NB7NKJASm8+JO9ugcKDfQBREg/4dIV3SQufftG
xJyoESXAoG5TuW6a2vDhfLZ45WDDuVBuId4uiZX0E/5xT5SzW1ZWfZZi2ZHkRWDq
F15PIfOXXfHXh1PUJOBlx+fwKC6mrQV7oRMRVWunWPwk0tSxuPolCIKtRuodS1Ee
9RzI2Xy9QLX0AjUSr1iAjvCmcfIfvxnyX4KRvwHuAxOFTNJUxR7pYRwJz7xbUeW6
JjjjCb+52/jmC6WmLr/aSsNq7PyaWHBR/N01Kt0Z3T/fWdQ3+cYgnDTw0wmvqR55
xJ6a9qiYytowff0YaDGwaWEUpgisrfFVNei9sVYLo+4pzT1OXx2pQ31NweMn17rm
A/9xue4vauFZ/FPQ1G1ys5FemIO5z0COpXrceLejBb+5ZozQdHSKmxuaEHaReu4v
jR7j4NYDfP7LFB3nRB6I+QbjuxHy+xl0bESB7iALO7P72Y/4dR+6gbHZLngirHQE
2RktRXo++8uJ4jqfmLBVzszG1C5R2AG90hA7VLZs7LU7V6E3nzwZllcgxCSSR+gN
e4f6d261oCkJ+pT4JdCM0ZbrpfxFBitm9R7QuTkrd3dTbQ7OVU8t+3rzY2MeIt8R
WNgTc58ThYo3OABAGB4DspLRIywR7Dr1osj1du90vIWnS1LWWSqKQdEu7E9Oha4M
qvwrtktLmGgKVijKI0PgxuxXWsFS98Na292l9ZYtbtxptKpWI1G/rNarBetgNVG4
J0ohqzOZd06F4CQHfI+1dE/a8g4xDcdZmnDDS4/fr1GhhS3HZVm4csjIyB+YSHmz
cMIt1LW6aFj1/PS/ofQJ7eEjme5lSlRsY3CjAeM1EMJdXn9SLXtntPDaAm9Q62Wq
rgE+NSeWtyQyj37let2DerOY+rWwGtpx9hD3v/np/VWEIwSopORrnbNXb9VU6ILI
1kfRe2mjEgtU93OE/4d9l1HNEu3JFe1+l3d2m04NrU0QQOx2bwIT9TCWVjYDqawO
OP7C7/DyxgkfE8f+BKsaRkoJ54h2OgA7uboeXBEjEeHwsIdZkM32vQg/tP4ftAOd
4Hkl4ZxHqJF4ETuQv1KHUhT2aJQmQJJWpB5UoIe3/eiqKvHLujFsBsT0vidaeeqK
x/QSDxYAYVCByJmcfutA4fJbC7AJvkJPTyYdgYqWFIMDCgu2QmtX8nuwDZchRfYK
BGBze0Pdcr4coEh/9d7fqlo6AtcIZKg/9ofWnzPRqA4zgL/Q0JP0mGQYWUf6G4n2
aUNyAZRbfoPlNXWDY3cKy7kAHGZO7qU3QMeqpIffSDHHbaZ6CtarFBcDEwrLvk/8
Cap0aBGX7BxatCLjbb4iZpQvKKyPMZzyRD5oIgW8t74Yc1KnLsTKkp4JDDKcMQLo
k8h75c088PDo09secT3kqCkA+2a7I4PS3l7eTNjxa4HmGMDQa7ulso3O/LHmHKHG
TyilXA1Q0qluw/QmyVx8jA0EkDHsrVTA1KvF9O+kA1+9Zf8zg2riX3RrAaGXBCFz
w4M3JosnZVCMRhEAXi0DNJfwlZ87MfrsvDtwLHzHayajuDaaCfbcPs0CARxHtTmH
8qxz75U6nL2PNTB36aoiMWMhUxA0d9J+e413A7Cl3NtSye9B6hwxUj1m1ik/ENrv
```

```
Ma2xbwJFeQKyT51pm4Dg1C2ptRbrka7/33XHNhmh8WWk6VbWLNf/jlKoFxs2qTff
5j098PdbTSIuKBYh5CRSClv4NbsFZt17Vp9QVWRuK1rT8SCeA/Ev4HVgdX1lBTcX
2phDUZmWU2pi4A2Bsj/bYQHkaaxhGNSF6drlcRNfRzKExdZLK7ybaFQtJPnzzQVL
HOU0mzMMOS2rktQghpqwDrm9cnFjNn+7ZYfrqYq8pZ7I7wllMBRfnzC3emmNbabN
XQh+mm1LudlDoiO/F5KFV5g1lPdjrB/+dMjifWIVo6HqiXSYS7VwQTgUwPuPxZwf
UKYoMQqJfZ5VfIOWiBV+lpxF77Ihxp54To5BtpTI2asTSs0CtfRhpGamp6Vug59a
L4GtPFutrR1x8W6nv+YJkg8d7bWgebF45xL1Da/NNr47rF79bzieUR/kvnvNwMRR
HIWqYaWcMoGV/RIYLK7lmVWVIn4tdkXX/pnefaQj1r/swA5ZG9cq+maBzyA7zq8S
nKhasKLuBnWuPYeqkZyXgaaxIwWVJnKw+YYRCGXvJNYhh91FNK0NXvrAk/TPQ3Th
9skjLzc8TQggBQ+0K3GZ/+oz5U96F5kf2FJj1hAnA31TDOtqp5sWLUkjcFWXMJMT
HtLwuI7xpViD7HRpV+YmpuCdrjwBel5ylhMb1yVj/Fm/sBx6Ta4hcf0zybJsro5Q
KmIroLxeBUDet/aE/GUw8rK7/4eS9IintAoZbng2eLTIRBnecieXGXzjCP1pswTK
4ynBMzZCsrN/kFltskTGCbA2j3PGUyiPWYvtZCTEBSlD0LWlfkluXifCvugYtPnB
fnsDYBw3pM4oi1Y+CO8LsnGou2aqEyVUkxwX5ow8UriHbrtntNOfUYybUJZ4l4ZP
9UE4Ow0Yava+QPV1y8mJlhqidgWMygJF0v7lFgjjiX2tM5T781pjGgxj7gMEKYYn
v4t/De+30UgprRwpEPZ91DySE6y5XD1cKzrjzaUU6kMJ3ttyK4rDd0IYqn83V8zQ
WXuONNqZzF49SzC6RInvoooW2ipvs3/ZDwgVwhDYgDHtFqIvj8ROewB/ZiUVMiBS
/NZbdV5ArfWTum2s54sCVEi3+1ACeLiQoylQQc5mjI9lVQvqwjpzMOp13EQj1tTb
rCU4jZj+nRCqj6c9oe/SduEVxfGBZQ40vGOPoQf6EUY/S/yBBX5eiUA13HNj6tJS
N5uV6LehKQuuN3+OxKH0A53c+AlGJePocc8L8XUCS5XxutQEWf78Blp5IWxElNIs
5lnG8xMR4XpcIOK7H1b/KWYJ4szYN/+tXGo8vCy8azYZDT155MRzOdBKiCj1+HQW
T4gkpK3/uzxitiioEeQbvhDN9LQEX6xpb0vok9MVPBh1nImm5pQIBB+G8X9cb3xO
Nb1P7Qu5qdp3LJQMm+ME2eTV2dKGSrffe2botW9LgYbq8DuRO0iC5dGjkSNYx4+8
GHyB84Fox0a/7o2w0+1n+ujCGgEOKjvBtgMLfy1WGw1s4xktp/OrqYdit80QLV7d
kPJhCkpS6MdFeEtn4UOvSh+2DWFNtvXqkJWww1CNN2qupeKhA3afYAt6W3HkUHvr
DhgawnJz+0Q/iRlrzbu1pe7r3udX7zxQl6eV1k4RlkLJ6+v6zxhn12fjRjjL7Ufh
euwO8zxtyLvbwq6HW+9iKmc08nxGhitj0Uwm0mOWMA3sASsuMT6FefSiQpu9nt93
TzaNiS1fn9zLlSr+6D9sLwcobNz6Hgtq1/d8u3hIXHJxH0ZTRbh3KmB40HyrFsEB
Drxf9Brn6DxMOeGg2VEgzoiE3dn4nvdHNVs6GqgAjQ8pWCzFrWijTJ11zUYa3aT4
CFpz2no5GsnXFfCVyDdXwNuDIhhf+Yke+PJ6ss5YdujZoRux1+C4l9hyoRTnYF1z
0LE20LdFUPBqDMoPSjJyOoxncdF/vCqVaBcbMuAFypxsiPYLSA46RWjdOPasPTfN
Zalwzps/loBuMHnUmX0Zkw62fF81BzuO4Eqld3Gg0wwn4Gy1EATQGC3TfnDlNGzv
mps8qen5F9ER8xv2gyUtsxwLY3RMbSlQp0KMk4uqa6SMq5cw1u6aCPy7wHkRRJvi
Y46Iax6rMcZOWmcuGqEotZMo00wkCF9dQPFkTIMtacpFqMqoPpDtOw6MnHm8TC2J
/Tb1X6o1tpNDRzwglI1HNIOKT+c83eVPfnd5FRqLK3FZqHXKkeGwP8YnQkrLCO8L
om3dcdznc+giDxhkVjNnG7jtflm3ytUK3aouJqGgVO9sZ5EVzps1LiTJSgbQYoQT
NIKMi/ZQXf8xoffhv7tAGQA9tfRpmq/BNu5FoA08jucgw5EjPqqX1NIIvv2ce/wr
7eULcsBUCgnT5/apRBZBb/fV+uZbVRtXajaf+r3dsrfYZwVGeHr59X90slEY6kEJ
qsSPGhR2iMJBUSj6haTGWbx8dsyodtQrGjtnO7uy29oJ4i5eX7e0aOaz2fuAfdoX
JkxmKxYCGJIq5SVmfjynb6rNE938KGQu3kwPDIPzamZ5e295y6Z/BLi6zLe8myCi
RGHm/1mx5jX0scQL9s7p+UZPGdQhpfgZQeXmMgSQtS48cBGMdDdXrnuWBOFVMQ8E
gjrDRsVd4hMCKvOMh2bPUNq8/FPAPNRDN2thRts9ZZTz6/ug86wUu07a5GkdLLmu
uFc5Qtu+3kj6FhmjZuFJ3IMExKzQsl5T3aUEL5YJpOSfUrY3ir4CEcZ9Q0jEpffB
3Xs52uHXP8QcdtENvNX5K1ZlXNBkpJW8fWmuYcLMzHVQ8072kEEz287GoqqZgRMC
wG26oS+yTRMHbPF2Jc+qeNFwi8nfcuA2SJx2Gw83eXGRABvxBspdrjFFc+pJLJcw
RnU0QfVa4IoSr6xCg3e4+ZfveKS3BSQ79ubHoD3cTo2/W1PFXhHH3x5vmL8gVXZo
zAFrrhDfVp63SmqbCngwkdLZr/myoN6oMWh/EyvNiWgRfxpL8d/JZBw6rdm0smya
wJ9k8BzEg9a5nvHPjwwG932xyOHR3eevzuqH95H8vi1ZLnag3UaCgXBQrO6DyOgz
PnAwG4hjOTzO/Cxn0FMQYr1ZxgeTgSdhtJblh5TxrfSsjFEXLWYguB+KBgoryMtK
Z8Q6B9jtVLNjAAcowjpyhFuqZsMk4diKco6xx7gOaeN8WcOoapIgOtifZ2YLHzk7
zHOvQ0MHLiFKIBUyBQWrtPrhp1k6hBwuCBCjsDYSbRfVtroeDemOZLz5eBd79hJo
3J2uN7kQHjKEPmCAPMpqzPBRbLrzx+C77cBjImtOzQXZC7pRmwqUUKfC6Hht9pz8
AanfaaO6H9z8ShHB0GewOhYf12M8mmx1Hb2FEla5VsU8knQO7hRav9lP6Q5+MPN7
P3vF/fXy2RpdiGEEo2PirlQ9Dnyrtp60voy/31QNp7ntj5tic2ywV0+QAn4OEx/8
ewy5zUJAe9Z8qGsExZh8opjsjoXCThnpcU43vgYwHLPGcSVxodhMrKA42YS4xPEg
v1wU4VpTbjE/Xx4oNKWiC7ppJsceDIDrT2iNIiri1hjy6qVgsNh2ViCMAnyIxhQK
a8kpg0R7EF4ChPkP2SZO1qMgju7IItOzch4fLxel3rKR9AKKH1xi+rXsovbti34k
hbxaQCESEHIKkGgXW3Pi6o47N3rvTCZMfQUOVBMyAbxVykaE44kdLp33w525g7ms
```

```
HXo6I6BV5pIP5LzKgqC+grcFKaslHNgx/Ulc0xdYR87eB0pjrvu8Km0AabzMqaIU
c2MaZiZx1p081hpkwxq49kE/gqzRUeTm2gCSlpiR6qEvDuUjetmeCaBH+b4dvVRU
8J6orGOhKFp5yNv8pTxmVYHl05JcjfQ0enjbCnlVt14ro+yuYcpBhjwYlHjJNOsK
yd3ceuRRKbwH0i5OTbK3TwG19I+1JnUrTq6rYKk/FUanQ35DWjpPavdhBcTDgSWQ
zqJJlQ/ohh14T1KMvzC7hVHiAWOIGAnlkgHF0I5uUoz6exhrN+iFg7fkCkxJAjsq
KlT6lXlv/eLwmJ9yYcbYAlU9DfJISIBScD0AmY45Q1Y3rQsfHPSB37Cjam5M1eQY
q3cc1lbskiaMeOSEHHdxdofyTTN5gDCHMOUBgTsFn6nr+LZVj15xECpjxgTigBCu
Da7i6FlcOyCPDNX/ktG46PFzMCvov+IisDm3E1GMkH7bjQeIpjJ5OzyzAlNKhpsL
wtr5PSW66oTqeF64dOegwlJDNvoa8NzN5hMzD++Gy2YkijQ/WeYhkWTDAQMch7Sq
ks0kVKvNzx1T8nfCO/QDU6a8E+UnejBAQi6wS1BU5nQ1B3Xiy6Cda76PNppslyjp
aY0hifDuxfhLfUl8jftimCOm8WkX6iGtobaemLcq6hi1rAN5c2GwaNu2uYPcKMo9
iSTTGAfgHHbfp5LsZy7J6bUBRG3lWrp16zFJ9vhNWJ3Y9ppkOeMZEsmwrINNaU+S
aO+Kx6Qae1b2cT7W6CfMUgFl5zsxyXt5MHDLIPsjaRb1C613ajjLeirCT2p82U19
zPqw7+YxLEp5RfAQrUJ46N41crO9mr5Jzf9EyFqZMPXjwhK8Bn7qSHM+3lTkOqWv
QWrDc84Nh54ZV267GbL1VK+Y2IzmDGu/gOs8FWo8MOtiMhOBDjPVO+H78yjJV3dk
V+SkImA9OVxjMCjdj7OPUDYpzaTKfs+7D+UH7MGCGFUVj7aHwYFaapX3f5H8ZCoy
N2sa2UQ3O240J62YV9hOFunyciSOrv58c5JwWO/clMEUy6uh6rEcOGTiO+glS+I+
M1W8R1srDKScPyJ90l2VOtvFMqkIGKce1E7k/GwkkxlzT8o0SEKJt+XQk7p8APwu
dkeH0UyqxgoPrbKjhDkwzaK8+8e9yDY0PYWxRATikaXqEZtJ3M2Yy/KVY/epiFPf
5k+INNrDLe57zvP1Kg0c0Nr5mql2QT2jcr2rdGEWM0/1oNLlesmKqm7sCxp9Yky4
3pagPWZ41X2CHJ06xJ/fsnlIUNTBYpdzSHtg7DNd+AWVkMpvge/JwZaRjoakoRAn
PrSvDF7QrLu2hKNTq2L+akOlAULqET5wMRoih/h4PWf5JNziJDSHnmNY3jmR+e7K
rW0SeczSjg/3dwx0Z2jl48TjPqQaleBZ9/cakgSaxY4nsH4jB1m5VHRyCNmCVMNk
iykfrVnCdEIYIRI7gdECvO6yGKCzwXTZtHAdQCOBkpzrLF8OzQF9wKwTG7x/nGki
lJR0WcwUtZyUI6e5sT92lPG2QOQOpcAtqFmz3/GMxrT/18L5GHIM6ynAsqJ6JH16
J57gixKv8spUkYT2bzJQWbSdq92fp+olwM/AAVurRqOhqOtVFuAnpK/xWzcDBO/i
D11Y1BU3GUk0Yya2RFHA24hmDJdfPgT/7DiCG13y64EQ3WUo8vz7KnYp2UKSLqAn
N3/2Vx0wpnuE7SwMUCQPlKz+Q3fZZZkKtgW739NT5OV63zPblvzWMBUjV+KYByoF
hp7RNLoN0UKRGy5/vX88/DDyoSs2DOi2NZb/A/tqNTQ=
```

C.3.13.1. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIITWwYJKoZIhvcNAQcCoIITTDCCE0gCAQExDTALBglghkgBZQMEAgEwggmEBgkq
hkiG9w0BBwGgggl1BIIJcU1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUtcmVwbHkNCk1lc3NhZ2Ut
SUQ6IDxzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUtcmVwbHlA
ZXhhbXBsZT4NCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFtcGxlPg0KVG86
IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIwIEZlYiAyMDIx
IDEyOjE1OjAyIC0wNTAwDQpVc2VyLUFnZW50OiBTVVBIFZlcnNpb24g
MS4wDQpJbi1SZXBseS1UbzogPHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1i
YXNlbGluZUBleGFtcGxlPg0KUmVmZXJlbmNlczogPHNtaW1lLXNpZ25lZC1lbmMt
Y29tcGxleC1ocC1iYXNlbGluZUBleGFtcGxlPg0KSFAtT3V0ZXI6IFN1YmplY3Q6
IFsuLi5dDQpIUC1PdXRlcjogTWVzc2FnZS1JRDoNCiA8c21pbWUtc2lnbmVkLWVu
Yy1jb21wbGV4LWhwLWJhc2VsaW5lLXJlcGx5QGV4YW1wbGU+DQpIUC1PdXRlcjog
RnJvbTogQWxpY2UgPGFsaWNlQHNtaW1lLmV4YW1wbGU+DQpIUC1PdXRlcjogVG86
IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpIUC1PdXRlcjogRGF0ZTogU2F0LCAy
MCBGZWIgMjAyMSAxMjoxNTowMiAtMDUwMA0KSFAtT3V0ZXI6IFVzZXItQWdlbnQ6
IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjANCkhQLU91dGVyOg0KIEluLVJlcGx5LVRv
OiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5lQGV4YW1wbGU+
```

```
DQpIUC1PdXRlcjoNCiBSZWZlcmVuY2VzOiA8c21pbWUtc2lnbmVkLWVuYy1jb21w
bGV4LWhwLWJhc2VsaW5lQGV4YW1wbGU+DQpDb250ZW50LVR5cGU6IG11bHRpcGFy
dC9taXhlZDsgYm91bmRhcnk9IjhlYyI7IGhwPSJjaXBoZXIiDQoNCi0tOGVjDQpN
SU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1UeXBlOiBtdWx0aXBhcnQvYWx0ZXJu
YXRpdmU7IGJvdW5kYXJ5PSJiY2UiDQoNCi0tYmNlDQpDb250ZW50LVR5cGU6IHRl
eHQvcGxhaW47IGNoYXJzZXQ9InVzLWFzY2lpIg0KTUlNRS1WZXJzaW9uOiAxLjAN
CkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQNCg0KVGhpcyBpcyB0aGUN
CnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1iYXNlbGluZS1yZXBseQ0KbWVz
c2FnZS4NCg0KVGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBt
ZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVk
RGF0YS4gIFRoZSBwYXlsb2FkIGlzIGENCm11bHRpcGFydC9hbHRlcm5hdGl2ZSBt
ZXNzYWdlIHdpdGggYW4gaW5saW5lIGltYWdlL3BuZw0KYXR0YWNobWVudC4gSXQg
dXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gUkZDIDk3ODgN
CndpdGggdGhlIGBoY3BfYmFzZWxpbmVgIEhlYWRlciBDb25maWRlbnRpYWxpdHkg
UG9saWN5Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQotLWJj
ZQ0KQ29udGVudC1UeXBlOiB0ZXh0L2h0bWw7IGNoYXJzZXQ9InVzLWFzY2lpIg0K
TUlNRS1WZXJzaW9uOiAxLjANCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdi
aXQNCg0KPGh0bWw+PGhlYWQ+PHRpdGxlPjwvdGl0bGU+PC9oZWFkPjxib2R5Pg0K
PHA+VGhpcyBpcyB0aGUNCjxiPnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1i
YXNlbGluZS1yZXBseTwvYj4NCm1lc3NhZ2UuPC9wPg0KPHA+VGhpcyBpcyBhIHNp
Z25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0K
ZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVkRGF0YS4gIFRoZSBwYXlsb2FkIGlz
IGENCm11bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5l
IGltYWdlL3BuZw0KYXR0YWNobWVudC4gSXQgdXNlcyB0aGUgSGVhZGVyIFByb3Rl
Y3Rpb24gc2NoZW1lIGZyb20gUkZDIDk3ODgNCndpdGggdGhlIGBoY3BfYmFzZWxp
bmVgIEhlYWRlciBDb25maWRlbnRpYWxpdHkgUG9saWN5LjwvcD4NCjxwPjx0dD4t
LSA8YnIvPkFsaWNlPGJyLz5hbGljZUBzbWltZS5leGFtcGxlPC90dD48L3A+PC9i
b2R5PjwvaHRtbD4NCi0tYmNlLS0NCg0KLS04ZWMNCkNvbnRlbnQtVHlwZTogaW1h
Z2UvcG5nDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiBiYXNlNjQNCkNvbnRl
bnQtRGlzcG9zaXRpb246IGlubGluZQ0KDQppVkJPUncwS0dnb0FBQUFOU1VoRVVn
QUFBQlFBQUFBVUNBWUFBQUNOaVIwTkFBQUFjRWxFUVZSNDJ1VlRPeGJBDQpNQWdT
NzM5bk8zVHBSdzIwZHFwYmZBUlFFak95d2l3WW5DdGtES25iY0xrNjZzcWxUK3p0
OWNpZGtFKzZLd2taDQpzZ3J6ZmNxVk1wTDJqbzA0NDdnWURwZUFyaytPbkpIa0lo
QWZUUFJpY2loQWY1WUpydzd2anYwWldSV00vdWxpDQp2ZFBmMVFaMmtERDl4cHBk
OHdBQUFBQkpSVTVFcmtKZ2dnPT0NCg0KLS04ZWMtLQ0KoIIHpjCCA88wggK3oAMC
AQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgP
MjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBT
IFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpM
LcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrszyidmbuZmOpB5voVQfiLYYy3iOx7Y
OqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF
5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEH
AMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z
5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAAaOBrzCBrDAMBgNVHRMB
Af8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGlj
ZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQE
AwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj8OeOr83zdw8wHwYDVR0jBBgwFoAU
kTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCcsTKc
FqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4FzkgRyOg31/+Cw7H8e30iLrPIFlWN
1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMT
g1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7FOD7PfB5v94M5274XYx
W2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8A0enITGXnoEkAFvvjiCqh64P1hIe
Morj36pgL19oWZD6YrzSWHUz1F00juyuOfQsqm6hvrDTqNpHNZ015fOURza1SkCv
i9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqG
SIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEw
LwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5
```

```
MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJ
RVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2Uw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgWPk2af0+StijS
NOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHUa4xQUl5JO6VqY18LANwORjrc9BaX
4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4D
xMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3SryCqeHEFbZFkB4urMk4xrIJC3Cz
WruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog891
9MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgEykRiVokFQgqQ7XNDU+r3SeOWwks7
AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIB
MAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggr
BgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYDVR0OBBYEFLv2zLItHQYSHJeuKWqQ
ENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3
DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOHG25nY/0eNARD6/oF0/sYonX2doiz
cGMk53riugAocCn5zbzhW/JVdYn30UxfyrZlRAzEf7GHqgB/NyjOad3pdpVYeDh4
ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqGJdGf
8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+
Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI
364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCAfwCAQEwbDBVMQ0wCwYD
VQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExB
TVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69Phq
zpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwG
CSqGSIb3DQEJBTEPFw0yMTAyMjAxNzE1MDJaMC8GCSqGSIb3DQEJBDEiBCDqxAGg
S+1eHkWHxwhKH54BovlMmxx6FJnth3m1aP2z+DANBgkqhkiG9w0BAQEFAASCAQAF
sIpGZtBsgrjVl9N6sQu/kUOdnbGSU9JKm6bXL+1vef+4jDckomzjYI5A1sKXxfsK
nBWwgEsEv9V03839X1gMAUc09cx1wwcg4LAUEDWgscC/iNJQo6Xm8fTs8yBMiM/+
0yMrreXIgeXR2ikTG5ub9mPrnxOxaefdnx6HMTh6jGmIodN2BAPIW2KahYYS0BQZ
g74NYeBJX1euT3/ZUqLmupQ0bephgj14pNcslj0qPSRmBf8pZv/9tzYOuSj5CwK4
pzvzfqRN6Lsz3AgFpXd0m7RiYCEwcAkgLLgJ4brnvtASUAmKuSRJaePB7Qcbewy3
4DJRpBBHfebD7Zg7DtDN
```

C.3.13.2. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-baseline-reply
Message-ID: <smime-signed-enc-complex-hp-baseline-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:15:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-baseline@example>
References: <smime-signed-enc-complex-hp-baseline@example>
HP-Outer: Subject: [...]
HP-Outer: Message-ID:
 <smime-signed-enc-complex-hp-baseline-reply@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 12:15:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer:
 In-Reply-To: <smime-signed-enc-complex-hp-baseline@example>
HP-Outer:
 References: <smime-signed-enc-complex-hp-baseline@example>
Content-Type: multipart/mixed; boundary="8ec"; hp="cipher"
```

```
--8ec
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="bce"

--bce
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex-hp-baseline-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_baseline` Header Confidentiality Policy.

--
Alice
alice@smime.example
--bce
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex-hp-baseline-reply</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_baseline` Header Confidentiality Policy.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--bce--

--8ec
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--8ec--
```

C.3.14. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from RFC 9788 with the `hcp_baseline` Header Confidentiality Policy with a "Legacy Display" element.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 11205 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 7286 bytes
 ⇩(unwraps to)
  └┬ multipart/mixed 2668 bytes
   ├┬ multipart/alternative 1427 bytes
   │├─ text/plain 482 bytes
   │└─ text/html 642 bytes
   └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID:
 <smime-signed-enc-complex-hp-baseline-lgc-rpl@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:16:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
References:
 <smime-signed-enc-complex-hp-baseline-legacy@example>

MIIgTAYJKoZIhvcNAQcDoIIgPTCCIDkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBADQPkIuGlBhlGBvHWV+5XhSHz6YEXDsOGhxo
lwaqsHHut09RMi+VovM7fasvln4F4tpKCfYbV5kAkFrNFB7fY2thHH58YpkABzF4
oA0kDcWHqVho/AVV1n0Kf7kplDCR0uPfibSgWjJQcsRARuwB0aRAkUMJKl9EcZgX
KWz54wcwkZkcKGn2SxhWSea6HqhB1no0Q0Iexgzl4LdEWlcZWkQYfWZ6VAY8r5tp
h0txgujzFUFuYLebbKS8LC2G2jurs+ktsSGDwnLzOqSeQyN17rlDnEC+aQMmTsRI
S0DMwKAb/P3z5u6jk3Ryu2HRBIZsTsJhIhgkuoZqEFG5/ZS91I0wggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAR0Pqih31TIW6ROhwnDGcMz2i
5f9z+HpFsjLj6EJ5LU3DXhsdT+6XcF2fqtCJUjvIgqVBj/5ixRYR1wPzypgz/QI5
MYBi2hrr6ch/tWyUDSV5R2FKLD58u5ZLlt5KKW6oyW3L30zB+hl1NEaIjUFyMSJm
Up6/JEPDeJwg3fAygH9XHUxE1ocTgWuVyVqFsjyzAja3S2cvUOvm6smEGdPYcBxc
```

```
Lr1zALPmct3Dikn/pTZizIDA1zQR78mwbPYJ2mJsLYxGAjoPhEh5X8y9PrzJNGsO
gQW1UtLI9dDSjrijLV1vKWWaV2coMcsXxQiLAVoVWDJxjEDM2UoY2ymQAX39HzCC
HR4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEGhYozFbuzK33IcI4CwfeAuAghzw
eiwNUm6ghKAi3x/wM+7u99irte7m5KiQwuC/6W88BVZk+Xu8rGHeHgl8Py8Sdfxx
e0MvM1Bdc8NwsUAJK4PphSZkK8FPKczvKF7kV1+XzBTQRflesQido0IOKfLHDBMS
NKbvK8haTRiB/4EBAPh2C7evfTYfKeN6Wd7GKkzphO58dB8t9ABpJP+mCG+hvuhv
v3iLc+oYLfFCbaI0c4//GUXOG1a0209Y96m463rYQyfneKlKN29UysTC4ziEAtgw
PhZPf3kjlEaSfxjicrEjR6d7kTlRDhEyH4QOexadosQYTXo+Fg/2m2NZc539z0Sx
DXSy4eyDDI85wWQIsLQ2fh599Vhag0tXk4+ElCzdSy+UqXwmX8hMBHZoWU0j65No
PgWcZQ4IT7qctJd9NDBi3a3R6OFYJSPjNEu1TmW6kEQlE+I0PtlxiqTDDJu9odKt
uQzHsQBEG+kDFTvtPIu3OcZniFN1Xhm4cc1iZMdc+fvwom9SXl8R3fiK3zFbOZbT
C+/DQWjxrjsbCdukOfXqI1o72SQwgLuHDpfs2Kmz0bHrMlORN/RAhKKem2Kb7s7g
lPBbmp9zkvErc85RU06EXRsI5SVGOfIfpC6B49tXJhr1k8Dmm9v+vsQytrco+jX4
H4Sl38a+9o6hJBQT09l2hBdD0g/q80z8a1V40hGwlR4H50jMVXlEJp+ksfIS2HVl
/HVEe6BNkxhD6q9ti7Lg3dDODkh8meLgkaXirmSC/IDwY4IzVepKWnENn5iMemf3
8/nZ6g8m7xph0riq9NLXLqecLqQrhJfUEvBtxw0bm+OxZGkPel/5ib941dSNKexk
DZ2cq4gAifNoAWu9q9S9bz7+ODD68hRdoQQuUvDyV2FzB6cyOBeoB2tWLnknl3FN
rYiqz/1S76XP9duGIf5rmb4rhfAJlnrvKipWfGJ5cUSm641Dr63ou+HaOMaXf7wS
p3Mm594E+vI9Z0ri2A5bmbEV3dC1l121YFX5xfbU346akePA9V/KzkHPNJi0k0j9
2RUVtRA5FmXizcTRi2rdY38uIEvBOj7jNLzGErG6F/li4OEm7SiwovzvuUsVSSON
tswvOz2xkJb+WaTc6obJCWycUUm9Dfdmcl+SGwCMf+i6zMgCNUf4TBuLw0HBpCdo
zXbBmbiBRn9UD0aZknlxwOVevKqORyPVO/u9zRcSgHzSPM5KASpLO417prcfZhL4
FcrmPDisDWYS3WN67eyXyWtM2aM7LnoUl5kPNYlwBe7qIaxwch8i9k0KBVcU52gY
mfJnMP8okcU0FauGPZBN1M96/M35mrj/IRiQJod0xM0XaqJlZu3A8TlRLfaGnleo
JZ+a5r1Rx2gJ5/QMUV5yd+Bsv67DYu2l/TEtvElnfJmm2/3kFN3bmHKb2ibpkIMP
PNF9LWD+7D3qr1vzKl+jp3eLYsskDs/i7cd+MIZ+z4T3I8WAmpBP75LnSHk/V6rY
nWyC3MaB4OxKWBsu7iURIv+hoD8wqGenoiG4NsEPNsuhyuPz0BVPkEFm1aVh8XzZ
qbg4yh7g3IlXlJPMW4QChsPo6lKOUPhaqExZucEgKQye7OHA7u1DIOsmiUZBNSz6
Mc6HqKO3lU7akhQrKNZjOI7pqR2CK9pQVVUW66DYSV6wI/Ms7mnr04G3Hl7Nvt2Q
JD0pLEGGEBDcT2SibcXxrRgls9CWPrV2+lbjG6tgwDRwq/lFaFQMt16SHB6z22U8
ZLmlk3Awi8m21EoEiIMJwandgQ8kURItgba2XRgiuE7R0b0XqODRT15+au9At6b5
RP8NZ6qlpmIEVT6bCZloyQbMT1pPpdM6FXW4fGZzQI9kd73gbhg3kMnqmEuxqLvV
e6jsqTr1a7BH2vYTMFQXfqYSoof6WTac7IqmC7Wcu7Ydkb1liCJ/Ne4FJ0mlx1Sq
9Poz/zpgjgbTLQ5QLjvMqkdVJAQpQa0QWh4htOSkgrMbWbybZHoEYTHwaXudlw6h
TmaPxrDL1bFYRPf5l35e9VoHufhjE9wAEwU08adShmvxPbGzYSSWCU20zQ6F5GdE
O7L/OwtFl+f7b95uv8M2FT4HDNPRK8LrdqvFYow6++1/2QsEgGZny/lTOzbcZl8K
HaGT3rheElAD2sr6vvCALasiXWmJ15cZfpn0rYQS9V+cYo2X+wi7vZ4SWQsGhoK2
yLMK+M3V2Et/4gfSCKN5uBg4TtgHSFYn1TQuEvTjcLiBPZTL+JZdi5YhBhkhSNwI
8Ka8O8TE7aYrkBlU2SLT3RaTFU0NP7uOdCSxTudwShB6yeBPySDcv8U+CYnlzuwo
GAr6Db9leTk5Wjzd4+1KcP5mQ9hT9X11qgqobfGxSCfzLLkSoJ9PvBwNoFn1FwPy
08GlAm/rJNZI8VKNILQhGfiEazumOlmE0IiI/0GxT6oqQrX+OKQfmqAUg20VMXEG
LQRRu9W2QzXlfcFOlDjzM1PjtwGpsM5so+yLfV/vKiFnZfQUgUholBq/cJX2ISy5
TbmljK7/zCwzGoBjQrJxykFGD1xHZwWY3TEhpQoewduLE1nX3lZtHBHvV6bt2CMD
ld639Jczp5QSAq4yGtZjZYUqHqYGIgNqov8GyLfiNaLUhneojo2V41SL1kRIsF5U
EYfjDYXv/MSorcMCI0x8/B+0qxtyd0R05QE1RZnSftQ+appE8XKLVPcFzQ8x+P9g
1yW/+CumfKFKZAkp12qpIIPJ6kAe7Ig0Zd3uFgd6FtXbVMUFHqBHGN7ZFC0JwlhJ
NQBjvZbqAymfdlcsDgqAm6e3Fi1uhg7i29iuryC15icudXoGhdzR41vvqJu/hIjB
tvNW23j19JZuJtu7IJn/J6eqw5nu4UFG5LlhiqjsKx16Ae2r2kK8Nl4EZ9hMhMv+
UOMldoHTno6dsbXkCA0HI5+Uy5ZbweOLOP0gi5ZemoyECyWJTWsCLd22N+EHbdx+
0+G/WAX9y2av+0VXTPqCs6PacoeCg7Dbah0hp/5Amw36ADIWYKjsa6jUFdZtxi12
KDqY69q6dCZm/Ctfn6FVOPhft/jhl4bqGlmRTy7YtxHM8aqoC3bPz4/x9/WuffQG
4zhj8TXva4QHmQnJ/bhLemNz4b6SJWnulNcDvkTetwUrcI6X6/UWpMROLqKmJWbH
ZfC2siIAPZRWsovSNbq4VENFWiP3NUwUUa0AHVZkldg/sNJxbiZvAUBCrMsIDKlS
4RuMY5M//5Zc7AyFiCfmUSn/l9G/Jhxoc6jQhyZQGAK+eOP2WdCrybn4dPeNP2Cv
czxU90kFJwnyre8eN37GL46o7cECX33d60hgL4hPBlwYowczrW+VUdNUbpUlRTGn
Rj+rcHVRgEVjeGsasFb3S5Lb0aY75Wy/pOumQYxc/5Lm4IeF+i2sJuMvJQxuPbcx
gw/J0y0H3VZXOcLbin6GEqC0rkANi3thkU/LjtOUzXHm5vkmfaNXMvXQMKuK/gXW
UP/W2924d7VWajoidXXE1S8XHEllhrT4xkxZ+3Lx8oB8AycEUw8AeGfXx8rdOsri
```

```
VVeG3x/Yi5Prvr1gJxFeNv6Sbwq2RDLep/GJBxIY+tcuTy4Pd7CtBmokIOHCUySB
q1KR6WuhB8/rdfcUa9oooJUPr2nB6EToNAUvNRFdhqzWvvuxT4l4CurGUwc7pM3w
PFaeW5xxadBIDTehRXmoUc4blfa7BAfM9H0IH3r968njQWUfC2XgUh7wpfOAD9NJ
yYUMxfy8RRRwmBwBMA5ja0SZr0myCvEHkK2LOhFFhKLFtw1tocNVP3unRY9UjrgE
T+FAgqqhZEWgPvaKJFDzl7la/T9DVfvpXyTAEX2n1jvL2UYpyV+0bjP1/7cEnvTD
Q/KvrQMszNS8Ams2VZiqQfrV9odGf+OXGO0cCXNdbWJtRC8TV4+mSnfPO7f3dHvs
fOkeN7ArJmiZIUevxsgQe1mCFGp6+L4/XPalGV6LzIUY7kS4HNW7gpn8lDYw6Jwv
TMwvJ5gUJw7cAV4zm+8Syx3IdhyT844J4e8s1nxiBwYDSgfMDa3tJVxWZk7CVaFQ
lSH2e3j7hlWDL2gZ0BZemstT/snE3UgSlQYOy39HohGIffuwVxKMkcRpYk1ADHU8
GB8wfDAsSDQ0s452ucbdaY1k6iG2XxjBiovNUiJs/IYgj3n+Lq3MH1WpkRgDRj8D
4vd59gm9YzXa2lrielU2I+qdxTf94P7QhwQitrsvmpmxA5NAG9ola6bXAvUJqilO
q0wrlB7l0tiahXlKIHQEVdQB2rTSNZQ5EtcEgAYGs/Lh3FL/pm4Rcv+DrBuFormk
YVTElDSNesh8Q2EmOPD8zaUU86bYboz0bDtA6Ry/H7RpYzirBr1ymwvGSeCnLSnW
KcbbXS2ntv5ohU/Ksn27t5pJJ1n7bVbTrwoeJ2J4kev54vbjupoR2am97I2Gzlcs
G+1K8vJ5L/ECkdZQx+4BU/5a5be3eMe5TpNDmMfT0WRkSC5CLfj1/YqXAIjmxVDo
CJD25BaX0SwSooHrl7hQEvax9oAEjgsG1xJTYU0C9gEUF6abW9hravxxEYgWvu+z
11q0rwhWavVshkk07DPjpcZP6FOvsEJNLfmw+Ob9RcOpaQUJh9xpw7avQSkeQ/hk
K7LElcxUXZJYGEKlu2Ou1vuczdFrJob3xPn/3DE+vfopaQl1XFxFhdkFtk630JX7
3gouMVNfdmBgsniIoe7CutNayFoNiCeSbUNDPsOFNiWR/PGiwUsF0pOs2fK64yhl
dCwHijMoBLN39jj+LJSnzMpBB+lxiqTAFrcBTc29CDK94VOACLHs9fhUdMmWMu6q
Ms9eTzWZ7cHZpPZTVNnXlVIKx/NfKFl/QMr9ZYYHX5/sxxMXNjjiSM4zvnxvysaf
zOB1YzVgKdc47IvsXYuvN6+jZXoYzNZN65yEKu6ZS51TpOyvl+WyA3JWYGm4EZ/E
IIJhnxhmlhJfD18GztEvTzLkqY183BkxPdsi01j4i23uxWIhX6WBUUph8hcjq7+f
X0KdAA/ObVcE1QQW8yYbKagulN+WJDU2LENgPeNbX217JDgmWgX0pZHt/fIzBucD
Et6r+leFWvbezdNAnCj0JeqRshjz/wwaz9u7gckF9YBR1XEqNM8fePXeYGNznlbZ
qQYyXivDvFmIgXwebiLTyR14OA4y6ZmbQPut9ne26a5r+tmzpD6/Ehl6EaH4z2Yg
IYIGnwRy3Ri8u7AuAZTEvv4hzsUj7MpIV35mbQNKpKslDgfD1jFsWAlLo8SJ25iA
WvKuYJAXFqBkksL0ZIMuG37O/HjVHESyaahCBy5M2I+BblReyH4dxdZB4kdWBuJW
jwoN964SEpypk+tP9OR1IBHpIuu+Oxvg8iZri8JG8sWjqFOlLSSdG5V9An3/nX1P
hpGa7sFpQUIxRuV3RH8VuhXVRqeu3M1cIiX53W+Iyuonjlv82HvS9bN44uE3sO2h
PT0NOgPZMqG9Letybzt78iwXS1qQl76oMDFfx1iHS8n5y1nSkzzedvnGNKzlHqdF
V3QclzBW6T8mPrqGp95uTBTDSC6EPFZ5QG7E8fw+8d8GJjCHQah/DHeEo3fRQAL4
GOz+KLHmkjocKZTWVLTVw2sHmo3k0wCk0TSUEjjfSQE2n7QOdsOXQLaAMYvyfw5x
RGfPCPyjMSeZxosnGftHp3u6ZlA8QW2CV/WLYai+Qy22z5jvhN+duvQbEI+6p4RU
BMdDZH4xGF06aPfpeD5f0eH9vsXoRIUG9TUB1xZ3yYLrpQh+AXjmEWzG7b2pa5Zt
fNC6J0c9aKvdLY+HMtdQ35Gq+wYVMMtyZLDRDcs9sDnzubxP5loaePKahPARYhU9
07/cKG0AHZPl2ffWGC0Xr9ayOT41LVL+Q8TM5syz6c1ZAanK6nDCWf2iksIrkQQt
/ko3R8s401/ajye3AW9lWrW5eUOE6/dF41Ec+znHd8GGk9wH/rG6uVeet1TfsrkZ
OO4v8Sy/bgs/KFDZH9p1Tw7skDdFl3ER5202JrVgcBrVTTjrsw1PIFb6lFCyoguF
z0jOaBRgGkd13IhezPlrr8t1fPppZvUKCYxgv/JPoRAxnTrjTtGv6z0R6POV0vZ/
MZBPDnm0lPa1mFidN7lRAmI0VGhgvY/1+tWKWdBbeV4NtoOheRXZgqGYK57qTkMS
1CglYPADZvwyvVcGtNhO+qVwvjuIYhRSL+kthY6pxDRrFwerzyOw8wGCJXpl3Swm
8Tjip93eMjniZ6k8e187E2iW5ykgZWheSrKjQKFVj/zUjbwxiwfw9WlTUY16O+Fu
Nkm+qWTz0lhxmm4PoKSTeTn3uMBaFh25Vc463RGTiBdj43Mtm4/SMWfKEJ93kFgC
bISYo3n3MfXJZsO/AuCDnHMvy1DmpdsG+zKbR5+YS+RgiK4Vf+i418xempcJUfP7
zPlNzSrRt0lncnHij1mWSmQuSR7nAOQtqYWdsasx52Jk8o0XPdixWcutEQVc5vEM
MdaYHqvy/cRXBC3tm0B/JKnbDO+OzaHgUcgUW4GJyKxf3iRoK5CIZlBdW88L8rXh
K+xxjyTes9alqza9rFB/YaBOZiz7PCZ8mgYIfe+BlDH23KfXtaZVLAQ9CQfFO9vX
3Ydu5U2HSCcSmt/+KcWWP5B8RVg8a8ycoF/ZEeTp72Uafx6FFKbJi1LuLOIr7JqJ
Vkn/9wjq+NVOzDN4+bYI9kPFi1LzqTE953xLm4UfBhGFStMeGqCmdK+KOYcA4iZx
MxIhLDtCbOrKsPVxguaom7iDNnkL8klJigpw5qr9SuHv8cTcYpmgY/KlxDcDcV8R
1V5WYamz6KPwdfh1BiigRU6dHBrvNY+fBHEV18PelTqm5TWD/ryP/KebvIsLgQhf
VVF1sWZHB5ZSTFiGmXU088isDjJSjtQ27m0Ux5JS07G1U7RTK9N1ZQwmqg90rXrM
EntLIfVAGwTg10cX8ZV1IwojAPTB1DFYLeYjzDdkZFR6c8pKDtrKqx1ExdUrmj4E
c0gIjbnnnwpgNbQXhfYU25F6opEipOCsTQ/HhOeQjpbwnqaDsqht67NNouKMWco+
T1gKXuaEF5VFMPeIo9YTwOPRtcqtsMullE9vP5jA6QKn0+1zX69ytxwMUy3fe4S0
FefRP6E3taViJv10oWqifzJtyNcsBLn13619yxOug5WBvA8UKWXLaFf5BR1ZYMJp
KG+hrREh2o0cojLooFgL82H5bJYIqiCnv8pb124aghXsMWapot6JcQjjoG66Ni9e
```

```
JrfixhUMDKqBMHvhKTIocysMLjAZs3fUlkZyByexP4/DceJ2YLmD0tTD50Zx15av
kh9jGBrkYDadsGfunLFfyi+aDhDtC3I4kDYXWE4dLUvVwjjn31sBz7qzICYfly8w
2OgZy7Ao63BHTHX3tGjNer2I4Z5HdYlv3NeCIxAKjcFVuWERF3OOi1r54nfcboVy
p5HVP4ZYZGKqcTaXNTuuCtkTBwYt3SBXe/dbcn7PCwkgW9Q2uwQk2z4/+3Frq4YP
8lcjwimFTo1QODAaQNzaQAzMK0OAAxLDmxZLQdN6NAwgcF0ieoG69uu5fgZGO0NY
qQyP4aWoY7WfXllAeVoDiwWcl+N5WMviK9uBbI+gTem3AiE70dr3roxFlHcArQS9
UZHGS50tTI/4xf5qerK/B9rkU750sQKdvbAJZkXaxg0so1r4qpSRIvsHGfBTZjP8
0OH+7T2VRaBQSb8vGTcONqmzhvWrkf2HUswPFjLtlcWszbHgnhusb1dOPPWkr8DD
CjElwQcg0m+6WPQqIH3QBXt+aOndZ4kHEdurcjwa/AcVHykc/aR8mR0+bP7KRsv7
SVG+hD6hOL2cBVL3HCWF7z/K4f+YSQ9KTF/efP/Kbr2o98zrQ1IhKDIPZ8sJVPVz
WcK+GU0JUDreuVmVnWrvDM3Pk2/3K1/23xGzfDF0S/gF9OPHX1jH/KTnz0KHQxFE
sTNJox/80sTqIsuTiw3b16bG5KAGgeiLWSAzUO7eOU5goB9QWT+QSblMmdumGhzF
jQFGmNL0aaxJa1U/kq6T2NoiLetQPJDEdr6UHloASF/mZtbPlQlgyKxbeS3y468i
tVQWEHyePSzvIYfknfnCeeJtQNaABfICfYBedlzxk4zuyRUSlrenW0RCuCMuIOQL
uRXdnuB2aC3Gnb1KVcWilRO2C+O6HhodXqDNwWSQjku0o2mhbCZ5TAL87GzVSdI6
9FgMsfD4GyH3LnHQDr9jjFqhbARBWqhCJoy62ES8LlLg3E41b1/TEeP6c1IJ54uz
j3H3nhzCPeUA7w7jc324lioLT9QtiWnKSE4OkNarGwxGq+lJxAZ3qafimRe/DGC0
ysAysJQTLN4MgsAr1RDvnXY+UD/J2HrZZlYguTLc6Qz8NclJO0eHYGec8hbWw4Ji
OvpVNpqSKi6aW9atAWONoQ0c6YJqetNab1lSWXSYlZTwZnf3iSlgC5x2k2zrQOkv
kipyixPl+BK0cP2gzXZihacodnfL8QJVZuNdCzfM31skCehMV4moXBmQeOGU/z+J
y2jFdZk3APNq8Jc0fDpqtGedriwbRnmG8RysfS5vaa2pdZdtpLb+TK9OyGcDBLb9
2anQNQnafUXz4AKY5j8C7+eTiWt5bfUtN9zqVUcMxcjpPitaldyG0xMrXMThftq6
PaUFS6pEnw3Rurz67gp0zBIa+ajmwFj09LqPC95JH+PJttnrztgc3B4eD7xuWiW4
AWybu1vWGY9bEzwNHr6Jn2XMx4T5CadOXGzid0JcoIu+/SpME1fWLBNr9H9hCC+W
drz/lwkYijOvw6RPdsp2Go10W8/DXRdcses32WZyfr1RZ9S+BfJs01hQmVh8cs15
/aQhCPIxtmWQUKXHCzWwKI6J7LJyugfpImWGL3Xt9dvwIz62Ma3AECrPx3SsOLMA
y5Mb03lft3FXOD+ZQs6kxcS/E7NfM2bch3BjY/3jOk5b/YxZeUxvXAWJ+W6l1hva
D2fyDbAfCZTtIJGEc1vxO/7MxzDyYnLuFavEPhh0YWB5S4tbz/2nWQ23SzoWazo3
s4RIO3aPl9ogTraNAtkrB0BPgxdFzUCbAEf7guX816wSPeW72Iess7TUyt1TK9wV
oCOlTEfuggTROFX7/VGfduLQCjI/8xvfQguvYDt4NwUAdeIu70a5TnO1DOxPioz8
wwBrXOhzXEd1oZ4Xmc9rxqdCsq5s7bI7M/0FpSs53nuQrlZDqTrJMI+rW4jhIrb/
xJmDE2/0i6fUy1eZWMpoDDcD2Om7S5vbOquhsuyV8RbiPXnoCJsNMbJIIIotkVMR
5yEhltLdD33cwnqKKqWcHKUO5fWtegP+ZIVxIG226U5itJbiU+uj0TUZsbCu52uI
9RQp3Q8gMwkQ3PAaXqHmknVAUeTKSU34RV9kn/rlN+1mFC49ribsHUVaPzlG1sMg
Cg3rt243Q2zMmdwdokmUT5euga4Abw9xhTRgoSCEGoQhlMW1PO3ZVs+Nmr5QQW71
ITfHV2UGUm/F+b6iZWA+TQ8RgHTVzHWrUSlJuCqpcFxxY/ezzeB0iappZTkGN2E9
77owuDPHV8CyTQvJs+v2YcP+rgBXtCzIPxVjz0v/mfNvo7fXo6y+709LXj6hhAro
xBPAaVxvnB395oaa+1ZMCDOzxmSYnpMj1qP0pnwYdvGsFeUFWZa20O4gveQ2qMc1
r6WYj/48a7roSpjBTI+ZFQ/5EnkdLBJ0DoXi1zncQYPnHl9VdXDuucegLlkEhF7W
dhiRCnLWywqM9o5+WwAFrUq7IQZy+g5Ar93Ymwitawv7XsMw2SIeR0Nisf1r23Ai
OqFSKIhOajCncNFAGCv9fC6/m66B7gGba5y4SAOqm7qWpPuVAZvc/kO41v2gAPl6
GpZyX492SC9oN3dOJZELsQ==
```

C.3.14.1. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIUrgYJKoZIhvcNAQcCoIIUnzCCFJsCAQExDTALBglghkgBZQMEAgEwggrXBgkq
hkiG9w0BBwGgggrIBIIKxE1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUtbGdjLXJwbA0KTWVzc2Fn
ZS1JRDoNCiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5lLWxn
```

```
Yy1ycGxAZXhhbXBsZT4NCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFtcGxl
Pg0KVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIwIEZl
YiAyMDIxIDEyOjE2OjAyIC0wNTAwDQpVc2VyLUFnZW50OiBTYW1wbGUgTVVBIFZl
cnNpb24gMS4wDQpJbi1SZXBseS1UbzoNCiA8c21pbWUtc2lnbmVkLWVuYy1jb21w
bGV4LWhwLWJhc2VsaW5lLWxlZ2FjeUBleGFtcGxlPg0KUmVmZXJlbmNlczoNCiA8
c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5lLWxlZ2FjeUBleGFt
cGxlPg0KSFAtT3V0ZXI6IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcjogTWVzc2Fn
ZS1JRDoNCiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5lLWxn
Yy1ycGxAZXhhbXBsZT4NCkhQLU91dGVyOiBGcm9tOiBBbGljZSA8YWxpY2VAc21p
bWUuZXhhbXBsZT4NCkhQLU91dGVyOiBUbzogQm9iIDxib2JAc21pbWUuZXhhbXBs
ZT4NCkhQLU91dGVyOiBEYXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEyOjE2OjAyIC0w
NTAwDQpIUC1PdXRlcjogVXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEu
MA0KSFAtT3V0ZXI6IEluLVJlcGx5LVRvOg0KIDxzbWltZS1zaWduZWQtZW5jLWNv
bXBsZXgtaHAtYmFzZWxpbmUtbGVnYWN5QGV4YW1wbGU+DQpIUC1PdXRlcjogUmVm
ZXJlbmNlczoNCiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5l
LWxlZ2FjeUBleGFtcGxlPg0KQ29udGVudC1UeXBlOiBtdWx0aXBhcnQvbWl4ZWQ7
IGJvdW5kYXJ5PSJiZWQiOyBocD0iY2lwaGVyIg0KDQotLWJlZA0KTUlNRS1WZXJz
aW9uOiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L2FsdGVybmF0aXZlOyBi
b3VuZGFyeT0iODI4Ig0KDQotLTgyOA0KTUlNRS1WZXJzaW9uOiAxLjANCkNvbnRl
bnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQNCkNvbnRlbnQtVHlwZTogdGV4dC9w
bGFpbjsgY2hhcnNldD0idXMtYXNjaWkiOw0KIGhwLWxlZ2FjeS1kaXNwbGF5PSIx
Ig0KDQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxp
bmUtbGdjLXJwbA0KDQpUaGlzIGlzIHRoZQ0Kc21pbWUtc2lnbmVkLWVuYy1jb21w
bGV4LWhwLWJhc2VsaW5lLWxnYy1ycGwNCm1lc3NhZ2UuDQoNClRoaXMgaXMgYSBz
aWduZWQtYW5kLWVuY3J5cHRlZCBTL01JTUUgbWVzc2FnZSB1c2luZyBQS0NTIzcN
CmVudmVsb3BlZERhdGEgYXJvdW5kIHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBp
cyBhDQptdWx0aXBhcnQvYWx0ZXJuYXRpdmUgbWVzc2FnZSB3aXRoIGFuIGlubGlu
ZSBpbWFnZS9wbmcNCmF0dGFjaG1lbnQuIEl0IHVzZXMgdGhlIEhlYWRlciBQcm90
ZWN0aW9uIHNjaGVtZSBmcm9tIFJGQyA5Nzg4DQp3aXRoIHRoZSBgaGNwX2Jhc2Vs
aW5lYCBIZWFkZXIgQ29uZmlkZW50aWFsaXR5IFBvbGljeSB3aXRoIGENCiJMZWdh
Y3kgRGlzcGxheSIgZWxlbWVudC4NCg0KLS0gDQpBbGljZQ0KYWxpY2VAc21pbWUu
ZXhhbXBsZQ0KLS04MjgNCk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpDb250ZW50LVR5cGU6IHRleHQvaHRtbDsgY2hh
cnNldD0idXMtYXNjaWkiOw0KIGhwLWxlZ2FjeS1kaXNwbGF5PSIxIg0KDQo8aHRt
bD48aGVhZD48dGl0bGU+PC90aXRsZT48L2hlYWQ+PGJvZHk+DQo8ZGl2IGNsYXNz
PSJoZWFkZXItcHJvdGVjdGlvbi1sZWdhY3ktZGlzcGxheSI+DQo8cHJlPg0KU3Vi
amVjdDogc21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5lLWxnYy1y
cGwNCjwvcHJlPg0KPC9kaXY+PHA+VGhpcyBpcyB0aGUNCjxiPnNtaW1lLXNpZ25l
ZC1lbmMtY29tcGxleC1ocC1iYXNlbGluZS1sZ2MtcnBsPC9iPg0KbWVzc2FnZS48
L3A+DQo8cD5UaGlzIGlzIGEgc2lnbmVkLWFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1l
c3NhZ2UgdXNpbmcgUEtDUyM3DQplbnZlbG9wZWREYXRhIGFyb3VuZCBzaWduZWRE
YXRhLiAgVGhlIHBheWxvYWQgaXMgYQ0KbXVsdGlwYXJ0L2FsdGVybmF0aXZlIG1l
c3NhZ2Ugd2l0aCBhbiBpbmxpbmUgaW1hZ2UvcG5nDQphdHRhY2htZW50LiBJdCB1
c2VzIHRoZSBIZWFkZXIgUHJvdGVjdGlvbiBzY2hlbWUgZnJvbSBSRkMgOTc4OA0K
d2l0aCB0aGUgYGhjcF9iYXNlbGluZWAgSGVhZGVyIENvbmZpZGVudGlhbGl0eSBQ
b2xpY3kgd2l0aCBhDQoiTGVnYWN5IERpc3BsYXkiIGVsZW1lbnQuPC9wPg0KPHA+
PHR0Pi0tIDxicj5BbGljZTxicj5hbGljZUBzbWltZS5leGFtcGxlPC90dD48L3A+
PC9ib2R5PjwvaHRtbD4NCi0tODI4LS0NCg0KLS1iZWQNCkNvbnRlbnQtVHlwZTog
aW1hZ2UvcG5nDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiBiYXNlNjQNCkNv
bnRlbnQtRGlzcG9zaXRpb246IGlubGluZQ0KDQppVkJPUncwS0dnb0FBQUFOU1Vo
RVVnQUFBQlFBQUFBVUNBWUFBQUNOaVIwTkFBQUFjRWxFUVZSNDJ1VlRPeGJBDQpN
QWdTNzM5bk8zVHBSdzIwZHFwYmZBUlFFak95d2l3WW5DdGtES25iY0xrNjZzcWxU
K3p0OWNpZGtFKzZLd2taDQpzZ3J6ZmNxVk1wTDJqbzA0NDdnWURwZUFyaytPbkpI
a0loQWZUUUFJpY2loQWY1WUpydzd2d2anYwWldSV00vdWxpDQp2ZFBmMVFaMmtERDl4
cHBkOHdBQUFBQkpSVTVFcmtKZ2dnPT0NCg0KLS1iZWQtLQ0KoIIHpjCCA88wggK3
oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMAsG
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBM
QU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4
```

```
WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExB
TVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfkacKTg8cc2OtJ9ZSed6U3jUoi
ZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrszyidmbuZmOpB5voVQfiLYYy3i
Ox7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOaGdmnx4OG/e3p1fIKM0dPzZLo
OAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXCN5XL7wWTLMLeNf9Byb5ksKqU
uqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWzB2zNS2OF+XIVnzRG5DeoULq8
v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAAaOBrzCBrDAMBgNV
HRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNh
bGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB
/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj8OeOr83zdw8wHwYDVR0jBBgw
FoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCc
sTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4FzkgRyOg31/+Cw7H8e30iLrPI
FlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMG
HjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7FOD7PfB5v94M527
4XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8A0enITGXnoEkAFvvjiCqh64P
1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQsqm6hvrDTqNpHNZ015fOURza1
SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnXMA0G
CSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdH
MTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9y
aXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQK
EwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxh
Y2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgWPk2af0+S
tijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHUa4xQUl5JO6VqY18LANwORjrc
9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rT
iz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3SryCqeHEFbZFkB4urMk4xrIJ
C3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfo
g8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgEykRiVokFQgqQ7XNDU+r3SeOW
wks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFl
AwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAK
BggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYDVR0OBBYEFLv2zLItHQYSHJeu
KWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqG
SIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOHG25nY/0eNARD6/oF0/sYonX2
doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZlRAzEf7GHqgB/NyjOad3pdpVY
eDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqG
JdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp7poIccGE6I9Tsg+RrOA9iCQs
Pn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtzOKypyQ3eoZ6EPazXqMyHAVcs
m0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCAfwCAQEwbDBVMQ0w
CwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxl
IExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw6
9Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcB
MBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzE2MDJaMC8GCSqGSIb3DQEJBDEiBCCY
UuDiqUQkX8Y6z7GoBK5oZgbF9o0kqfOxpi4tDaKThTANBgkqhkiG9w0BAQEFAASC
AQAPvlBItCWJNdtkeHveM0hBpLsosoAUG3bMHg0JNi89kzV02YK9YDjFSG2nX2Wj
pYuKJVi7UH1aGCmyA0D20umbcIuBqtWXX+W4SRhzNGR3P+lxlVKMe//qPlTgdZTR
t9Eg+vmJwrIuJVcZk6+tagnOinCl5watJ0BDEnCQcgywe+5EvT7+kRrIV8eZWj1f
7e2ut4xOMYVOKwWBOpBFtY27rlu8rMjqf6JT1wpvGvaXllsTsBPqxfOPe0x321ma
HGAO/tnCcM7FXtFChgFR6rfpRDvTBvFtR81lDbK/vPYo/PevKjR8mX5lgO0GcFwg
30JDp0rABngu4wItcNYBsHNP
```

C.3.14.2. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-baseline-lgc-rpl
Message-ID:
 <smime-signed-enc-complex-hp-baseline-lgc-rpl@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:16:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
References:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
HP-Outer: Subject: [...]
HP-Outer: Message-ID:
 <smime-signed-enc-complex-hp-baseline-lgc-rpl@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 12:16:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
HP-Outer: References:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
Content-Type: multipart/mixed; boundary="bed"; hp="cipher"

--bed
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="828"

--828
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset="us-ascii";
 hp-legacy-display="1"

Subject: smime-signed-enc-complex-hp-baseline-lgc-rpl

This is the
smime-signed-enc-complex-hp-baseline-lgc-rpl
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_baseline` Header Confidentiality Policy with a
"Legacy Display" element.

--
Alice
alice@smime.example
--828
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/html; charset="us-ascii";
 hp-legacy-display="1"
```

```
<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>
Subject: smime-signed-enc-complex-hp-baseline-lgc-rpl
</pre>
</div><p>This is the
<b>smime-signed-enc-complex-hp-baseline-lgc-rpl</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_baseline` Header Confidentiality Policy with a
"Legacy Display" element.</p>
<p><tt>-- <br>Alice<br>alice@smime.example</tt></p></body></html>
--828--

--bed
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--bed--
```

C.3.15. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from RFC 9788 with the `hcp_shy` Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 10445 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 6720 bytes
 ⇩(unwraps to)
  └┬ multipart/mixed 2273 bytes
   ├┬ multipart/alternative 1118 bytes
   │├ text/plain 380 bytes
   │└ text/html 475 bytes
   └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
```

```
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-shy-reply@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 17:18:02 +0000
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-shy@example>
References: <smime-signed-enc-complex-hp-shy@example>

MIIeHAYJKoZIhvcNAQcDoIIeDTCCHgkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAI9iPH5/b2KLsDbl+Gv6Q/yOjrEsmu76WuOA
rQu6BKFkeKtgemTUgvvcbc//DMQLqFXrciCBw2LNPzq6pxpgaaS8xFcvHttAtd4j
pci1n9SJvAggSTzU+vaHUEdgf/PTP5mBDy82PbZx4cZbuIM4prBq6/haUnmxARs4
xSEbfQliaYCSFRt+3GAhXLSI2y+6odiA/0DxltHq+PiTc2SGn1BVyNyxeNpxbAkm
G38L96SPP3lgeb1oV2F6aEmwBKUeMoHoFPfGz3L7aCKCcbaXgp+phC+8qlMPJxol
sPgSToVMCakQBk/OaveXL5HaMHYd63p2G5vBUcjvUsEsyP5N0j4wggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAnQrNiuXf9Kn9FiuopsfQYQT0
L6euHqh4ENdEQeBLZUsvmaO98nqF0Sc6Pe9QKlIJbnFFBHLGD/52Sv5vZH5aLUgh
BCeM5YiBg6J5Di8EmE207ltptn1+mDColCceMsCpiBiSohczFNY4ME0Yd30NsYcY
qEr1TbT8/CqmSBtJrkVVNAi+XCYPYo4yQTlRjneBR066DaPvMsR4G1YZSb/xcKih
5w49gwQO4qf7N7CH3t79Fo+OPRwRDF1MwVMTK3L4BAZzH//M4+h3w3u8XzM2djUK
/4YQ9EyFfhoTGrbi1o7KsZV/fMlmGxaIdtdQ+zny1ZzGijJG0GjKbJ7fxjCHkzCC
Gu4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEECpxXzqAYIhfW/zQN9X1OhiAghrA
gmLziupytMbQFUjii3dvaXG3GoyMPL4f+eEcPVkk+YShdVj5yKdvuD+Ck4hz7YAw
GxVYDWVflW5ofL+YdOiW5/OYwJ/6Q1i8gEmfl3JTnjSA3vIx9wP1bu8K5hS4eyd8
dNbb2AwprX/Fwd1hSiTsnJ0eov9RcdmmTLhyD7yG6VVMZ85ZhJE7i6IygHxq8MlF
Cef4x0QJf7XHmd02Hi4t/7yjSf/HsaSNct2jp+XB43tNtYpl1r3acsibOvP4lAp/
XZuR3tvUNeXL/NTp5ulMqfIQlLKC9Ah0znPX8H7g9ccTPig09nm8qWeaOMyiJ9Vm
/jPJPN6xPTJT3jxEMXj9V0DmlkG4aHhkf74vfQKPNt/lx5Tl79Cit73Sw0ajCqgF
IOPeyvUww7u4kGXhTxlv+CirX6W7wPGPdQku7PXwl5r2I8iBWFaOiqPhuoluaWnK
CRN9QQOA0PAScDZxyHB+Z0E4JMgzt7rwDiGChcZn/OwYMYEgZW75N6kA2Ptc2pfw
+9l9AXkRIJcU0t3p3Kk9JiFC/AinLP2XfseuQYvtEUviBlD6snMquAkdkvlsI1po
SjJNHyPqC1+x/0jVqquEpDVhHQ7JYci4CfzTaEGxvtpGMtAYgHXOlTe34+xqvg7/
Vwjs+NJOQVT1Oj+bQAu1IbtAdg1hE6PHcWy2Sl2Ej5wWvbrtoyi/9b8hBoGGnLIi
mRDKj2PiA0dGKiOq0d4tIzmKnzRUPugVwjLEpW9BBP6p0BcNYBbBKdOQvmOdhlkb
V2rggBQdIUeDvb9bgM7O9oCZIokmJqUDVrD75VTWPel1hPv4ab8XM09y8lC/+4R2
8X8NJyLf2RLGmRhvvAYi4LYRaP4db7pEDCK3cEZ+hB0MG20Lfuzoe1RmOtU5Eu+4
8DUuW+7aOM+72/px1p3v2Yruf4vX9EZJJidWnqOXNcopts5oIMjwvKfpW17fzrBX
JUhpTgaycis/SAHAPdomO2aS6tDMYSlhv9hLTCrsTnyFB04AOV+j8R834An3VRZV
S+Qw8M3jlWD1TurHPGpQAdmvRUjKzXOnXA/Ior2MdEvkOObluFHTvCqC3HRx1+eV
IwuHNTcWedC5EYfIzIfKgjkKf3gq6MRd5wfjqPCCN/WVDIHGCMs3BZJVAX+1aXqU
5GXgij0n9l3vliknqGz+FqPBRNS2kGjeW+6A/3fq2+T6R7xbMl0wwcziXZAEWIYQ
MmhqOpy4FqGKh8Xd9RMZ/w+XEOLFY56FzvlkWoL1tF5gvpcNtInyfszUdvyyyWB9
mT4O8LwdgZap/bvHOeU2JsfcxLd2E51ssXhqYaE89mRl1BZ2hhyU1KRwbsALwJhr
F6jEyqtWAKnlv55ZyoHBKLmvCRkvi8iQ6lVOKZ787sCmVduFEieMzzw40hupwpqX
nyKAdiFZca44nw60vHSUiALT9umlq5mGnomqI/Ka13/fzjz9dKJ6NcCi6C56ty+p
ZhoOCuMQ2n90474Re5t1qlQjwVZwAPnSKBchQUW+tjbn0TWZ/QnnpCuKTdQqqkdL
iLQJZZk02qE55zybR/PFELI53Xj+RqL3Zzcv+FHuOu9Ykv+fmRMiVon0Fdlh/G5C
/je2+oFF8mmcKd2Rbm8Jh+xcRAvXeXJRkNSz2NVfOofMrCzydb+WeKF4cO4xIRi2
fhbQiqcW7WcDpBVg5XtLJKLGGkx4speDOf4HQ6RatuKfm0VfHcHnRDTzahdLtdoJ
uiQDBbn4ymQFbVTR9h21VcncUz1M0BeCTYVh9BA6kUbVxoctzKUonhl0r6pKWsTD
MODLU1RJUi0R5EsFbMkA9nRaMflcvkDOFRY27PPqwWAjgnBNUIZeO4gMXw/yM1gc
hmTw6iWgPREtmAXfoS/rDay3sH5GKzY+Be7kdVInlGFQjEaLnaLuedI3tOZQ5cfF
```

```
rLpAM6rD8to2o+Kcd0hRF3US/kPTV0cXxVJhL5/k4HpPL8bmnls+qzoQojJCfFkR
zt0GEUVlnxohyrPfEjr2UQ9s/+edUwXwTaDbWA+JPaaDkxC5X9Asbxain9tj322c
8uO8kROdqCMtVo4ihyABJhk8dlhETuzYAegeSXT7/UPoWO1POf0OO6pVn2/TG+os
v736v8ty7ytVOyR1XVRaTmxSHOZhamStm81R1mwIgqbYcYT2ljrp5pTSth4GpyVd
ave/jH0GXIe5R6Rljm3kzmkWHii9Z5FKBpHgMksUHm0mtlWAGa/DrsFqFuG4tNVU
FRIpgZbGXPgTVgMzfnh0/C0BjnBuFMggGpYSX8MTu8rznuiSfSoRffSLMP3VRD8P
n+nCqncj9Z+k0c9y58Sg61ice7iiBgsjFzh49HH04h4ft19xtySOLmIXpCVR+cY+
SIAqgRgXNnx+jMPCKf0DQMqAE0C5XmztiSG7XWlE3ufS0Gw9zSWxoHFbPinbU8nc
8vokU2Jk7rJujoNjwNeLc6UgnsixtpQlUlNhC9apAZo/6QzUiVkyZh30I7E3GNZp
IlvBhD1pGbbxBkewC7L3rfA5TbAci7tNNX46beoEfbI73HqtN7+EnAkxCVsE6mH6
JUNSPJI7RJu3/sFyq8KyV2EzYfwhb+ww9tPYhKCaokeluvmEqzb1qMw4atpSBWU0
lnyku3ffndauOW0MVpMmbtlVMqz2NFJcfAm132PQdHSs5Hxc4XiStJBZ6/EeGn/a
lbhjdpYf5Df73zb1icUxU/El5Gkws+S2oloCa2d0XbjY0ngr/9l28xJJLEyBQDV9
GxlsULqjM+ipoQb1PfhH9UQOH3HGTdd7Ko3YcoiGhN2Fx/mddOvbROJWbx1OsV49
aLxozsMx7/CTXNB5IQz0VvyF/8B3ChncqJTfBETRfU02mlp8MehfP4ZKSVCSnRmJ
9gasdKFk7m3etaqc6Vd0XOdeV0AAl6AvGv0/cXymmyN9Xdw1+Aet4StR12YzlmuR
SkXmXmOUWIZls1jqCz5plFuKKDaPTMFdqE5MIUBewJ2E1RIzKjkgW62YUm9tToGD
z9uaIpxFdl7Y6/kmeLrVjiesHDpvA4dfkCtIekOu+HpOzjVOruI6rJC6aOC6nURW
/qyQZ459RU0A1brtE9//7aBqhXAUzzgZ5COu0OPgFeNikBhlUJNeCceypG7kFDn5
EynDYo7WAGhOOEaurGB0F+Zb6QBWMGIYQpaueSEl8BZcXMwVKGeGdVA9oW/X5pvP
nvQDvgJ2TZmBUpZ4bIHgi2dtMAb+oXnkYREqAYqc+nxqFh51M+gdVstRL248njRW
P5y3NAXRxnkGb4lp4rUQnb5i9hrtqeJruqWFK1bQ78rNc5qjbyFN2LARRmDDtXDZ
UgC2553rSgZycEO5OJkC7JVDOl6V4qGftBx1npXrXS3WEJjNyP8ZkwvHKXEG9xyQ
hgYf27vBcss2SPws633HkXmyCRpturu5J/AQGzfjb2kvnHh3s7usQkiUqcP0/AD0
uQPaEXqLhqfRsXkw4m4ZD3YJQbVNQ3ICal34CqA7bwjfpOQrosgzpx67QG9+ksTH
Wyd4hk8GfceC0MiB8vPNcg4j9vBliOxw5Ip1WFBy6TL4PUAx1RnUQeUDlv5lXbt/
EzviUnnBaPsnZsMrMYZmj3PRsCKLr118BAXgWgZjrS4b7wsahkTZiVKRc+/bXMv7
7Ta16UYQ2mTLM9qPGOv9gJFZtQEs+HQdJ0HG3on47coqxudJclPSLvK4Gvlux0iO
0GyIagZXndQkWaXGy4KHcyM8nqmwhAbmhLtTX70egiI88pkj3i1dOX3Gi3KEXL7D
6zHlQUYQ6bVeq2NB6byFKGiSZz+9i4J3vgfW2l/lMwu26fukAslL7cBsXyREjTLw
tYGbw5EWoHOxr8Mgj7HrhGPLXX/gmjYmg7YRds9WWte+9FsRYnUTc9oVEGoIcE9b
JPxUpluje2b0eqz4dG20LSdk6UELU7ZrKZGItOTGKgLzNb4Vag4z1d2RD105w4wQ
CzBtH8nERPO9Idx8IabEpLd8t/E/W7hVjWj6pJEqPB9Wp4Q3gGts6xiZ8IIs5Ihv
x9NMrWrtpg6nuTZ93lPakPyVeZKepmvQgKkOLpmdKXwn57W3IS3YXG6Jvufaatsb
tCi14KxiMbPBpEBz5vNzuUzMUjFl2GLii3AlRvMNJNAkbRc4T4KV2cK08LZtk5c+
sY68S2ZsRrPjKNpSiI70MRpSBfaQ1L7gGzCNUdG86geJ9kUUw0Ri+wv/PCyXmYQX
7P0xtHU6WwLnxKdViVpfT2juSOQ2+LD/pOwag5FaPsBsSm4b4a8kLAZfNyFyrdGL
SnzL0CipUe09mfbCscMtAJEyh6zvETUbiMOuRCC3iZDprXPU3TDUVT9Vmfba881c
hCwKk+4Rz2QUlEjdaUJwsbW3SUftO2U231x7lBRf/D+LDZmUy/BhSe9+6x+Z7upO
v5BCrvEb4F1MTyenODG+JU+Vev7rZp4A6eJT0GNDpq9AkI3rIlGrtVFGg18cga7P
EQgqUWIstSL2B9HpZrTCuor3g1kzQNFcCDpo3KvbmJ0FcLG3N1m3YSFcXrAipbhT
uz+4gmThKBi1ncX1Kp1p5NXXbnCD7JF9h0vfdVMA+eIYGufu/YjaVrm0jfhkcESk
k8rhAae91JqXKD+tUXkRPV36lLpXVAhnohPQnbWwnVdJ+gPchJS3RyABFzvni2Lz
309Sjg2r4N0bt4xJm2F7T42373w60JpHJO8RFnSNppqyVX3AD/3llgAb9kTB4xy/
n1O+je8faJ2zvoD3BZqDF2/8gacvEBU3xBUBJi68AaBlhhciNY7SicG/SS/wRgRi
nNjlhHX/2SRf5vGb64/4RvN4WqUCEMG4m1Zs1e9352A9Mi7gsl7ITMwDKCrCSQs5
d3fbhcniS/29E1rxMxu3LNXAzebs1bY4+NYeROp79rQwGFFH11vJw6hwdLxjhE+H
HjJ3F0lmIwj/TSD56JVDrdzASZEFWoTQ0j4Wb+dnvLRFYQJAuLgJUc4But5/rYPZ
BDSbuGRmstkzJmgp3bPX9QhWscGoDxFTYvFWZsG0Z2A/Q6sBC4qMmTxuxUfQA7Al
LsjZoTjRQLjIN6jkQ0n3hjW7oF1aX5ZbL1hE2YrBei5K8K/32Xxh9rU36kn+mdyU
fcFdCSBm8Jw+4utPG0PcC913tEP/apykXIU0EN3NFMmuQC4wXgLEQSprqFWIZrKq
OHD0TB+ORlATKGHvzJHnVUhBw76t+MUi0DpnOLl9eQuuBbABWLvSbX+z/JVCy475
3LxsIxrLohS95MgkpzqtCrjCAW8vawfLDOHSJNAMxlYg+9WESc8INI4YGzrJP77A
8L39Js0zxij98Wj6T8QK+/MrLj7paOcVMMvVVB2fyUHl+91171UOCNHS1NMFVvYu
uTptL82CogEZcYawyMMyV0Brfeqj9RkBG3uGJdo5h+mn1jtXqKxFVpOt3gYaylXM
Ap7yZpZivcQ3cs/uVCaDX7/ohHm8JZaSrpzCeTe3N7yUu8RjcThYptJweNutNxCm
olh+n4mWcSWLaXs9suKqeCReWfJhNfeeGgJsxRNDcbxm2/Pj0p8dSWcdsKIe7KdF
PuFApDm3vtsDpEyvX60cfS8J6xyQnJdzIqyW0c1d8FU4/dYJIzNFNHtEmoC+Vies
```

```
ssW5H7zPZFPuEsMzGfJtnuEHhkWNhNavbsVo2jK+LPXfQN0Z+c89Bc2d85pyFNeQ
kyAw5tlOYMoav0WqBrb+rs4dXSOA17WKJcPypn7c2tZjoz87qFYmre+3frC+oegc
WQyMEP048xuFqRB7J3+usCv+7p0Ur90Mnvb1364N9hxfdJtJ3cgDoIigx5sssp1n
Z8GyaDmqGqo0uvneIys9+wbYDjNYFQLXUwL6Fgzj/qldPoF/YdrMBnSRSUm/a5E2
CPGOJgJc/krcLOYkSF3gJ3verbcoycX99kU1o/HlGL5DLro1A9olD9HaUg1oKPY2
pA2k+yAIv5zoj/4es6UndtxnLj2CEunOojzEGQy46kVkfgYVfx76UnWcx16k/E1C
ZKu4gOL4N+jbDwu0Pw3j8eW3Q/3esPTfE0AJzRTtgkGdI6UbrNkNXVWxfKDLchqW
18U5RMrvD+zfV4yyK/jjy7YDd508ildX4R3lLcnzSFJeDF5mSnhePCBmWSEr0z6u
62/LoPj5HHNlU/LESRAzNuQLwlWe9DzaGaeyfBHBYvFvUn/BLxPifGPsBZKbEPg/
9q8UPNh+vPFRdQp9YAU0UV3VQZXhQxRNIiaoFF2x+6MEA+VoKH1ANo9zbzkPsCtB
EdeK4Dw9t2KXJlmM/fB0C7EdYX5UbqVr8VM9GPt7DUndG4WaxGH/7OrVA4uOMtDG
YS/eHjpHEkhxv81pguuEuV3pXEQw4h5I/DUCeMhYt3zEhxPPCXRKOqCDNfZVaiyg
GjOV+wDYTg0y7SpHdXNxfA7Khsc8NFK5w4Cx9PLGQpg310c4HNxCSdT88O/+pBsr
eTIs5Ym9NZLqzXFPnc8ixFCHXvg/eZEP9iEbzEw2pMDePzOCwHGlouYpgHmlGUfr
/gn72roI+uT/gYH8Lc2SYNR7gOQqEUmZ79MzziePg8fyvxd8IiOSpUHMlkLbQdjC
YislsKmjjSWQYJrsSXKB/jomZuv4V8Ix68odD6nAlT2/FLxH7hq7YFfdFaTeUaU9
vCEugvwN5Z1+VdXAWp3egdU3fY3yDgrIDqTfkH8mlk/Sk8XEhhMnYFeYPQ8sDmkT
8ZwI+P8D5RfP0fMRAAg11rCPm9woeXA9JEGNfBtKpEMEez2am99nKfIbkL0xvj+e
yZTOEkjDVXtugIbUf7RMmGoFj4oHQa69cDWDfMXPJoXtF99LUI62Dr4rDGrSPVUt
dgVwS8IWPahbRPn09NixO1rb+Q1+3UyUcovJuNwia8RT8jH5z11SL4s5CwC77jLb
PCzez5nGqm6tuFLQ48togUaMbkwmGxhxE3mLVDlOh/rQ2cndcvHNwkhUJpo3A9Dc
mn5wb5OYXknZBjqv9Zi+6xufiTKUpoFXG7YvyKp2Wj3xNSBDDLi2ovA6BVCNsRnl
jjWeVtjcCg2cmm8nKEix2KXb7VbiYkzV6selYCZC2LTprlJxIwzRH8oKM5mmR0UE
0mXtEhiUbSPrIYEJKgBS9x/541nFj6zPR8VDWPBC/z+Jz/+pQGjO1tn8Cw3yaZoH
aNAg6NWu9Z94WdiOras+rAXsrccFofWL7NDC8YhQO7a4o4cLz9Y+sG99CxMrdOOG
L6iachPXuUyjpTxqE1g5U9bIGqoZkrmDkv9ZjGxidFA/ofjXZ/kV0zfQ0R1TZ8g7
/EMhFMLtcWu+SCPl7IxBgGK14wEUN4gJdBvWbNvXItyOSSngCEBwlG+cqZxtzHvO
S+lrIEtuFP1ziPKXisDekRlJ2n9ySsGz3ff4SQYHvv2f5OJpjK3niOtzXrhzjqQR
E7LXJlAYxc/SdKkB2N8ajOG7vld5ydA5dDZM1cbdNkeGgxaCZd6hDb08Lc52Hlj6
B9NQgygtF0INFnEUvrVsI3SJKSrQAeafppe7/RrC9FsuwDe2582BKbX9NnCXQamI
ND3HDvVFLi7tnaJ7luGtQvqV4BHsF6WNbJTisWxTJtuhqQ3N7LvyBGO8DJnwzUFj
D0vaWHTdeMmsvkQz8JO/fMxq1GxGnHkjjg8BmmkymS2sA/RXLPJ4FIGgPg1eNymY
6IphFEpTwyoW1IYFIROIW6KiVArA4N8lYpoMeprzO08I8MA5Gf9XoRJRpLMo2zOf
hJ6UCYO2rgunUaa4kMbpSW+l+7wUPEgbxM47UQKZ6FRjU0lMnmYNxHnoJIOCHJ4R
0nPO2O0dEYk8qYe+YSGsVa6d/dGskOBK5YrZeXmSiTHiZemAyahE38rZJIZrwC6n
Kjm1MDaTiS0QhtNSVctjNYqJzkesSJr7ihxP7M8uvBONV9hs3dpiJr7oXFKPR3gU
mE/Jj6gtBe+xcuhluqPvwLPRiM6rZEHisjct8KYVzSFhXMZ/LqM/r4SAnDTHoMlp
PJOQzqUqUSDrZp6FefbzrHMKvmh/BjCPYVYrtRhnCyeq90h6D7pUjsdKV81MzX40
TeIfRAlpv5VVJlN9A7QItE9sCvT63b9M19YIHltZLrZI6oAuRLVux0TphgJnuH9Q
nrDVlhFYzmcIIz5zeHcSRLAnE4xhHY9eNbBkfr+0kSmzYO1lj/z0kWs82ZxFsCv/
X8m9r88mMAO8UjvSSdaXaU4QMpgyjQjdIDYp8bzX/sySZsSwue6Xfz8+HV18Km0/
aurM5Cnt4pPCyecHh6d3ktp0atLFfAgkvXRy1qeB/HQ2FpH6WbZTxdq0AKKsPHpJ
Q9E9KwXmooTajSKyLamS/eO72pQ5G715KDaEkaG/O7LRXS/gmKhk+yrfULj2uMAF
3Z1f/irjt2aDlYOOfpQtkO396ZjRlpTb5Z0YwA9Z/h8nDiKils7wm7aOr4MFU863
64FshXZDst8UhD2fg+FErcxLn0cBsgBAwoQ/dVyAThn5yg2/RdQUXb+lbUdoWQsa
KjA2/fCE+MWIvNI/7kVOJu1oF/kIhKb2GMS4qP+mL7iyGRexfKuXg9t2ZPcrzDVQ
DJ+U8ShhTwbwxKow+MYEa6tyNr5n//R3X0PqWEh2Nm4i3RHsHAiyT5y4XAFV4bqw
8A+j/IsOYb6YOnXSmPcAqapvfpBkmFYVmKeKEnX0qvurU9WnWIPUVex2lZORXWpm
Z0rJpkGeJ0Qzl+lUTlyzDv3F0OYfu2YM087UwDjusFXkZx4q0us0RRlHOivRhsSm
fVPvCEJpPP+IkbKC9rnTNDRYHZXe0fwL0BayXeP5vzu0xhTPj2scw7xGGQXSV/K7
rXZIyp21dUgWPvtC6GsnaqqB60ulY7Z4RyGIROF+dpIqGPa7cT5DWaxFZxA28zCe
my2SjL2+P8CiOO0cynhFSW+RkxwemTxUIcorFeRbwY/QGJPxOt3zYd8Ac3xMUpl6
5e8lO5xVK4nonot1XfxBEb3KLU5szkNM1KzoXNFxjvnfiwrSX8UNGWAvmDWiGWut
7D7b2mazbiAoTMEOmX43as1FHeco3oDjeoEiYyc8b/6nLj9/SMSkxzgncrxvEEAG
amhJ49wnRgOUWYkZzyOOaCQqA4xnGl84Dj3tQy0afpE=
```

C.3.15.1. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
```


```
MIITEgYJKoZIhvcNAQcCoIITAzCCEv8CAQExDTALBglghkgBZQMEAgEwggk7Bgkq
hkiG9w0BBwGgggksBIIJKE1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LXJlcGx5DQpNZXNzYWdlLUlEOiA8
c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNoeS1yZXBseUBleGFtcGxlPg0K
RnJvbTogQWxpY2UgPGFsaWNlQHNtaW1lLmV4YW1wbGU+DQpUbzogQm9iIDxib2JA
c21pbWUuZXhhbXBsZT4NCkRhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTI6MTg6MDIg
LTA1MDANClVzZXItQWdlbnQ6IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjANCkluLVJl
cGx5LVRvOiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNoeUBleGFtcGxl
Pg0KUmVmZXJlbmNlczogPHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHlA
ZXhhbXBsZT4NCkhQLU91dGVyOiBTdWJqZWN0OiBBbi4uXQ0KSFAtT3V0ZXI6DQog
TWVzc2FnZS1JRDogPHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHktcmVw
bHlAZXhhbXBsZT4NCkhQLU91dGVyOiBGcm9tOiBhbGljZUBzbWltZS5leGFtcGxl
DQpIUC1PdXRlcjogVG86IGJvYkBzbWltZS5leGFtcGxlDQpIUC1PdXRlcjogRGF0
ZTogU2F0LCAyMCBGZWIgMjAyMSAxNzoxODowMiArMDAwMA0KSFAtT3V0ZXI6IFVz
ZXItQWdlbnQ6IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjANCkhQLU91dGVyOiBJbi1S
ZXBseS1UbzogPHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHlAZXhhbXBs
ZT4NCkhQLU91dGVyOiBSZWZlcmVuY2VzOiA8c21pbWUtc2lnbmVkLWVuYy1jb21w
bGV4LWhwLXNoeUBleGFtcGxlPg0KQ29udGVudC1UeXBlOiBtdWx0aXBhcnQvbWl4
ZWQ7IGJvdW5kYXJ5PSIyMzAiOyBocD0iY2lwaGVyIg0KDQotLTIzMA0KTUlNRS1W
ZXJzaW9uOiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L2FsdGVybmF0aXZl
OyBib3VuZGFyeT0iNGM4Ig0KDQotLTRjOA0KQ29udGVudC1UeXBlOiB0ZXh0L3Bs
YWluOyBjaGFyc2V0PSJ1cy1hc2NpaSINCk1JTUUtVmVyc2lvbjogMS4wDQpDb250
ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0DQoNClRoaXMgaXMgdGhlDQpzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LXJlcGx5DQptZXNzYWdlLg0KDQpU
aGlzIGlzIGEgc2lnbmVkLWFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2Ugd2l0
aCBhbiBpbmxpbmUgaW1hZ2UvcG5nDQphdHRhY2htZW50LiBJdCB1c2VzIHRoZSBI
ZWFkZXIgUHJvdGVjdGlvbiBzY2hlbWUgZnJvbSBSRkMgOTc4OA0Kd2l0aCB0aGUg
YGhjcF9zaHlgIEhlYWRlciBDb25maWRlbnRpYWxpdHkgUG9saWN5Lg0KDQotLSAN
CkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQotLTRjOA0KQ29udGVudC1UeXBl
OiB0ZXh0L2h0bWw7IGNoYXJzZXQ9InVzLWFzY2lpIg0KTUlNRS1WZXJzaW9uOiAx
LjANCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQNCg0KPGh0bWw+PGhl
YWQ+PHRpdGxlPjwvdGl0bGU+PC9oZWFkPjxib2R5Pg0KPHA+VGhpcyBpcyB0aGUN
CjxiPnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHktcmVwbHk8L2I+DQpt
ZXNzYWdlLjwvcD4NCjxwPlRoaXMgaXMgYSBzaWduZWQtYW5kLWVuY3J5cHRlZCBT
L01JTUUgbWVzc2FnZSB1c2luZyBQS0NTNTIzNCmVudmVsb3BlZERhdGEgYXJvdW5k
IHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhDQptdWx0aXBhcnQvYWx0ZXJu
YXRpdmUgbWVzc2FnZSB3aXRoIGFuIGlubGluZSBpbWFnZS9wbmcNCmF0dGFjaG1l
bnQuIEl0IHVzZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBmcm9tIFJG
QyA5Nzg4DQp3aXRoIHRoZSBgaGNwX3NoeWAgSGVhZGVyIENvbmZpZGVudGlhbGl0
eSBQb2xpY3kuPC9wPg0KPHA+PHR0Pi0tIDxicj4NCkFsaWNlPGJyPmFsaWNlQHNt
aW1lLmV4YW1wbGU8L3R0PjwvcD48L2JvZHk+PC9odG1sPg0KLS00YzgtLQ0KDQot
LTIzMA0KQ29udGVudC1UeXBlOiBpbWFnZS9wbmcNCkNvbnRlbnQtVHJhbnNmZXIt
RW5jb2Rpbmc6IGJhc2U2NA0KQ29udGVudC1EaXNwb3NpdGlvbjogaW5saW5lDQoN
CmlWQk9SdzBLR2dvQUFBQU5TVWhFVWdBQUFCUUFBQUFVQ0FZQUFBQ05pUjBOQUFB
QWNFbEVRVlI0MnVWVE94YkENCk1BZ M3MzluTzNUcFJ3MjBkcXBiZkFSUUVqT3l3
aXdZbkN0a0RLbmJjTGs2NnNxbFQrenQ5Y2lka0UrNkt3a1oNCnNncnpmY3FWTXBM
```

```
MmpvMDQ0N2dZRHBlQXJrK09uSkhrSWhBZlRQUmljaWhBZjVZSnJ3N3ZqdjBaV1JX
TS91bGkNCnZkUGYxUVoya0REOXhwcGQ4d0FBQUFCSlJVNUVya0pnZ2c9PQ0KDQot
LTIzMC0tDQqgggemMIIDzzCCAregAwIBAgITDy0lvRE5l0rOQlSHoe49NAaKtDAN
BgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVs
YWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQ
J+RpwpODxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+a
uzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVe
A5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShp
lcI3lcvvBZMswt41/0HJvmSwqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5
NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/WI+w
hUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgB
ZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAww
CgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8
ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkq
hkiG9w0BAQ0FAAOCAQEAgUl4oJyxMpwWpAylOvK6NEbMl1gD5H14EC4Muxq1u0q2
XgXOSBHI6DfX/4LDsfx7fSIus8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZncxG
wy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxODWq9opwtA/lTOkRg8uuivZfg/m5fFo/Qs
hlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpfB8
PPwDR6chMZeegSQAW++OIKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTSO7K45
9CyqbqG+sNOo2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdB
BXntdX9CqaJcOvT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVU
RjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0Eg
Q2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5
MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcw
FQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBALT0iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LCOwI2ju
wdRrjFBSXkk7pWpjXwsA3A5GOtz0FpfgyC7OxsVcF7q4WHWZWleYXFKlQHJD73nQ
wXP968+A/3rBX7PhO0DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZO
63dKvIKp4cQVtkWQHi6syTjGsgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf
4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I
6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAA
MBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWlt
ZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAd
BgNVHQ4EFgQUu/bMsi0dBhIcl64papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTCOfAcX
DKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAHOJojanzqmgaSN3/gqS
Q4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1iffRTF/K
tmVEDMR/sYeqAH83KM5p3el2lVh4OHhyI0qNuz5oShNaACSioQ23WxHGVy9vsdVf
nbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6mrYkKTM/R
CGnumghxwYToj1OyD5Gs4D2IJCw+fX5ODxh52MbNRYXTus2ZPRPM8JXNQC4GWv4k
m3M4rKnJDd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk22OH4ConlB8f7R7s1LM2
cSYxggIAMIIB/AIBATBsMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBT
IFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0
aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrOmqnXMAsGCWCGSAFlAwQCAaBpMBgGCSqG
SIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE3MTgw
MlowLwYJKoZIhvcNAQkEMSIEIJqUXzqD6DHL5QxaWDH8cjQd+BnWEDsqfNBB2TB1
TAOkMA0GCSqGSIb3DQEBAQUABIIBACXiU0FE8dQ6qbdByg97uCGlmOthKkgEMr5O
RkpoX6ntzZW8Bzj3xOt6fe6wwhxExszASuxN0STebics6GRcN/EzXV/SUDEOW7Y6
gK8c4LiuNfD76ZQLHbPhIMYDidhYb5lDO4MZCJosGPFCgGitf5V089h6WjZMY26F
YpL5lQfXgVAP0A4Y+2f8RaEP4Fsh8SLcV/EzniT2xCNCEuZwsETA65OnGJ6A6ktM
ljaEywaYkm0bVFuJ2ml4x0YDd/pZpr7CIgDtzh/97x39apqnNOnzTGnGgZi2T6yK
4flYxBHvYI53lUd/ub1SQMH/+X4zL0sbfb5+idTt10u1pN0Qcb8=
```

C.3.15.2. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-shy-reply
Message-ID: <smime-signed-enc-complex-hp-shy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:18:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-shy@example>
References: <smime-signed-enc-complex-hp-shy@example>
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-complex-hp-shy-reply@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 17:18:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To: <smime-signed-enc-complex-hp-shy@example>
HP-Outer: References: <smime-signed-enc-complex-hp-shy@example>
Content-Type: multipart/mixed; boundary="230"; hp="cipher"

--230
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="4c8"

--4c8
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex-hp-shy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_shy` Header Confidentiality Policy.

--
Alice
alice@smime.example
--4c8
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex-hp-shy-reply</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
```

```
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_shy` Header Confidentiality Policy.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--4c8--

--230
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--230--
```

C.3.16. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from RFC 9788 with the `hcp_shy` Header Confidentiality Policy with a "Legacy Display" element.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 11530 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 7520 bytes
 ⇩(unwraps to)
  └┬ multipart/mixed 2834 bytes
   ├┬ multipart/alternative 1629 bytes
   │├─ text/plain 580 bytes
   │└─ text/html 752 bytes
   └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID:
 <smime-signed-enc-complex-hp-shy-legacy-reply@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 17:19:02 +0000
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-shy-legacy@example>
References: <smime-signed-enc-complex-hp-shy-legacy@example>
```

```
MIIhPAYJKoZIhvcNAQcDoIIhLTCCISkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAAI/dYMbzc3zEiYx+UrTZSpSeDOwGmzAeujC
jAZv5gFxjb62n5NLr9K9d+shGjdaYbpCxj8JfQmFg2jOB1MlEkf06RXo/3A8M+lY
DTEbcZxJSVsoxWD5GFybNQm1kCUSaPtWJd0PdXv27sdv4ylWZOw2AW1ecaUnK70f
Lz5ge+Uz8gSOU+nHnxESOAMqUAsg8lgk16IWSnm+Vnt6YVeaVfiA+DL/+lG3Ijf8
+KvkwSasTh0Bg8lRJ3QepmHqyZcJopJz/TOsn/6zp+wk4VEezqF19ofdlOO4Eyck
h8PN2ksrWuj+8xts5CxdYBnAn8kAiA5yusP1O6xJz22AWQY8oo0wggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAQDa6AeSZzIQh8pQjClWUIK5a
FNESnV+b49enYnj4vuGEHnnB0TM5btNCYLoI62CvyDsSMyCWdLBiFPBn2w8H2IiL
m2XbWwXDPUlikcO1CGEmSmJJI/7GYScU0naGyrKxTOBefjovgQwFqJmBFIAgo/xc
DyS3betIuuvZ3PTlQPYLQrTHIke7WfymJw80dcgP6bY4JQp5Pf9ErW3GvdKx7wN4
gGyqFvCm1PGuc0OeHO0jb40GcglfzqabBQXax3Vr+XxDiiwwa50R1nPgIhf/mYOU
07B+4GH30ogzveQ8KRQ1Ry2By41b+nFO42U/nO9bC6FAebCGj7qNq1x9G4dpETCC
Hg4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEHdJN4l0uotCGn4QEUsJjjWAgh3g
30f/pefDZUamG+tfMmvMOPZZOznkpv2sR6nXwJGpqMzgnUv35t8MatduIQvjL/vj
1wkZ1W8XgKKrC+PI1cz2HaJioFVglFMp6lVuzep4gZZ6coK/oq/0eZfm466TIaXt
kUaja40Fs7B/BzyWI8LzzjRuZFWJeiLfh4HHEXFFNJ9n6aTaNCUW1AsFCyi1y3H+
dP0Y35mB9o9N06LO/B95yjJ5cJcfOf3clANxMBZWvrbof94epVrOputl9dQMCNiB
aGdlvI1lg2pXDyeNYWR5jpdTBAN7Bfmg9MPQBWzRT6Deq9qkD6aLwOJW96dMW4hh
fLCOEWGuMe6UEh8hvsx3gVF7A5wZ/fbs9pZvrHSDDU49+Hkf9RBvBepPtqXt1dxC
kEXd1sXae1z/ZrUVkBjWLoZ8HHPyEhoEQz6GtxRl9yffDA3eRBoaaTPUJJaU62OL
oJwlGb9efDum6jmbG5cHTBcEjWAja3NK7ZX0RmG+kxa4nDZuKOw57DhbtVJhHsTU
Ocz0vZK/EqRDHXiPnxXysHM3V092vmW1Y2GKhNCqFGl+5AGiGcZ9SxgZ3tbMWVMi
YkSSf/pU4h+MCPYKIgXs8suP8XaLyvk+nWnAitf+emaI8bootKazlEWSGtIqC2M8
6DwNaRI2aZc9RkgwFd3MU7uYhM5qhp5cvgLxWc/Rg30Ly0m0V+GLza+3AhiMVPo9
YNuo02TxfaStJeC5jaEd2212Zm/0ZOgbvDw+lAD8DC3i3uDgui3xtc0Ljc5DziqA
/usC5pl2hjw9vcG1puqDWOz2OiDwvtasiR9m7k5CN+ViSSKt2brNAx4aqbUO321f
UcsxeDZ8pUDs+SAm+zuHMUcbWczHW1bRYlo0DehOvaPbOX8qxhJ98JnNdNooG2ko
5U31iT23s9rTH6/Ebcsn5BJeOvHk9DFX+Mzl9+k9phWiihxn4zTRXvgDC+L3GByl
EIhWRE2hgG32fKmGeAaOptLW35RPYZDNidMQzD9eEcO4Gn9kNO1Jq3E1vwLixx+7
PcgTdVuyPJvmRpJ2TaLJFM3bN+ywyUY8bVFsweaaAXzr4onnC2HJShKaUGuOTbnO
RPJOgpZOB0ujNdqZsJjnyeUTlkwg8IxzsfIP6UljfJNrHR78quPmNJwgRN+9ycEo
2GuHtfYixeBVucNptDx7O8p/+K21MgGFcDtCmubVzQzm82QW3xvBaU0mVQuE0mqD
xnC8pc6UvVnXK6LBqyDzbBWk6UxqHDIwimtst4P12KOZ/MJVmMBOWyyef3PcIgSz
5D5seDL/ZkzEmnypKFcMYPQMrrLWwcSiYuCXKKqjh0eKWkt2ioPrrdPUDNs12aU1
U7LUrqviOb+ajNQ/uBOBmqSwGlsot7Tz9+x8sM4ywWhJ/9kAZt0zZO1VoIIcbX6y
XW8oNC+AOk/nSyHX5vbQ5c9paHif3s0lDxalcn4T5PmZ7vsG3TkR97N7Bbas64rz
zjL3YlsY2sxSVhM15E+RzF1bcJXT9vqS2n6tZmQdLIK2r3xEa2MQmj1D0281FDF2
4ckMsHxmhw+IdwS9JHG7mdmOLHYMt9QLMsxdb9ptfUqZw8jpwIxZ5gjCIw9PLGgQ
n7ZTm5eNRzfyCi37prI3oR6j8s8H5NS4OeygduGjkSUEnsap8iovsRmb+SX1y67k
Ti7Pvtqc750/1FelnnWudpnbSd4ZTnfHi+D6Qe7UUmz8OJKF8B6Z69+Y+v6qCS/q
jF+6JxVz3SoJU6yMJQY/EXCwd5Ft+kyYVbCpc/YK4Rjg5XGAZrIdHqorqXJDLs7+
3DPx65mIeyIkFoJRsh2U0HWGOwlW+e722h2lx/gyG0roN1ltcDqfhIZJHvTEr8LY
wO2qWpWMZXoSRHXyyfcdJ3kUmdjXUHCmVMoKAp5zuBNiTlH6Fn0+iux4qQMSM6sg
nTt1rRuH/9hc7hBKfHbCdXVj+TJzs74ChtNCHPzZqsdPup36y9YUTQ/CC/pLUOHX
FEcIR+PayJIszHa//x9OkL+gzhRf4HD+vTUc51M2hpScoZyj15yFZz58LWkAG/1F
fYB/upejDYznMlO+bNwYh3pJ1NpPfciWVZ2DajxMS5g71T3JJfJKem6FxAWno0AK
vgCjghD5rIIEfhD2gn0FZphYMbakpDcijFFIkmSMzcAWLBJn6IWlBQrJZs+S2q0n
xdR/d5CS0lSNtSSQVE9KqwpiD7nt2Ux2CDJRXI1csLhowgDM9GQ+iEHwlRT7JzcP
DeminbPXOgGmE6LUmgKhNY8wWUxc+HUTenvHw9/x3+Owcg31aptvoIjexN9kkLMx
8U854Za+/o8+3f+Im6gpz5orRWsl+EFDrH8ChCMl8OvuT44HwIvW828zMxTcBfU9
/Pb8dSZNnNB63zJbx39PDH9aN5FROXQNLODfVfQ6Rn149NGMqvaHiNuJ7y5ZUVqK
S6HTusbIujitQ0KJo91qEu7wQxHLP7STTFO+slJpST/zm7H0L1uZd0/vGZrzz0Jp
```

```
WzP8OUNAk2U2kc5kkc/dhsmTIQdxN1GmN0Kdv7L6XbWqHt+JjuK80C5WGnCYgrLW
fOIfkyLdwTOOP+vflQJoY5c9ACvHr6m/mrzHDDai2xxrilQRdxuFcoMFOpGO1Cw1
IcucA8FD04z+F/De4bsVxf89HUauVFIPMpv2QFfF576IS8/VpJlMtUHbl6R/I5QV
UcAPa4+CbT8Ldm/mKDdH8JfH2tK4x/c7i0tSojz+vJ8kFBOwi/rF9PAsaA0XfCDL
9zhdoEYBogXtPggzOfpWRi/ksW3P2SyBEZKHHn9mvyyLSFKpqNKSqRxJqAb6o8/H
OyM7mTiIWZtZM84Wk1raN0TCFvkHGTOsMIlxf7+ukicoNevX6ZVHjzu6jl68MSOE
TjLMUzZlhXFLVOeEsPBkSlP/auYqKaj1c0g0xSyAvjoyE7O3zMurfxNjoGBGsaRh
I0lwL/DeDypkNfpcTnyqBK8PbrozDSuSZOQ6zVSurHvq5PQs0fb8yKcKkg4yztPA
stv1geh/ZI1loQZprXVK7WE9OHLhg9z0a8AWiyvi4tMfDwul4P00XyX/HzK257kA
OwtLZQXUfrfj5PK6u4QZsfaURH0d/87S8fhIyskmAjzjFbd0VSQQyFuECW5RWwnj
5+q0almwJV4yRPSm44bcdPXHBiZHKqq2v/wW8YfzTWSIM62VX+VUZMYriyIXxq8d
VJKPfy/177Jfnf0vLshhlDLwt87nZCrkjXlEazUtcZOkbgXb6VJw1Wt6CY6fsTjy
YtVUNaPuw4u+0qiFyIYdHLfIEF7ERvqEN9HcQZpIVJ+txy0lyExLViz6MYVLGMEa
EvKkDX/aFNQb501wi7sDivcL6M2c8hAuZYzF0x8DuPiuEovicWQASsS/odhsfEVp
tKMqB2woHSX6J4aOQDfQ4SUDUrXHqcTyqDiygX1cYi1pHZ/vCN1MQ7OVrgDyCql3
5zisTrvcI1KX6Hu9T4UnyeK5HPP5SB6KfHp2Br7VPe1GARo0WXGmR7FnI+hjo++Y
ZABKQRj4ky8iq2uzbonTgmuQNtM0MN5c4sez4xPfJE/zFk57NM6VXvt9Ya7Q+2p3
RUbz5QzI1/1M/FLf0KN2LDyL/FxdHxl5t99dwoIieDJDo12V6xvpQC0ZhgoGGuMQ
RJLuXzkR+0KzaWmV6dSNVHOCW+yrvwg4oyZqoiRaCZsECxYe3ur+coIz0MPbOiOf
RnKYVn24AqTZ1rTcuBUxj7OeSLGCFvZKLGZli8bUabyCKr54gwaxrQRy9UZxTXal
1XsyDz1fm5XkcciUZn6rFlwvNxbYDmis14sl9R/7w0Uhw87kOZ9Bt1sDg4zpOr9X
+UsbTySGkWS/NTh6BaYrAeNuJz6ThXTghrW7NhNn5gcPht4jwbAajgcF/tIBmwZn
ad6OhuhtoK35b5EoNI+xYgAsntzccPCmKbQ3wHn2oaziQQ5pTGb+XYAOfmlUwUWS
cWuemvYfDQntdcEGYleE4U0dWpszd9bXzodgzH0ghzI8RnpxDQ5heYbWdcsNCkKm
HcduBeUegEBnMgSzIC+ae5DNs57kqQGFah0l/JMQ+ek+MdrXcqEfHIcuJcE8D9Cb
WX4UpITxyQ7lF4/BPd/Wxc1eK7OyGSCGEYSG366ywtkB9DHVzJmyAtqxAcPPJkpu
DcJ9kIKqtGzOz9qmNrYopT+hztesZTNwfiXd96bUyd67ny07dedM9epPxdSiDtnO
PtedT/epOTrN/wkX6N5uyY7uE53m0XwQRUCCVS7cTAdHRPAZ7pp7l8FzAwnM/9p/
vk1dsafHwL5IpbfBUTTX052WIRiXqXYPfeFVO2TkmCwFv0QLtK6H88DRzVDUF+IA
DVDlQrVZ5EBKopm/AF/cNqfkWDwSp2hMA0I5BHFu9nhLRQqzRL6TZol0OXAN0UDe
17AKdmHgSUwFuIwocdpPULqKV18eIwOtUKSZre8uqhLPYu5SsGQ8V+4jitMD+Equ
ctdTPsTafX/8v+l86NO05XDKbnxMTNelYbyMETw4HQmeaYGzjbFqoc4LzQhKh5W1
VjeQ0ZxKtzUgtKuQkI2rinI+lWPd56XbsCJ2lH+pa4tAB7thMYiinf91v86GTyCt
nzzeLdHiW6F/19WGmiKBNk6aMG+C85Bk/GbMmHcC+Xdi94NKO12kPyIE084N6BNq
kdCN8z0f2kYQLCwnhCV6t9cEsq6XsIIfzL5ULbaPY7DqOl7XWH5T2+2DZluEII9N
LDYO0ocZhiCHp0GeiEy4sX8b5tWSgZvj8U3uV05PfcMePCXpvuFlxf3SWswElhEJ
LAqpWlClsCS7nFSxH7M3FVALw/egqd+TSZ3hPEu1QaGY5EZ4T9gdF65MCEihsC67
U0yS5C8BKXZkmsL++E4J9QkjnAnRSj1Poxvi9ZUvmIiTD0Dx3Mn7Gkprqm/WJwmK
KbazwoQtBSYpooNXcJQAut3lHhl5erm5sGwtRZb63uA5kNBty6/1tVsPDVntVrQu
PlLlAQ/XUuOlNAlV2LOQck6YwF3HusBeCjZ1xNZWJC3jbUhsXkwxx2IffNcfJREh
fuANjE/GytAK1Z3VdJFqKGPD3qlG8t8xGWLGrA1T/oQdsqAKhTVR0rWShj5NKaoZ
P4MBQz8tWc1VlL36tlirD93YIcqqu0fVJvHSV65MCZMnoe67ke1pdcYKB0Wzvd+r
RBuOe4vbvGI5YstRAKLSLdcQBXxqfiVqChxKPQdeXfEjKoyL64vymFuHibrENpaP
l7IOXz0NKoluj55xyTUzdzBT0e/WKJRpDpal12ZknrUkcXIzLRpnqC53EmNRJ4Qv
s2BlhFpYrC4VWSBppu2Du2B1TtVDOxqad2woWordPIiex6dGb5+dqaOLSV6DH+Wu
IRc7gCfT07KGHVTZ+JkCZaoXG4qGFiRqEob8MwydAKToS5L47BVxgPZxJW2Tlm5H
nz1W9CJrJ3kM1IdagWUweiCjqnhgC4W175qoRvh5DxV3DhM429YVR4+0oS3FwDxh
/1JgNTWq4ROZRI5drPfjUdaS1XopMJ4GJPn6Dm7tQMuoGd3Sk+2Vni5fEgyjMw4a
en79UkQz9x6KD29nOm0bpN0zNhjBfps13bYGxqMIZMWAwpy2yq8DR3QWo6Z2BMoZ
Tsbs5THzpRb0Rl7slX4rmjg/X+1SAFzTxhxpyrULS3VF4n9NYBlgKyyNWUI9S46G
F6rXrxZaxZlR9EvpXUlATo3ZV94BhP9of5zOdrytS3zAXwT7E4ajJWsSGL9rvdx8
83PvvVisD4AhqzfHS3DPhgJd9bXLMAA0t+bLtQqUT56d7R97AOfgnM4L1C2xRT9K
pobr29Nt7bQuKluMoh4NHjexc4QiU2DZIy79G880AuUDf53z3NYcbY93foyKXhYk
/WfJD33tao1cjFbCcrJR3/LY8FTdtYOAPjPQwfmp967y/98yvrPqvJvHeuUFW01r
QmaCVLgwKEG0D3q+hs14APAWMBHc519UMJBq61ObMmsMCw7VMKpq3oCghXabyctq
WJ1akVeBo6usYSnnknLN9+6WMsqiNmeb15MO52iYyZaU77jeDFRfIs7+B+yyycdZ
3x9N7XyTbqGZr6UUJYubInE6UclBO0XSRiBsm2/VVFLBJRfckFMvPkK7IccmY4NL
2e6quWMl2fadmB0JaMOztUjfRCDdoaBBOSw24fh4zfHyyGJYzbLoznuCPeCgOB7b
```

```
E4fJg5tIADSJivl36YIyOCGqpj4768yvjzzjg+rz14lTVe4si5GhFgXADW7LtkFb
o8EGRwDDAOxCG5st4HMz/1YEjm90jyqRJe0V9lDt4rWjzmADiOT5BZnbVoso5Ie7
+hB4WqaP3lN2eipERlOSGHiMN0sibXgQyvz3IMmstq5u7OU5Qe1qPIOYjNFi9dv3
tcxIz3mOpaTMQRzIBxOQdF5421AUxljPC3dGktjROPE1pdgPzpfPHX3LDda26ibD
9c12AZFCsxap68AFiGNPpx9e2EzrAk8BM3L+T3DszTAM4jb+rpOgljEJH/pLnT4H
hRYhCU0PTMUXxmf3b2WJU5UMuf6OM2ZPT0woWYBCKRO5LPoBu0gDQdCpkHrDEDtB
UojQaiAjJ2But/ox1qM4PREt+1Bw6JTvkZOZdttDbmTA2nKFbVUFXH2Nh3VykRN8
5O917c++CZX7Gg3F3p6YBCzkqIIC0VVS3bkP1P5ZimETngRSTJ5DWE6/5N5zhM3J
sUKfM0BaGQGm3D4cTrYpcZaomPrnFmkKyrUvlBkGt3oyJM2EENfX6z01kod3dZ9O
kH9OBLRjR3siJfUulodi5iF0Pn0gZeHzqHKMlNknAwVVg20Vnpxuujy42NYNwnx7
askd28OvZAgF24osGkrZCX/zQXfqLhNEFseKtGQEqZhy6/Ew+rkk/w2Z7gkF00b4
xr2rcyYW2JsyMtErWp6KQPVNEdYzXi+qJBwWPXas3pzH16hMjHD4d2Q8pCfUYK0S
YGW1xU69cEMtgSs8Qc9VCIowLttDKBQOBU2eH1MVRGO6BgowKqC/WgtmA9rRanmA
3x+rEAxPncGrdFOUOEmXEN/Maw61V3RWZec2oSe9geH/AYj5QOTDmHLp0j3iiQyj
g3CJIsUXhKPgjSRnxPYqYOFUUACNaoAXD9PYRZqem7G6zHIiRqGCx7iMjpiSBND4
IUVWKWiuC2rvSqBmB6ohuTRt+tWshZ5Ksvi31eCCJSDB48XY7pU5N5Itfo1kB8Vl
F9j1bhzuAnCczqy6PHi7H05+ulWLbehlS2EMlzIqM+MziEiFUHoMuh+isfM48o3C
Js0v2oOyUz6XhmXxQesMMz2pM9Y2Lc+tcXh6QSX+RXcDMHZY5I1aNUk0g0V1o2cs
O+h6v/W/nRzSiB3f8YZJr2c2hUt9EAUj9TvCQa8SrPTen6K9WFNHOQWdd+bqbdL3
QiMh+8pLNbIiQfonsPgW7UXi8M7r5K5PewR1+VHFU89UVNU1hnu+JAbhOCVF3LCb
Yi+jFiM9uSeovg0ytMrqa9qUtcNonoKP3Q8GHh0ZQrXOOF8S7jG9E1le0Y1RqJ4J
0Ys8sscjyYYF515irOV7t9R5wRDf4Syr/rhZeHBUANGevqyHkH91nTUDs33FAquc
nCPUGEThKi3+pEoV9eIcobGjSIcWd+sh4M5akRrquUXvcbOl+6VeI/yZrUfC+tL8
Z+RE+qzLsGUfkfOhwbwEprtuyaSQPIpfe6v7GlHMYtS7W9NAOSZbJ7KJIbKtdOcO
CMtiWxcAszutTu1sst5ac1syV8TwgsPSkitp5qlJW7rHl9vaf3A+wLcDrn9kxCAf
/IzwKfGqKjbRc5OvN6CZwD2wGS2e/AaQn8XVHXNLz7t/SuBiPlOBpJmvtRtnEsE8
zWivISOrTh5qpdDbp3Gylec/8ltglYu9c+NL53R3KEq6AkzPRwC44yTz0OPBLk+M
HkPCnWorX7rMGy2NPWaUa4OmeEnHeAQYVRF3I3KdKIEi9i1IM+hpjjftq9+8SqhM
OVQ3l5+s1C0y5RdsowbOZZDF/MISYHa9loTGX6Dry0W6c39g4yzn2tyf6carMycq
RqQYR7FnBMGvbhQWhbNn1joKBkQoI2kiTrdn3QA7yhbeoLO2fug64A0l7VtdR6v6
d1FXKTcNFBJiTkNim1X9Evk3F7E8/FOwKQqRNdW+2wsiKCyFcBGu1LM1rjJDBdnV
xh1RGzz/LRz66skHMLnOgsNM2V3TblE28PZQNrmNqcSIv5eK+CXTlO8q2yp1MeR5
KeupsCiu/2ARCmTHePcO4ZoQllXzQwquc19p5jca+1kIQwFsNpM41cI0XCPzMVCK
fT6OWJNL41TYzPK3rHqN67GrugV98BBY6KfpAosxtMgZ1KoelrCAlD68BaIJJbCW
sXy4FnXgslZLs3b+R9yOuKbrWEli45/UUIW9e8zvB5pceNxWSg70WgykOvnBmvcC
sgISnVgTD1odlMa8gJwohbrryLzFbtpb6dbp5tBMP9tESizLizWre9UkBPtx9Q+P
p7MT2kne9Bx2XB2kZqb2uqhTo5vjFgsVRwzjImJ9wfs12XZGChkeGqKTyKOQ859G
WJxGUJCoLt74RLLPOJTJEgBibmGvs/fc4PmQcqxucp2Fs0kMZ5WYItF0DzpMbdcX
waNzhg+MauksASn2tm7D5a5yd7uTaSoTL09gFBr35gRBdKmg8lz4ux3bttYYSQTF
9ioY7srsLj4QbHLLCfTqh0+MVvifbizFmNDuR29KuATR1391X9OenKKpIm0S9ipH
aLaY41RR7PDA+qjtypnNr0N0ramUOP7MeAaEPPczIarmrz1K5KbJrcUzOqiEDLoA
ZggjdwIpYYlAbpCY3FYksI8l8Wo75sPSo7scdUTIfl6FwhwIJ6nqLIG3QG28ovpN
XCBdcdSvc3Ixt4wsoCJxguuUA7twFZHfoGDu7f7Dc7bdwm9UBJ38QL7frr8/UYQQ
Ltb2xTiZKsMFEc7q3KiH8y2Z1pjRUf+0ylkb5XI/5mClpr96L/ldErMb6nn221qg
PldLvNA47EWriCXnvbCuf4ikKoh+h7F7LpmDpEmEj7JPgLjDE8X3ShdTzZOBNOeW
1JucBZVnMsVseOlddvc30X+BqiizXsNQ9c3atc9A0avuhslocANQoH9x08VRkZky
m2iHfeL1HbjRw+PchbdVfXxwlgO/+AfiOCEVKMHkB03mbbmFa9oFh9e8zQ0Uia9L
43TQolX67p6s6KpI9o1r5/bUzNYtNrO2jVd8TjCmg7m6JkusTBXktJDs/iwCJWCn
ZQI/ghEtYaBtDGHfal8xiY/B/g6v8YkezPf8VXxlIUOrGTfzk3zk/PD3TnbRLy3N
ot49sr1uKpYYdofnGfleclXBVbvAVZsm3I58MpjdOCQsLCxYNgxVPIhFkptUUjKf
/4nQ/X8kdmH5gSs97JF7P2+pw6EimubVOvHTX+gKbp1rHzWUEUtH4JQLssH+8v+H
hoJtKrmhoEPysT+tjPJtbWMsptslap14bwHCfNrtlQnhsE6jrrPFIUB7a7DNL7D8
FDfRazcq1w0JGs4un6GaJ7d1CYzHrOVKR0c1T201uIwzJOyXU3+YgMYfWqIYViW1
AGwZj1PPXM8aICmdOyVpWomBq2tUa0fCSHSD//lltDpr3sTGahPvbV8clhQZhHkF
jyYq5D83dsNKFbcSnsctx4SP71LMaKZw9ttsEzHRRU0duUI149uKpRU0ciGPsSEc
gHhBEgKruGdxX9zWeGEFuBzrgpu3C3LXRbhlGNS7RbFlIIR8WZoD0cMPEVrOt4Y9
pOGMl1/8LiwQFeznZhQVIjLbjWcjDcqzqxscBh1TJKrjl26Le1tFMmHaY147SfiO
PORZOLmnvQxdAaFeN4c+U9pU8DZPMZFa3f3EmoMgi/t16vnw0F/eFywz4GjNLqEt
```

```
d27PzhPuqYPupgCu95ZLVo3727BMwF0+Z+Noqv/X5RFA8W3wXX6Cw0JsSYBp6Xn0
/HP6a5LoHU3yku+sC2C9EvVuPVEY/51uk7oIyTO0pC6T83oa/mQ7xMMSfuzVcsKK
YLvHwwvXZK6kbkyNS0ryODE0wwXoC1UnJ5PEX7V+0ondyRxe0D5SnIGAIR/SyllM
qzSYcMRUGBmK56IirKZ0XmoM34Gv92Z7TNMUZLReIAO1qUHMiOIfaZ1Tp7gbgBZq
5P6nHYB/zZ7qHM/LPSZdWA==
```


C.3.16.1. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
```


```
MIIVWAYJKoZIhvcNAQcCoIIVSTCCFUUCAQExDTALBglghkgBZQMEAgEwgguBBgkq
hkiG9w0BBwGgggtyBIILbk1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LWxlZ2FjeS1yZXBseQ0KTWVzc2Fn
ZS1JRDoNCiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNoeS1sZWdhY3kt
cmVwbHlAZXhhbXBsZT4NCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFtcGxl
Pg0KVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIwIEZl
YiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW50OiBTYW1wbGUgTVVBIFZl
cnNpb24gMS4wDQpJbi1SZXBseS1UbzogPHNtaW1lLXNpZ25lZC1lbmMtY29tcGxl
eC1ocC1zaHktbGVnYWN5QGV4YW1wbGU+DQpSZWZlcmVuY2VzOiA8c21pbWUtc2ln
bmVkLWVuYy1jb21wbGV4LWhwLXNoeS1sZWdhY3lAZXhhbXBsZT4NCkhQLU91dGVy
OiBTdWJqZWN0OiBbLi4uXQ0KSFAtT3V0ZXI6IE1lc3NhZ2UtSUQ6DQogPHNtaW1l
LXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHktbGVnYWN5LXJlcGx5QGV4YW1wbGU+
DQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6
IFRvOiBib2JAc21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6IERhdGU6IFNhdCwgMjAg
RmViIDIwMjEgMTc6MTk6MDIgKzAwMDANCkhQLU91dGVyOiBVc2VyLUFnZW50OiBT
YW1wbGUgTVVBIFZlcnNpb24gMS4wDQpIUC1PdXRlcjoNCiBJbi1SZXBseS1Ubzog
PHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHktbGVnYWN5QGV4YW1wbGU+
DQpIUC1PdXRlcjoNCiBSZWZlcmVuY2VzOiA8c21pbWUtc2lnbmVkLWVuYy1jb21w
bGV4LWhwLXNoeS1sZWdhY3lAZXhhbXBsZT4NCkNvbnRlbnQtVHlwZTogbXVsdGlw
YXJ0L21peGVkOyBib3VuZGFyeT0iMjQyIjsgaHA9ImNpcGhlciINCg0KLS0yNDIN
Ck1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9hbHRl
cm5hdGl2ZTsgYm91bmRhcnk9ImRhNyINCg0KLS1kYTcNCk1JTUUtVmVyc2lvbjog
MS4wDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0DQpDb250ZW50LVR5
cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InVzLWFzY2lpIjsNCiBocC1sZWdhY3kt
ZGlzcGxheT0iMSINCg0KU3ViamVjdDogc21pbWUtc2lnbmVkLWVuYy1jb21wbGV4
LWhwLXNoeS1sZWdhY3ktcmVwbHkNCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5l
eGFtcGxlPg0KVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQs
IDIwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQoNClRoaXMgaXMgdGhlDQpzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LWxlZ2FjeS1yZXBseQ0KbWVzc2Fn
ZS4NCg0KVGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBtZXNz
YWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVkRGF0
YS4gIFRoZSBwYXlsb2FkIGlzIGENCm11bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNz
YWdlIHdpdGggYW4gaW5saW5lIGltYWdlL3BuZw0KYXR0YWNobWVudC4gSXQgdXNl
cyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gUkZDIDk3ODgNCndp
dGggdGhlIGBoY3Bfc2h5YCBIZWFkZXIgQ29uZmlkZW50aWFsaXR5IFBvbGljeSB3
aXRoIGEgIkxlZ2FjeQ0KRGlzcGxheSIgZWxlbWVudC4NCg0KLS0gDQpBbGljZQ0K
YWxpY2VAc21pbWUuZXhhbXBsZQ0KLS1kYTcNCk1JTUUtVmVyc2lvbjogMS4wDQpD
b250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0DQpDb250ZW50LVR5cGU6IHRl
eHQvaHRtbDsgY2hhcnNldD0idXMtYXNjaWkiOw0KIGhwLWxlZ2FjeS1kaXNwbGF5
PSIxIg0KDQo8aHRtbD48aGVhZD48dGl0bGU+PC90aXRsZT48L2hlYWQ+PGJvZHk+
DQo8ZGl2IGNsYXNzPSJoZWFkZXItcHJvdGVjdGlvbi1sZWdhY3ktZGlzcGxheSI+
```

```
DQo8cHJlPg0KU3ViamVjdDogc21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNo
eS1sZWdhY3ktcmVwbHkNCkZyb206IEFsaWNlICZsdDthbGljZUBzbWltZS5leGFt
cGxlJmd0Ow0KVG86IEJvYiAmbHQ7Ym9iQHNtaW1lLmV4YW1wbGUmZ3Q7DQpEYXRl
OiBTYXQsIDIwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQo8L3ByZT4NCjwvZGl2
PjxwPlRoaXMgaXMgdGhlDQo8Yj5zbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAt
c2h5LWxlZ2FjeS1yZXBseTwvYj4NCm1lc3NhZ2UuPC9wPg0KPHA+VGhpcyBpcyBh
IHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBtZXNzYWdlIHVzaW5nIFBLQ1Mj
Nw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVkRGF0YS4gIFRoZSBwYXlsb2Fk
IGlzIGENCm11bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5s
aW5lIGltYWdlL3BuZw0KYXR0YWNobWVudC4gSXQgdXNlcyB0aGUgSGVhZGVyIFBy
b3RlY3Rpb24gc2NoZW1lIGZyb20gUkZDIDk3ODgNCndpdGggdGhlIGBoY3Bfc2h5
YCBIZWFkZXIgQ29uZmlkZW50aWFsaXR5IFBvbGljeSB3aXRoIGEgIkxlZ2FjeQ0K
RGlzcGxheSIgZWxlbWVudC48L3A+DQo8cD48dHQ+LS0gPGJyPkFsaWNlPGJyPmFs
aWNlQHNtaW1lLmV4YW1wbGU8L3R0PjwvcD48L2JvZHk+PC9odG1sPg0KLS1kYTct
LQ0KDQotLTI0Mg0KQ29udGVudC1UeXBlOiBpbWFnZS9wbmcNCkNvbnRlbnQtVHJh
bnNmZXItRW5jb2Rpbmc6IGJhc2U2NA0KQ29udGVudC1EaXNwb3NpdGlvbjogaW5s
aW5lDQoNCmlWQk9SdzBLR2dvQUFBQU5TVWhFVWdBQUFCUUFBQUFVQ0FZQUFBQ05p
UjBOQUFBQWNFbEVRVlI0MnVWVE94YkENCk1BZ1M3MzluTzNUcFJ3MjBkcXBiZkFS
UUVqT3l3aXdZbkN0a0RLbmJjTGs2NnNxbFQrenQ5Y2lka0UrNkt3a1oNCnNncnpm
Y3FWTXBMMmpvMDQ0N2dZRHBlQXJrK09uSkhrSWhBZlRQUmljaWhBZjVZSnJ3N3Zq
djBaV1JXTS91bGkNCnZkUGYxUVoya0REOXhwcGQ4d0FBQUFCSlJVNUVya0pnZ2c9
PQ0KDQotLTI0Mi0tDQqgggemMIIDzzCCAregAwIBAgITDy0lvRE5l0rOQlSHoe49
NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhM
QU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9u
IEF1dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzEN
MAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNl
IExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovB
ouOP6AFQJ+RpwpODxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CV
t2Zp1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt
8p6hAQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4Tg
DqXjWShplcI3lcvvBZMswt41/0HJvmSwqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcY
bwW2lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvwDhJLAgFpW/jA
/EB/WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAM
BgpghkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYD
VR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HV
RDyAKRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0
WTANBgkqhkiG9w0BAQ0FAAOCAQEAgUl4oJyxMpwWpAylOvK6NEbMl1gD5H14EC4M
uxq1u0q2XgXOSBHI6DfX/4LDsfx7fSIus8gWVY3WqMeuOA7IizkBD+GDEu8uKveE
RRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxODWq9opwtA/lTOkRg8uuivZfg/
m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYO
nUmGpfB8PPwDR6chMZeegSQAW++OIKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPU
XTSO7K459CyqbqG+sNOo2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMC
AQICEzdBBXntdX9CqaJcOvT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgP
MjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBT
IFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBALT0iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9
LCOwI2juwdRrjFBSXkk7pWpjXwsA3A5GOtz0FpfgyC7OxsVcF7q4WHWZW1eYXFKl
QHJD73nQwXP968+A/3rBX7PhO0DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKa
w7aRphZO63dKvIKp4cQVtkWQHi6syTjGsgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV
+I65x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyX
t1TL270I6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsCAwEAAaOBrzCBrDAMBgNVHRMB
Af8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGlj
ZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQE
AwIGwDAdBgNVHQ4EFgQUu/bMsi0dBhIcl64papAQ0yBmZnMwHwYDVR0jBBgwFoAU
kTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAHOJojanzqmg
aSN3/gqSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1
```

```
iffRTF/KtmVEDMR/sYeqAH83KM5p3el2lVh4OHhyI0qNuz5oShNaACSioQ23WxHG
Vy9vsdVfnbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6m
rYkKTM/RCGnumghxwYToj1OyD5Gs4D2IJCw+fX5ODxh52MbNRYXTus2ZPRPM8JXN
QC4GWv4km3M4rKnJDd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk22OH4ConlB8f
7R7s1LM2cSYxggIAMIIB/AIBATBsMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsT
CExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRp
b24gQXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrOmqnXMAsGCWCGSAFlAwQCAaBp
MBgGCSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIy
MDE3MTkwMlowLwYJKoZIhvcNAQkEMSIEIEUN8MCE/gE8VaUWOZYNyiuSDKZahJOb
CB59LQgqpUl1MA0GCSqGSIb3DQEBAQUABIIBAEk7y6K+3YZB+tri+EVQFLmb1N5K
CUsnwbyLwl9bH3bv+8MFEYqYmiATHzimOxdQNBl8c6HR7GqnMQVJIZ+OEYiL1fz/
Ej7Up3VQzyR1KvblL4Xt1W7+ITh/6iAx1j1W48US9pMR+05Rz+cfVATn77voVNs3
fN0B8EsjPoVM708f/xKD5lwHv/72Mg1fUTs3YMaqabplXdABkdp1lQhZ6za+N3/k
yEYSmxz0Owd4JRKuAIdbzdFIC57BIGFICQX0Nr1c3aZ/wHvNvH2xOAp1cQ7M6Nu3
KImZs86OBQmc0Kdk8AzE4s0o8mtf3uhU+eJ/23FWjMYpGdgHaUu90GMnKnM=
```

C.3.16.2. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-shy-legacy-reply
Message-ID:
 <smime-signed-enc-complex-hp-shy-legacy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:19:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-shy-legacy@example>
References: <smime-signed-enc-complex-hp-shy-legacy@example>
HP-Outer: Subject: [...]
HP-Outer: Message-ID:
 <smime-signed-enc-complex-hp-shy-legacy-reply@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 17:19:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer:
 In-Reply-To: <smime-signed-enc-complex-hp-shy-legacy@example>
HP-Outer:
 References: <smime-signed-enc-complex-hp-shy-legacy@example>
Content-Type: multipart/mixed; boundary="242"; hp="cipher"

--242
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="da7"

--da7
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset="us-ascii";
 hp-legacy-display="1"

Subject: smime-signed-enc-complex-hp-shy-legacy-reply
From: Alice <alice@smime.example>
```

```
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:19:02 -0500

This is the
smime-signed-enc-complex-hp-shy-legacy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_shy` Header Confidentiality Policy with a "Legacy
Display" element.

--
Alice
alice@smime.example
--da7
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/html; charset="us-ascii";
 hp-legacy-display="1"

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>
Subject: smime-signed-enc-complex-hp-shy-legacy-reply
From: Alice &lt;alice@smime.example&gt;
To: Bob &lt;bob@smime.example&gt;
Date: Sat, 20 Feb 2021 12:19:02 -0500
</pre>
</div><p>This is the
<b>smime-signed-enc-complex-hp-shy-legacy-reply</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from RFC 9788
with the `hcp_shy` Header Confidentiality Policy with a "Legacy
Display" element.</p>
<p><tt>-- <br>Alice<br>alice@smime.example</tt></p></body></html>
--da7--

--242
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--242--
```

C.3.17. S/MIME Signed-and-Encrypted over a Complex Message, Legacy RFC 8551 Header Protection with hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the legacy RFC 8551 Header Protection (RFC8551HP) scheme with the `hcp_baseline` Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 9580 bytes
↧(decrypts to)
 └─ application/pkcs7-mime [smime.p7m] 6082 bytes
 ⇩(unwraps to)
  └┬ message/rfc822 1876 bytes
   └┬ multipart/mixed 1828 bytes
    ├┬ multipart/alternative 1168 bytes
    │├ text/plain 393 bytes
    │└ text/html 491 bytes
    └ image/png inline 232 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID:
 <smime-enc-signed-complex-rfc8551hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:28:02 -0500
User-Agent: Sample MUA Version 1.0

MIIbnAYJKoZIhvcNAQcDoIIbjTCCG4kCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAANFe+QhN1IuF/acKoQk/CrT7s6ncIXk72bZ
yqANUj5IWD/YQPJMczB4khaPZRacFIWSbcn3RHR8H9kaincGgB0F3pw+Ju1CaD5x
Lj8pX3ry1b2BNFPEMhbHQy4RsrZpwmL6qSc5X/qWbJNvA83xnnE+avEzW4JFwH1l
RRABOCiNe+lRF7L+X/kqJL0oALwBWLn1OsfK5AwCg3Vao4uyRUtRbC8P4Q7v+KPi
6qYEwXAe6gz1LCwD/EPyiDnMBlbNBid0g8nC8pt2Ymbz+SljAW9FDv9Xyv8iJuXT
+OXOgl8pfBA1a4zKGiRZrKN0PDf0NUh13p/0h7Wd/322eR+FTuwwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAHNOf6aUb4tfH2tb0OWz678eY
tSslVolgGLYIrJcX3Xz0ZVEg7EHJfwMMrfzuvaXtMu3VR26TZpJxJrUQy5bplIKf
rb4ZF95XeC1KMC5E88kpOX3qb+ALpsnRbUvldPfaG17GQl1LXRML16Xvw2BdQ/p3
O3EhpITTSdzFYJOjW8J58JGe1M6sjsymI0KJZdEtvG77dNhNAXZfmbf+fBUZ+237
Kc0nbd3dWtNmriJONPKwK5qF1UO1JHhGX8/UquWY7bjXYv/kH9YYZUnR3VCNFQZn
KndxvfG/jJ3HofDM6XgEZf+hogg9JVg9LN5IGmdmau7/YSt/7q8k53AL3YS7ADCC
GG4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEENLhBGpw6GdtyReA3vbppXaAghhA
```

```
yG+aQIQUVygKLkRUL7c+MZNMnUhD+I7X9lWOHMlTQnrHagQoCxlKw9b3v7LCUbCL
SabxdNhhBnQwFpgec8aHPFojjM592Zg/7AnYYDqMAttYhoabFG7wSg7+ntlJB/AX
CGFWd1ILOTHr/PghR4rgOmO5/FosuV0PdfBrshG2CoOWzeLtFhzUle1iVtqxq+1z
Varyg1qLwtxMAkMP052WmVhqNw9WSsvIxXVYcjWdbn7g+lJ5N1BfcjHXnjn8AjL9
1IzHmuHh4ZW9C8S95gdrn8ipd0oee1Ubpu7KP5C/W1H9MDU8cesFcMmUt/WLNxeb
09fV0ILaXDbnLIVTQ3xHdoQzg+TQCB4300i2Wvp6UhPnlE6Ap5mexGvObWlIIwEF
RKO4lWVNxEoGB223n10LH6mqJxpiqUK9SYIhNCfo8uxIdZ5R49B2jbzC8e1Owefm
i1QII6ZVnwPltALSvxiL97GSHG/32YmITrsZBpTitY7Q4tcDgzfFGRV23R89yorp
AuseNYbGJ5Mb1qFtbQZKycW+2RX16qt4hlcsf6wYBCzI9xOzsSCHJW4KVZc9GuIu
0Cmc3M5mFgrWwKhCvdJBo6fLwSqTTj6moGmqBLIZ1ouiamOOzxY+VBrpLNSrnnKf
SdEUgsHuJKo+A+oy0vhHYZqusnoE4o6vE5Sd/R11q655O/jI6ngCE70yZpcCxKV5
0JgsFeUSjBLtIqGVGPwKRAreug/2rcRWDBlW4QTZ0Yuw7Zu/xVPkAevp8Hn6v0C2
rxEpaXnhzITeCsS0qLN+G+vuQAzDxz4SlpWxx6HajBToje79ZtuF/YzAZfJTWsKO
MzxO8hOCxEl/7z355AmXrKF0ubZj+/Y9UTXlSqUUXV/5b0L98xU5NoAaAhzssysb
fXLHgi1CXMNZBUL6Ukv2ovWz/9ICXHd3GdmNUW1OIFRmPdY4obnMtCN0Jpkrbz8l
2Uilu0BVtsvsAmhfzgo/v7MMAoeFLkc+idCOexM3v4H2tQlJ1V8MB+yz3IbM4RMA
UvnAn1fxjsR7Scsg0txauodFltdywA+FnjPJwT9if73HZ2/Lb8bs8ri5iv5Jl+XO
FjsmhyKMUeEmlUXbJ2omjDnnYmYzogYXTs5XSmrZrjvoIbQAKtmxSKywQRNfHjei
81VcyyWadLUCZn7PdoQ5qtxSHPRr7upARLAHHljWAL08MHfJSNyN93jK1Ktxkefk
9/k7WAWsYvkynhGBBolvydzUpK8GwS06+at+UGgUHOTs69RrwNWPwJjuw2sS9hX8
DHy0eGAKKAIrhMcNNJqjnQ3aEP5imIVhTlh9ZEKQzF3ywpnlpAfGdBh0Qkq4cn0p
NVpG+cLWt/ccY/ROFY3bMAuvxYOr14fJNcTRbBY6uTpgSKEoQzY77NZ0fk4IlVcU
NA1PMf9+ZysrYblQB70TggQSb5R3Ik+Xr+BzS7x+pXiBuFlU7qSnxXmLIzyK5ElU
HfHkeAIAC8ReUSsomobYl+2mmyvvWCLqIR9K3FtGtweZ9bQ3NY3lOuONJAldB9Ge
cH2MdHvckaTJNx12aDKA4bm0gHEx6XXDzKARPbcbHDeu+eJ3SbGJ1C8XBqrXxgLJ
MxUxTVa3uc+Dk7ZY4jzZbGoRVLsUFvCnJklk64GbzydMGplEPH2gR2fjecRbFknq
6DWdaM1z5J13GJbi3g2mXo2JiWuUBQCLnbdKTAbXdNDBFbU1oVVqMK5PDrQ0cExW
Dnxa3r3ae2W6Pfvk6sS6LzpvMJUhGfQzhdkgBRfGrMaM7FG8hdr0ZAqJxhu+vS0c
ts3hiS77m/KQhyeEPzdNkVXAUHAsaHQ9PgEc3E6ZHvUiDJAYBeQ3e4kXhZZN/NaV
fAlGKplZjWc3RYQK0h2f6ADxcdG3GHAE/vHa9QkrWHUS4QuX/h0aFYDX/bwAg036
wsYK8WUVTtpItYfV3jTMbfAuLL8En8qYgJNPQcb1SOOC9Sv8qBg0PSlSRQhpG+oW
lkWTWEKOn4X0hfV2uo4XMIf93SMvRss8vmmB0Kjryr92tGX3CdjWJTjFJAtcNBVO
7Oz5lD84LLJW8vyGMvZ4trxnbVlg9REopeDVq2BJeznYHzOQoawXVM4n8Z0vgp4m
xlleVprwb8nmVUyOvxozr09V/ki9aSwZIFnHdMaVX3qwXUZ/1eu0AJJ395Ea6M4o
hM+Iqv30A19496kpHp8sfYeZsHtNNwQG4WbhpnXAdR5pJ1+CMjliLFgpkfmWXn/J
KIF2OSew31/v7JtxUUOHBNNvs+SxLwDqFK4RjuOUBJNEA0EgCvkfpdyAbqCS15g6
fx6do36Gz4mxXNMJRqP4qunv3MVxEb+igwEPOeSxWpw9vP7XaFiit91Euoj9/UIc
ROq0Vo3JuB9XM925T7erNHhkhdlUW2utiSjUrHOU0PIZqzbCaB/L+Sb1HhnAKFDJ
Rg2uD55Mwv5BdpBTnPmq4Wz3kzvuIop7hUzoCVDhcM4a6OIRXgyGeKHOs//ca439
zoy7aNurEjQSKjFs4dfj5z64b1GIu33X/Gpg634bowErRXGQ1FpOy6oGnD8LIkOV
n+VODMvu5HTDcYmmNtWLRBImmdq4Er8gUN8LjZIoh/z/F+QSGWoW44pHPwvCV6/k
6RFcaQKsPx3PHPqRhM9yAmhTWobMOnJBTLccFsxYQWXe2t022B7Ecdoa9QjT7OkF
+9KpNTPFPlYPMKi1F+IGf/g9KgVd6UHSQoTQOmunONXjuKcebamy4kRwP72qOqj+
jDMBlG+jC7I9neZ1/f50DT26av9B8HfyxVuzTBg0mDSCYvrA+yxHFxiyEO9zH5fv
oq5JRT2rXTyq2RZ/EUyOa5Ye0HUI2/veje9C7yOQMyJcqOFWukw6y/BHOo6M6q//
y+S9yMevzh8oxjkjCsx/lrM8kueF2klUxG/Xzm+uR3Peijqlus961Lx5d4qY2XQk
gIVsKphv1I47AYxtDTPx+mXRlm14NVl1skrcOppwfAvXwUBiEuxBrVrrBafj4l6M
VszKHsELw6Ub1/6NjEkp/C72s0bqRkDna0Q4ls3s1N23wylOkWooujWI+w1r9E1Q
RT8u4kWJtgBJYGmiBRWN9jMxaOpcf4VrU0HpxNpY7hITQ4b6/KB/28UE8EB+cFp/
NmC6+vx0jKPgGsLYGe0eaZoUUVXW19PmV+tbvRbRSxcLDSzsBRvCsEoeK+KBc+r3
7/n9Z5BVH50RQx31KlAEadF1LXVVANh/ZHBrC4TBTaFMGvgJjQZJ3Eax/RKkS5oN
/APYHw3zDNFWyhtXRtL0tEG2oyppspUmfG1ZwlAlrMa9dBOkRr3iKlVlyW91tOQu
8Q8gDHcdNahMDHdTAIeb5bU5nd7Qr/2uyHIg8sswxWHOjI+l37Qq6sg6wNfq6Xhu
to1/MHofcQlMiQGVucZIaQR82TjNzo99ezyu9ZAbu3J4pm2pLmHeQjg2m1+TO9NA
jdctddks6cbw/bL2yFGw3juupSLTYtYGK9uWqvHSp3O6zLS2b2ihEPBhe5V2UgLh
Xc/CvGAWbLTJgqM64FuUPsDjXByGcGreSA3bIG4AU5hhD+SwSoaFE53Qw6FETH4K
BVcGedXnmvkDZrDxwSoRpAqHAkPdrxY+yt7lFiv/dGtfQtMCYv8flAP/bVtWNung
wZODrmwI6rJj1Ooub+PIT31MXmm+FbM6yFq3EtfZbq2bKivzHUZpiwL7afe8s+RD
```

```
rlZoz4y2vOJwi/REMIDLk1q4RnFcc+FH/ZaG+gMdfkduY0iGfyqIIJeQx5HXhTDV
gxoy356pQ7QCVdAUoyP/7xp9gKqHbaNFt77ZM+68KGPKuEi6byYJki1gXrB9oJL4
JmF1jQSZMYqj+FgZBbrc9G8t7vTiF+8OxfxxS3G+GVdCGAEjhz4dQww1o4vIBmdy
mrsTEs205qD7Asl0du43DZrXSBt0ppfTxTEjrosTzRD8Skd9AvhFGKhtSFGePNL3
8UqnQE6jmbHHKQt7Z4DJTQ/ZyheYUawAPLLbpX4COwUHDo8YawF+vghitdt8K2+v
4dkQh9BdyFXpfqXSBDa6XcQPscLxHwjFJPczCeATuycA7/bNguS47InBGg5n+Z2/
nebOemWFiOd9Fg5uMOBruCHeHCNPN9BZ66RQ7FL+jbXO39Tq+QX/NnzW3WBnoTDJ
GEzULm2VjTn18gMlflVRjNENOC1yUH3E9jWMn8LEuTnUXTqfEfkkj9lwUXQxNeYf
uVvJ95gDas8aC/O/MmHLc6CFfq0l9MGu4FYXMfRon6cfJZCpgfXQnJAqxlxMb4wI
qMUyCSzZ3umKCD+UAf7MIMyCMEdOMLFoO6LoNofFjNooK011sR4qJcM/zXiFZQaO
eCoxyIBESCv2h/LeGRW6Sx7iacntg4Se12zPlaG7ckuiz6PCY92g3WGj9E4ARWIB
VDIkJo74MDUSn1osHHojKd13lqdAH7Am2UjoIVogx8cE9cSEnmZfwZBf2Pb2TxwF
FTWG7TqheJzJxWzj14sjMPwBZRJQCdmscn8XWEeEk7BBUEGbZi/3Y+PIMe9G1ZYF
3bu9GNmM4JcSdH9FX0NSUdQQrgqDey+C+UCjFD1GWY1Ja18vHK1C3ssWd3wWFBLF
e3/Vg4GZhYPSgmTVRk0l0pGR7XgMEBbGGZgloknFBetlJ8F6qIXylDNsMTQ9tNJ6
rBy0Ite6Qcvma+bz4CSR+y/FWcy93BFKVFC6y/izfdK5InHlrgBEZugR2rR0oPsJ
wXaoSHrkza1TiW/CsghAx1bjQ4Z1YtMaSfCO03nKQ4z32hFcxm/de3ZUJWlaEp5O
w0c7kqIzfD2w+UvtcceDo8uc7weRtiYi99K8x0ZtXTfSjWwcJcH5Unpcd3dOXVko
x+ag8enG3DfmVmBvXxsyCboqXJj7FWhFyLcPkZXe+OGDj5Ms3wno8JH8aKVdrSYR
XmNzsJP9a2CMSEDhaXfaWHQqYSrV3Eg2WXeCbGHUHPCUF5f0uc9RXNN0Wtb/MBuv
dcCNytFxYNgT21vpQ9VxLvFjw7Tt0NjLa9URRObzZrd9I9g0MJrmw59DJm2kbBoX
3qcIq4B693ajEaJC2qpBAszTCEq0AcUzAaf4KunE5LwGY/iYzxngRiW1EljyPY+F
wYGgIY8hMkQsZfgwBnzZvr9jhq0s715VEIAmJY4cdlMhRVUf+nViVTxHqSOraXlR
I886EZmgNqMIXoJQinAaitUNiUcxft+vrfXBhBnGOnvIQI807wY2CHQhcrTbLX5v
hgNnKY2Hd6EQyYnWRXGL59jgACyfj0dbdEsWtva20reWMx5fcPkVQ500H0E2hdfa
yBzIJxvOvkSLLwsLwPxcbu0S92YnFr2FrO7+G0w99FjGT/xnOhVEwkvzHjFzzzlo
fhSumEUFU6gdYi6fdjngVQxqdz/rfCWqCj9IEUrJxKUnsU322RV6vutgOjQ8ENkz
zqdY/TOS/2onRIIsaE/ul1P6Cvc2XezmZI4819aARPsqrTzeH5nVE3D6EWrieDHh
LOmvIEkE64ZIKwUfG8J2hs2ALyraD1ECpQKBakW+f7RgFrZNui/4LIW6Hxwe58A8
/SQvMf/OJS7dtwX3a3Z4w2nnnp2oXV1MgWvXnuEIPYDQdaIqh1CRJwk1fu+Su7Ys
2kfOs+Czz+nBq6CRDD20YpP3rBurR+JmdBfyvR10a+pwlWqWaADYfzmvKNXcikYC
h8xCp23xL7p62XgVwVtUEkbrQJBbCShBjZZxBx+RmAoYcThcsggLLLl/RHKGRqQp
XI3gFKEy27HV6X4G4qMkJhzuCAvHASoSQj4g/KLwaYf+njxeRSzwPRkjCn7Z0Men
EQreLcqvHQaoR4Exo8qFJFizkMrEr1uTRtyxFcvqJcLUffPhfUWAuPwzS+CeiK4F
Y+hLYxzieVmP4lpxu1spWJfQgUlO5/6pj0051nMwjpfJpB3tjFFYKhKrmjHqRSHX
owguPcxkPMI/SwpRZWRROOMSzh/ph6lR9E/KyeaWGTjDCDD6tdCjsLGHCuX3UzZe
+AMiDhW1AWw+HkmkLEOym4hbQnQhwuzYLUS6Cab/oN/UvBnjhrIdG8s3YF71PvY+
yPcq8AsmysxxVvL7Q205BeX8nRNhFeJc3asMBvSijuo1VMiGY/0wzzjasWZH5D5b
KTBJIqXP57aNaW/BG6eIiaSxVoLnsbgW57P0mpP5JxK4f6cvMPihO9rNItSqESuK
6oDyXjXzJaYblhrOJkOkVp4gjpHMmcsc1oruQDzWXMUNpdvPUnYnZ0yYKhmdbHoO
n+AKgwh3tmqItejAdRLthS3bwMdwgEEx2sfnnnKwEy6Xqdu5oaB8rVRtKcMxFIvA
NVefdCft4+2brFXPQv2HsQWYdVcdZMdUT8WLL7VUJ2mXiVP5422LEspTxFgBb6cV
jbfKu6btpQOdIEux9YkD9zH5ye54Dk/FcElFQah9MGZOGS2P3AKFLcLLxmprHWFv
2SE2EEkTQzp25c67nzd3/r8LNAmupkqTVHuuIvuMZgP9xIiOuYUzGrUL7k5EJTWk
OMPRQeYS8iv9v3QEarSPCJLyeUpZjXVu50u1kKgLAuA/s32/aVwGuTCUMNgGQx2q
jpozo5jYDAUv3l9EitrcM9X9WxvYP30rsVs4kNvRM08RR2wfs6sHb//t49xOL3hW
mbpAXbFz1WXIE+VvVoO9ZCsXx3JBRkWxyxoUpDibijBQirYkwWx+TdDm4DP27KdM
w70bRhM5jVqsYUgIfA756WFIpoaXrRpCHja1ZXyaFs8pyoSr7XZIZ380A8kexEB7
XsKfB3vBf0gcJsYVn3ebojEpFSjC4ayUxJxiNZVtluyIcz0gGdo5AWGo/0BstflI
nFbx+4D7xH2SwPC2XQIXrYJnsawqEb0H4+hPVg0C5fnqK7QrjVWLKx2b64z+VowI
xHyiHfWrcAfMygh5YBAQp/XoLzDL65VWKYbCVOUzFy2iwfoTs1RbqcAPRhjjdMJS
U/ep/EBPa8bF5KNKdq8G8OhcT0Y3iFEW45kO6E6kXs2w3NgHKhrU1wY3FLDD/w1u
f7SjMtPVN1HEhrQoEUGP14fztUBRuC6I2vyOjiJ0RaJG+TU2ZlKs2sE5ey1EUKnk
dvETYA8Qjso3JYb7WWMRKTtiaXj/tPMVGvqfD5OQxNLGcvS1qjds5eNMuXHuoflC
fyubtOU6FmS2oThM6r6/K17GXjg7Usui1XtL8ATuKMKn7nQG0zQJpFeDawJER6KB
8vTrjgYlZQkni25eIiOLH1XpaJXUIDWIyOeDxYCrl9BQHuKfOalo5f7WQ56cp2M7
if3rUpGk+50tx2RWBlWvzVJtF5HEB+1xbaaEaMCqS8OexHWQUcZApzhnQC9NeniN
8oeLZkojmOPHUNZti4lzBwqJvVj4Ag455hWXFMzy8lqlzOivvfYzIquQOYaxozXS
```

```
mlPRhaYLW4WkYUnM1+J40IZAecidJQ5iEEaYwdobd2LL39eURvA0aPdSQw09sZTG
CLhkZY/8LkshqjQaYGghQpnpGsdTUTvXqWoDW3cGZmk6neKVFtkwK/JmxT55kkCw
jig7s8ksL+8f/sOsI0I83n8EEO7ymicvVuYrAMxy3bYXeh+nsrQYgbrNwJxdU9CS
oPJGXqnV9iXVHbTXevXGyccoq7whEJeE1q8E9Yi1VlFSctOd63f3BsZ7Or8qKAYW
A7hG5SUmKYqajYlDwPqFJmX72sOofNh8qdn4K1P7zzfOjzi0Zs9mBqmAzG6U+Ciu
pYwRzQALIHdR2u5oHhnGU4sqIXXyN+RrRL4Z8zaX7ECij4TuD1Fiu/rGoarnirn9
oMFF1LZvBGlweg8kIBNPCbEZyO03EQBBjUhqSuXdo5MNHlZRfGtV0ea1pUKOMZE+
2syqcOT0iR4itBy2uqxReGVDpOVI8YM3iY+CLf4d+cZXTR1+ep27QWAEzz865yRf
4d1sRczE/iqpjcXuERcgLN7fr+21Ob3JFSq51iTs568sVnLyX6JtZCi4DLxtSSDJ
LXh0bYnUw7+x30zmP9zNMTK+6fsalN46iD/+MmnSC4h2/aCYBHplYPyFzPMUbSDk
+0uS/NB34PyjK+ZX0ouEo+fSvM/TFWNBHVlbiFZZL58/+F7Jk2f+ojtViMTrgHZt
j+vEd4UwxKLV/jgAT5ktM3WYSGDzlqLxVXgFAST6TYzGhGaxNkLUWBXfuNP0klNz
PwSS2ychxCl+jUgjtHtenhfVfQtyG/NzKnx0s5vazdSRe4bnVBmqm8i+dsUqyPCd
FYDZOpfnljZ1ywCw30yaeA==
```

C.3.17.1. S/MIME Signed-and-Encrypted over a Complex Message, Legacy RFC 8551 Header Protection with hcp_baseline, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIRQgYJKoZIhvcNAQcCoIIRMzCCES8CAQExDTALBglghkgBZQMEAgEwggdrBgkq
hkiG9w0BBwGgggdcBIIHWE1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6
IG1lc3NhZ2UvcmZjODIyDQoNCk1JTUUtVmVyc2lvbjogMS4wCkNvbnRlbnQtVHlw
ZTogbXVsdGlwYXJ0L21peGVkOyBib3VuZGFyeT0iMTQ0IgpTdWJqZWN0OiBzbWlt
ZS1lbmMtc2lnbmVkLWNvbXBsZXgtcmZjODU1MWhwLWJhc2VsaW5lCk1lc3NhZ2Ut
SUQ6CiA8c21pbWUtZW5jLXNpZ25lZC1jb21wbGV4LXJmYzg1NTFocC1iYXNlbGlu
ZUBleGFtcGxlPgpGcm9tOiBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4KVG86
IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+CkRhdGU6IFNhdCwgMjAgRmViIDIwMjEg
MTI6Mjg6MDIgLTA1MDAKVXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEu
MAoKLS0xNDQKTUlNRS1WZXJzaW9uOiAxLjAKQ29udGVudC1UeXBlOiBtdWx0aXBh
cnQvYWx0ZXJuYXRpdmU7IGJvdW5kYXJ5PSI1NzkiCgotLTU3OQpDb250ZW50LVR5
cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InVzLWFzY2lpIgpSU1FLVZlcnNpb246
IDEuMApDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0CgpUaGlzIGlzIHRo
ZQpzbWltZS1lbmMtc2lnbmVkLWNvbXBsZXgtcmZjODU1MWhwLWJhc2VsaW5lCm1l
c3NhZ2UuCgpUaGlzIGlzIGEgc2lnbmVkLWFuZC1lbmNyeXB0ZWQgdXNpbmcgUEtDUyM3CmVudmVsb3BlZERhdGEgYXJvdW5kIHNpZ25lZERh
dGEuICBUaGUgcGF5bG9hZCBpcyBhCm11bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNz
YWdlIHdpdGggYW4gaW5saW5lIGltYWdlL3BuZwphdHRhY2htZW50LiBJdCB1c2Vz
IHRoZSBsZWdhY3kgUkZDIDg1NTEgSGVhZGVyIFByb3RlY3Rpb24KKFJGQzg1NTFI
UCkgc2NoZW1lIHdpdGggdGhlIGBoY3BfYmFzZWxpbmVgIEhlYWRlcgpDb25maWRl
bnRpYWxpdHkgU9saWN5LgoKLS0gCkFsaWNlCmFsaWNlQHNtaW1lLmV4YW1wbGUK
LS01NzkKQ29udGVudC1UeXBlOiB0ZXh0L2h0bWw7IGNoYXJzZXQ9InVzLWFzY2lp
IgpNSU1FLVZlcnNpb246IDEuMApDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3
Yml0Cgo8aHRtbD48aGVhZD48dGl0bGU+PC90aXRsZT48L2hlYWQ+PGJvZHk+
PlRoaXMgaXMgdGhlCjxiPnNtaW1lLWVuY1zaWduZWQtY29tcGxleC1yZmM4NTUx
aHAtYmFzZWxpbmU8L2I+Cm1lc3NhZ2UuPC9wPgo8cD5UaGlzIGIGlzIGEgc2lnbmVk
LWFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3CmVudmVs
b3BlZERhdGEgYXJvdW5kIHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhCm11
bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5lIGltYWdl
L3BuZwphdHRhY2htZW50LiBJdCB1c2VzIHRoZSBsZWdhY3kgUkZDIDg1NTEgSGVh
ZGVyIFByb3RlY3Rpb24KKFJGQzg1NTFIUCkgc2NoZW1lIHdpdGggdGhlIGBoY3Bf
YmFzZWxpbmVgIEhlYWRlcgpDb25maWRlbnRpYWxpdHkgUG9saWN5LjwvcD4PHA+
```

```
PHR0Pi0tIDxici8+QWxpY2U8YnIvPmFsaWNlQHNtaW1lLmV4YW1wbGU8L3R0Pjwv
cD48L2JvZHk+PC9odG1sPgotLTU3OS0tCgotLTE0NApDb250ZW50LVR5cGU6IGlt
YWdlL3BuZwpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiBiYXNlNjQKQ29udGVu
dC1EaXNwb3NpdGlvbjogaW5saW5lCgppVkJPUncwS0dnb0FBQUFOU1VoRVVnQUFB
QlFBQUFBVUNBWUFBQUNOaVIwTkFBQUFjRWxFUVZSNDJ1VlRPeGJBCk1BZ1M3Mzlu
TzNUcFJ3MjBkcXBiZkFSUUVqT3l3aXdZbkN0a0RLbmJjTGs2NnNxbFQrenQ5Y2lk
a0UrNkt3a1oKc2dyemZjcVZNcEwyam8wNDQ3Z1lEcGVBcmsrT25KSGtJaEFmVFBS
aWNpaEFmNVlKcnc3dmp2MFpXUldNL3VsaQp2ZFBmMVFaMmtERDl4cHBkOHdBQUFB
QkpSVTVFcmtKZ2dnPT0KCi0tMTQ0LS0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0R
OZdKzkJUh6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjER
MA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2Vy
dGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5Mjcw
NjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYD
VQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAJqVKfqLwaLjj+gBUCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg
9r1mAfIDlB/wlbdmadXPmrszyidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07
k0sV+UdSNRFxrfKeoQEFXgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74
zFCWp2f1ZkuE4A6l41koaZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY
9VfVfcrv9w43GG8FtpSX+TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r
8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcG
A1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5l
eGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNV
HQ4EFgQUolNB1UQ8gCkVfAEj8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfx
CShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRG
zJdYA+R9eBAuDLsatbtKtl4FzkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5
AQ/hgxLvLir3hEUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5U
zpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGn
UZROSvSYkGiWDp1JhqXwfDz8A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19o
WZD6YrzSWHUz1F00juyuOfQsqm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgw
ggPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUA
MFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhT
YW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEy
MDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYD
VQQLEwhMQU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l
078oullsk4ASvSwjsCNo7sHUa4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6
uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEO
ls/gkUP2GxzymsO2kaYWTut3SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBl
fkgKN5wXVgkWFfiOucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4Ku
ElnAtJ7BtZcsl7dUy9u9COgEykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8w
gawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0R
BBcwFYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAO
BgNVHQ8BAf8EBAMCBsAwHQYDVR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8G
A1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IB
AQBziaI2p86poGkjd/4KkkOHG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAo
cCn5zbzhW/JVdYn30UxfyrZlRAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoT
WgAkoqENt1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2z
L3HR+M9CDr4Opq2JCkzP0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF
07rNmT0TzPCVzUAuBlr+JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSr
JNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRG
MREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBD
ZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69PhqzpqP1zALBglg
hkgBZQMEAgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJ
BTEPFw0yMTAyMjAxNzI4MDJaMC8GCSqGSIb3DQEJBDEiBCBeode6D2+XFP+H82l3
4jEbYjlqU5Tgru11NftjsHf5ojANBgkqhkiG9w0BAQEFAASCAQCPddNTo2dMep9S
Ux9R61FJylyqjA4n22MbI3haUrxVOgk1+FAacmva+eo8weKDd+FR3fYuy4C+PkIj
woclAH4Hb7QkNHQgv5DSuvqN1/QoIHpGvF0atF0NXKOirYFGIZmeytKJJ9WR67A1
Myuh/Yi8aaUDheliEIPsD+59pFRHDZIcM1MkNuSJGw6LHMCHSA9p7WggrLrD8trC
```

```
rR/xL2ZWbswb5sr3Y6NucbZS51e0UAy2fKzxK/CUFG/M4VhFQF1UgUZU/6hwXHMg
ffr7xEDPeco1Tq7/fCLCVYz5Ixf+RfCOid7Gps07qsQlMIV/awPSekvMyg93nqDv
ES1xMiED
```

C.3.17.2. S/MIME Signed-and-Encrypted over a Complex Message, Legacy RFC 8551 Header Protection with hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: message/rfc822

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="144"
Subject: smime-enc-signed-complex-rfc8551hp-baseline
Message-ID:
 <smime-enc-signed-complex-rfc8551hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:28:02 -0500
User-Agent: Sample MUA Version 1.0

--144
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="579"

--579
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-enc-signed-complex-rfc8551hp-baseline
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the legacy RFC 8551 Header Protection
(RFC8551HP) scheme with the `hcp_baseline` Header
Confidentiality Policy.

--
Alice
alice@smime.example
--579
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-enc-signed-complex-rfc8551hp-baseline</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
```

```
multipart/alternative message with an inline image/png
attachment. It uses the legacy RFC 8551 Header Protection
(RFC8551HP) scheme with the `hcp_baseline` Header
Confidentiality Policy.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--579--

--144
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--144--
```

Appendix D. Composition Examples

This section offers step-by-step examples of message composition.

D.1. New Message Composition

A typical MUA composition interface offers the user a place to indicate the message recipients, subject, and content of the message. Consider a composition window filled out by the user like so:

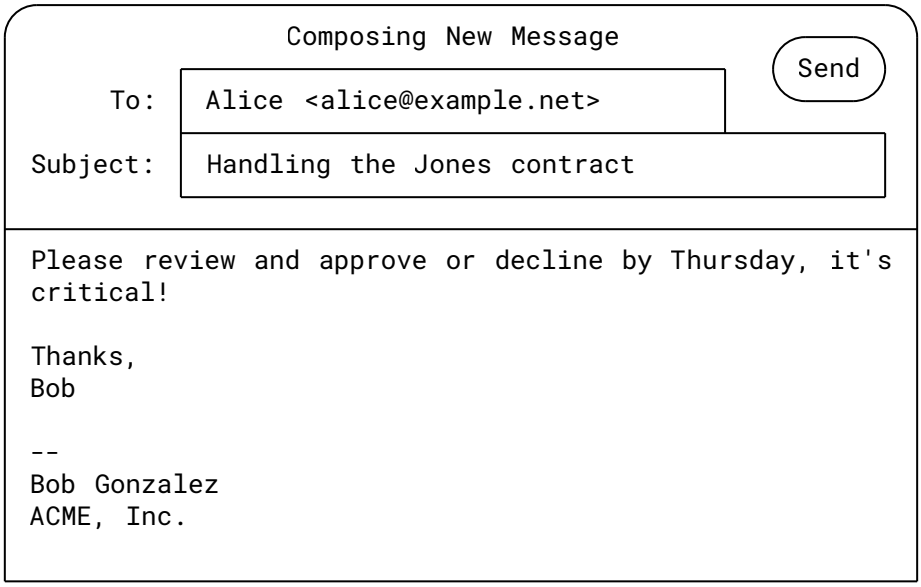

Figure 1: Example Message Composition Interface

When Bob clicks "Send", his MUA generates values for the `Message-ID`, `From`, and `Date` Header Fields and converts the message content into the appropriate format.

D.1.1. Unprotected Message

The resulting message would look something like this if it was sent without cryptographic protections:

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: Handling the Jones contract
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0

Please review and approve or decline by Thursday, it's critical!

Thanks,
Bob

--
Bob Gonzalez
ACME, Inc.
```

D.1.2. Encrypted with `hcp_baseline` and Legacy Display

Now consider the message to be generated if it is to be cryptographically signed and encrypted, using HCP `hcp_baseline`, and the `legacy` variable is set.

For each Header Field, Bob's MUA passes its name and value through `hcp_baseline`. This returns the same value for every Header Field, except that:

`hcp_baseline("Subject", "Handling the Jones contract")` yields `"[...]"`.

D.1.2.1. Cryptographic Payload

The Cryptographic Payload that will be signed and then encrypted is very similar to the unprotected message in Appendix D.1.1. Note the addition of:

- the `hp="cipher"` parameter for the `Content-Type`
- the appropriate `HP-Outer` Header Field for `Subject`
- the `hp-legacy-display="1"` parameter for the `Content-Type`
- the Legacy Display Element (the simple pseudo-header and its trailing newline) in the Main Body Part

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: Handling the Jones contract
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Type: text/plain; charset="us-ascii"; hp-legacy-display="1";
 hp="cipher"
MIME-Version: 1.0
HP-Outer: Date: Wed, 11 Jan 2023 16:08:43 -0500
HP-Outer: From: Bob <bob@example.net>
HP-Outer: To: Alice <alice@example.net>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <20230111T210843Z.1234@lhp.example>

Subject: Handling the Jones contract

Please review and approve or decline by Thursday, it's critical!

Thanks,
Bob

--
Bob Gonzalez
ACME, Inc.
```

D.1.2.2. Outer Header Section

The Cryptographic Payload from Appendix D.1.2.1 is then wrapped in the appropriate Cryptographic Layers. For this example using S/MIME, it is wrapped in an `application/pkcs7-mime; smime-type="signed-data"` layer, which is in turn wrapped in an `application/pkcs7-mime; smime-type="enveloped-data"` layer.

Then, an Outer Header Section is applied to the outer MIME object, which looks like this:

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: [...]
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
MIME-Version: 1.0
```

Note that the `Subject` Header Field has been obscured appropriately by `hcp_baseline`. The output of the CMS enveloping operation is base64 encoded and forms the Body of the message.

D.2. Composing a Reply

Next, we consider a typical MUA reply interface, where we see Alice replying to Bob's message from Appendix D.1.

When Alice clicks "Reply" to Bob's signed-and-encrypted message with Header Protection, she might see something like this:

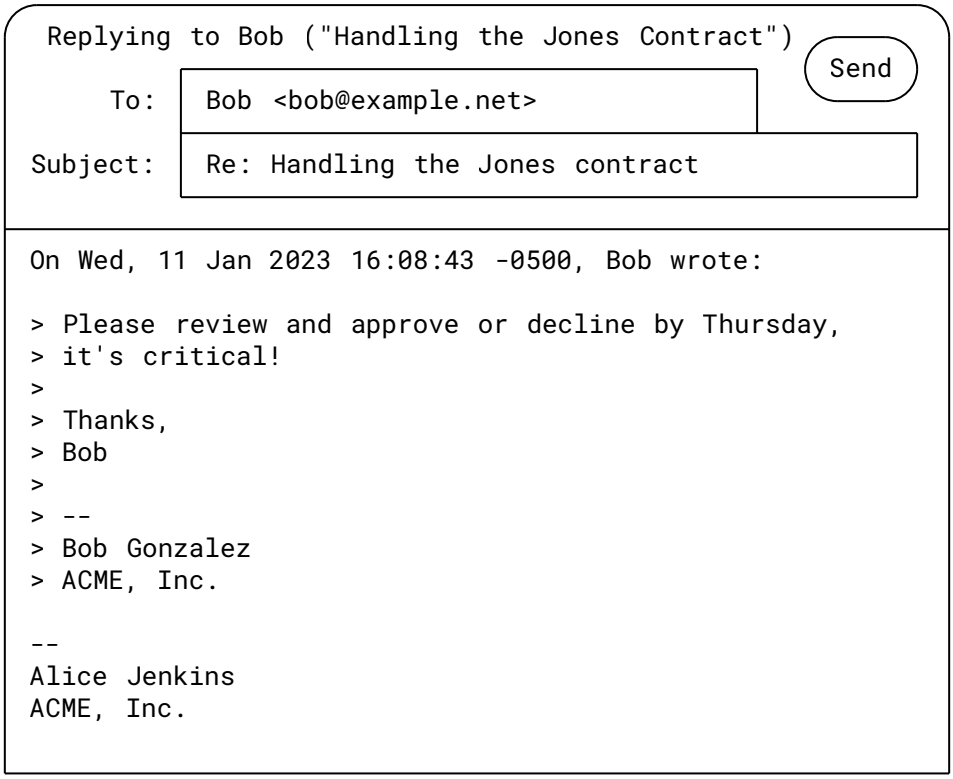

Figure 2: Example Message Reply Interface (Unedited)

Note that because Alice's MUA is aware of Header Protection, it knows what the correct `Subject` Header Field is, even though it was obscured. It also knows to avoid including the Legacy Display Element in the quoted/attributed text that it includes in the draft reply.

Once Alice has edited the reply message, it might look something like this:

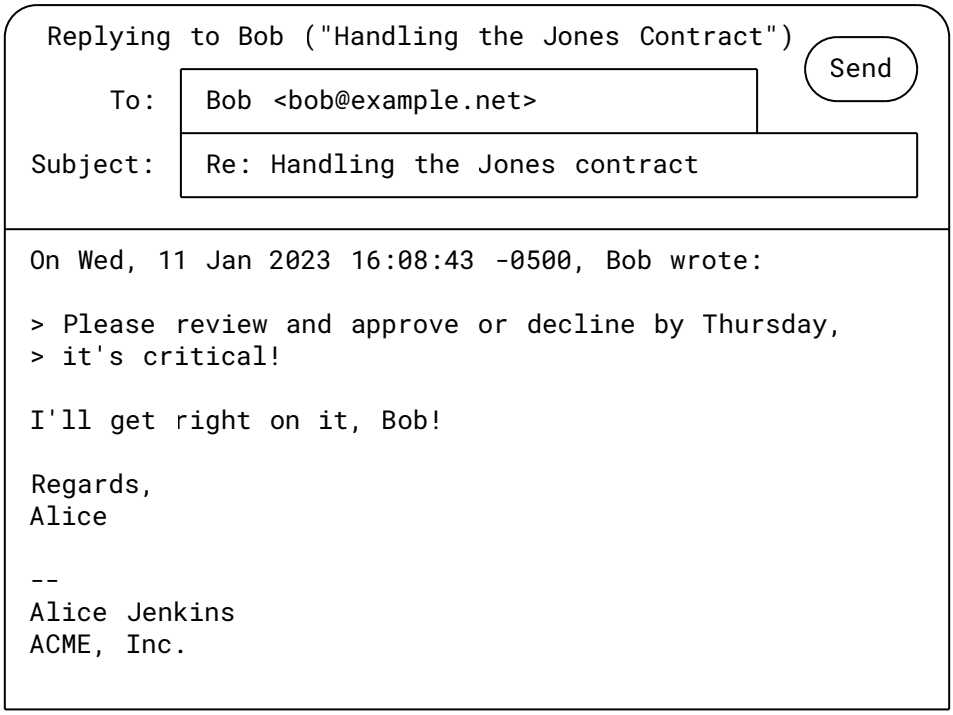

Figure 3: Example Message Reply Interface (Edited)

When Alice clicks "Send", the MUA generates values for the `Message-ID`, `From`, and `Date` Header Fields, populates the `In-Reply-To` and `References` Header Fields, and also converts the reply content into the appropriate format.

D.2.1. Unprotected Message

The resulting message would look something like this if it were to be sent without any cryptographic protections:

```
Date: Wed, 11 Jan 2023 16:48:22 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Re: Handling the Jones contract
Message-ID: <20230111T214822Z.5678@lhp.example>
In-Reply-To: <20230111T210843Z.1234@lhp.example>
References: <20230111T210843Z.1234@lhp.example>
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0

On Wed, 11 Jan 2023 16:08:43 -0500, Bob wrote:

> Please review and approve or decline by Thursday,
> it's critical!

I'll get right on it, Bob!

Regards,
Alice

--
Alice Jenkins
ACME, Inc.
```

Of course, this would leak not only the contents of Alice's message but also the contents of Bob's initial message, as well as the `Subject` Header Field! So Alice's MUA won't do that; it is going to create a signed-and-encrypted message to submit to the network.

D.2.2. Encrypted with `hcp_no_confidentiality` and Legacy Display

This example assumes that Alice's MUA uses `hcp_no_confidentiality`, not `hcp_baseline`. That is, by default, it does not obscure or remove any Header Fields, even when encrypting.

However, it follows the guidance in Section 6.1 and will make use of the `HP-Outer` field in the Cryptographic Payload of Bob's original message (Appendix D.1.2.1) to determine what to obscure.

When crafting the Cryptographic Payload, its baseline HCP (`hcp_no_confidentiality`) leaves each field untouched. To uphold the confidentiality of the sender's values when replying, the MUA executes the following steps (for brevity, only `Subject` and `Message-ID`/`In-Reply-To` are shown):

- Extract the referenced Header Fields (see Section 4.2):
  - `refouter` contains:
    - `Date: Wed, 11 Jan 2023 16:08:43 -0500`
    - `From: Bob <bob@example.net>`
    - `To: Alice <alice@example.net>`
    - `Subject: [...]`
    - `Message-ID: <20230111T210843Z.1234@lhp.example>`

- `refprotected` contains:
  - `Date: Wed, 11 Jan 2023 16:08:43 -0500`
  - `From: Bob <bob@example.net>`
  - `To: Alice <alice@example.net>`
  - `Subject: Handling the Jones contract`
  - `Message-ID: <20230111T210843Z.1234@lhp.example>`

- Apply the response function:
  - `respond(refouter)` contains:
    - `From: Alice <alice@example.net>`
    - `To: Bob <bob@example.net>`
    - `Subject: Re: [...]`
    - `In-Reply-To: <20230111T210843Z.1234@lhp.example>`
    - `References: <20230111T210843Z.1234@lhp.example>`
  - `respond(refprotected)` contains:
    - `From: Alice <alice@example.net>`
    - `To: Bob <bob@example.net>`
    - `Subject: Re: Handling the Jones contract`
    - `In-Reply-To: <20230111T210843Z.1234@lhp.example>`
    - `References: <20230111T210843Z.1234@lhp.example>`

- Compute the ephemeral `response_hcp` (see Section 6.1):
  - Note that all Header Fields except `Subject` are the same.
  - `confmap` contains only `("Subject", "Re: Handling the Jones contract") -> "Re: [...]"`

Thus, all Header Fields that were `signed` are passed through untouched. The reply's `Subject` is obscured as `Subject: Re: [...]` if and only if the user does not edit the Subject line from that initially proposed by the MUA's reply interface. If the user edits the Subject line, e.g., to `Subject: Re: Handling the Jones contract ASAP`, the `response_hcp` will *not* obscure it and instead pass it through in the clear.

For stronger header confidentiality, the replying MUA should use a reasonable HCP (not `hcp_no_confidentiality`). Also recall that the local HCP is applied first and that `response_hcp` is only applied to what is left unchanged by the local HCP.

D.2.2.1. Cryptographic Payload

Consequently, the Cryptographic Payload for Alice's reply looks like this:

```
Date: Wed, 11 Jan 2023 16:48:22 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Re: Handling the Jones contract
Message-ID: <20230111T214822Z.5678@lhp.example>
In-Reply-To: <20230111T210843Z.1234@lhp.example>
References: <20230111T210843Z.1234@lhp.example>
Content-Type: text/plain; charset="us-ascii"; hp-legacy-display="1";
 hp="cipher"
MIME-Version: 1.0
HP-Outer: Date: Wed, 11 Jan 2023 16:48:22 -0500
HP-Outer: From: Alice <alice@example.net>
HP-Outer: To: Bob <bob@example.net>
HP-Outer: Subject: Re: [...]
HP-Outer: Message-ID: <20230111T214822Z.5678@lhp.example>
HP-Outer: In-Reply-To: <20230111T210843Z.1234@lhp.example>
HP-Outer: References: <20230111T210843Z.1234@lhp.example>

Subject: Re: Handling the Jones contract

On Wed, 11 Jan 2023 16:08:43 -0500, Bob wrote:

> Please review and approve or decline by Thursday,
> it's critical!

I'll get right on it, Bob!

Regards,
Alice

--
Alice Jenkins
ACME, Inc.
```

Note the following features:

- the `hp="cipher"` parameter to `Content-Type`
- the appropriate `HP-Outer` Header Field for `Subject`
- the `hp-legacy-display="1"` parameter for the `Content-Type`
- the Legacy Display Element (the simple pseudo-header and its trailing newline) in the Main Body Part

D.2.2.2. Outer Header Section

The Cryptographic Payload from Appendix D.2.2.1 is then wrapped in the appropriate Cryptographic Layers. For this example using S/MIME, it is wrapped in an `application/pkcs7-mime; smime-type="signed-data"` layer, which is in turn wrapped in an `application/pkcs7-mime; smime-type="enveloped-data"` layer.

Then, an Outer Header Section is applied to the outer MIME object, which looks like this:

```
Date: Wed, 11 Jan 2023 16:48:22 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Re: [...]
Message-ID: <20230111T214822Z.5678@lhp.example>
In-Reply-To: <20230111T210843Z.1234@lhp.example>
References: <20230111T210843Z.1234@lhp.example>
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
MIME-Version: 1.0
```

Note that the `Subject` Header Field has been obscured appropriately even though `hcp_no_confidentiality` would not have touched it by default. The output of the CMS enveloping operation is base64 encoded and forms the Body of the message.

Appendix E. Rendering Examples

This section offers example Cryptographic Payloads (the content within the Cryptographic Envelope) that contain Legacy Display Elements.

E.1. Example text/plain Cryptographic Payload with Legacy Display Elements

Here is a simple one-part Cryptographic Payload (Header Section and Body) of a message that includes Legacy Display Elements:

```
Date: Fri, 21 Jan 2022 20:40:48 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Dinner plans
Message-ID: <text-plain-legacy-display@lhp.example>
MIME-Version: 1.0
Content-Type: text/plain; charset="us-ascii"; hp-legacy-display="1";
 hp="cipher"
HP-Outer: Date: Fri, 21 Jan 2022 20:40:48 -0500
HP-Outer: From: Alice <alice@example.net>
HP-Outer: To: Bob <bob@example.net>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <text-plain-legacy-display@lhp.example>

Subject: Dinner plans

Let's meet at Rama's Roti Shop at 8pm and go to the park
from there.
```

A compatible MUA will recognize the `hp-legacy-display="1"` parameter and render the Body of the message as:

```
Let's meet at Rama's Roti Shop at 8pm and go to the park
from there.
```

A legacy decryption-capable MUA that is unaware of this mechanism will ignore the `hp-legacy-display="1"` parameter and instead render the Body including the Legacy Display Elements:

```
Subject: Dinner plans

Let's meet at Rama's Roti Shop at 8pm and go to the park
from there.
```

E.2. Example text/html Cryptographic Payload with Legacy Display Elements

Here is a modern one-part Cryptographic Payload (Header Section and Body) of a message that includes Legacy Display Elements:

```
Date: Fri, 21 Jan 2022 20:40:48 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Dinner plans
Message-ID: <text-html-legacy-display@lhp.example>
MIME-Version: 1.0
Content-Type: text/html; charset="us-ascii"; hp-legacy-display="1";
 hp="cipher"
HP-Outer: Date: Fri, 21 Jan 2022 20:40:48 -0500
HP-Outer: From: Alice <alice@example.net>
HP-Outer: To: Bob <bob@example.net>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <text-html-legacy-display@lhp.example>

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>Subject: Dinner plans</pre>
</div>
<p>
Let's meet at Rama's Roti Shop at 8pm and go to the park
from there.
</p>
</body>
</html>
```

A compatible MUA will recognize the `hp-legacy-display="1"` parameter and mask out the Legacy Display `div`, rendering the Body of the message as a simple paragraph:

```
Let's meet at Rama's Roti Shop at 8pm and go to the park
from there.
```

A legacy decryption-capable MUA that is unaware of this mechanism will ignore the `hp-legacy-display="1"` parameter and instead render the Body including the Legacy Display Elements:

```
Subject: Dinner plans

Let's meet at Rama's Roti Shop at 8pm and go to the park
from there.
```

Appendix F. Other Header Protection Schemes

Other Header Protection schemes have been proposed in the past. However, those typically have drawbacks such as sparse implementation, known problems with legacy interoperability (in particular with rendering), lack of clear signaling of sender intent, and/or incomplete cryptographic protections. This section lists such schemes known at the time of the publication of this document out of historical interest.

F.1. Original RFC 8551 Header Protection

S/MIME [RFC8551] (as well as its predecessors [RFC5751] and [RFC3851]) defined a form of cryptographic Header Protection that has never reached wide adoption and has significant drawbacks compared to the mechanism in this document. See Section 1.1.1 for more discussion of the differences and Section 4.10 for guidance on how to handle such a message.

F.2. Pretty Easy Privacy (pEp)

The pretty Easy privacy (pEp) [PEP-GENERAL] project specifies two different MIME schemes that include Header Protection for Signed-and-Encrypted email messages in [PEP-EMAIL]: One scheme -- referred as pEp Email Format 1 (PEF-1) -- is generated towards MUAs not known to be pEp-capable, while the other scheme -- referred as PEF-2 -- is used between MUAs discovered to be compatible with pEp. Signed-only messages are not recommended in pEp.

Although the PEF-2 scheme is only meant to be used between PEF-2-compatible MUAs, PEF-2 messages may end up at MUAs unaware of PEF-2 (in which case, they typically render badly). This is due to signaling mechanism limitations.

As the PEF-2 scheme is an enhanced variant of the RFC8551HP scheme (with an additional MIME Layer), it is similar to the RFC8551HP scheme (see Section 4.10). The basic PEF-2 MIME structure looks as follows:

```
A └─┬ multipart/encrypted [Outer Message]
B   ├── application/pgp-encrypted
C   └── application/octet-stream inline [Cryptographic Payload]
D    ↧ (decrypts to)
E    └─┬ multipart/mixed
F      ├── text/plain
G      ├─┬ message/rfc822
H      │ └── [Inner Message]
I      └── application/pgp-keys
```

The MIME structure at part `H` contains the Inner Message to be rendered to the user.

It is possible for a normal MUA to accidentally produce a message that happens to have the same MIME structure as used for PEF-2 messages. Therefore, a PEF-2 message cannot be identified by the MIME structure alone.

The lack of a mechanism comparable to `HP-Outer` (see Section 2.2) makes it impossible for the recipient of a PEF-2 message to safely determine which Header Fields are confidential or not while forwarding or replying to a message (see Section 6).

Note: As this document is not normative for PEF-2 messages, it does not provide any guidance for handling them. Please see [PEP-EMAIL] for more guidance.

F.3. "draft-autocrypt" Protected Headers

[PROTECTED-HEADERS] describes a scheme similar to the Header Protection scheme specified in this document. However, instead of adding Legacy Display Elements to existing MIME parts (see Section 5.2.2), [PROTECTED-HEADERS] suggests injecting a new MIME element "Legacy Display Part", thus modifying the MIME structure of the Cryptographic Payload. These modified Cryptographic Payloads cause significant rendering problems on some common Legacy MUAs.

The lack of a mechanism comparable to `hp="cipher"` and `hp="clear"` (see Section 2.1.1) means the recipient of an encrypted message as described in [PROTECTED-HEADERS] cannot be cryptographically certain whether the sender intended for the message to be confidential or not. The lack of a mechanism comparable to `HP-Outer` (see Section 2.2) makes it impossible for the recipient of an encrypted message as described in [PROTECTED-HEADERS] to safely determine which Header Fields are confidential or not while forwarding or replying to a message (see Section 6).

Acknowledgements

Alexander Krotov identified the risk of `From` address spoofing (see Section 10.1) and helped provide guidance to MUAs.

Thore Göbel identified significant gaps in earlier draft versions of this document and proposed concrete, substantial improvements. Thanks to his contributions, the document is clearer, and the protocols described herein are more useful.

Additionally, the authors would like to thank the following people who have provided helpful comments and suggestions for this document: Berna Alp, Bernhard E. Reiter, Bron Gondwana, Carl Wallace, Claudio Luck, Daniel Huigens, David Wilson, Éric Vyncke, Hernani Marques, juga, Kelly Bristol, Krista Bennett, Lars Rohwedder, Michael StJohns, Nicolas Lidzborski, Orie Steele, Paul Wouters, Peter Yee, Phillip Tao, Robert Williams, Rohan Mahy, Roman Danyliw, Russ Housley, Sofia Balicka, Steve Kille, Volker Birk, Warren Kumari, and Wei Chuang.

Authors' Addresses

Daniel Kahn Gillmor
American Civil Liberties Union
125 Broad St.
New York, NY 10004
United States of America
Email: dkg@fifthhorseman.net

Bernie Hoeneisen
pEp Project
Oberer Graben 4
CH- 8400 Winterthur
Switzerland
Email: bernie@ietf.hoeneisen.ch
URI: https://pep-project.org/

Alexey Melnikov
Isode Ltd
14 Castle Mews
Hampton, Middlesex
TW12 2NP
United Kingdom
Email: alexey.melnikov@isode.com