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

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

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	8
1.1. Update to RFC 8551	8
1.1.1. Problems with RFC 8551 Header Protection	8
1.2. Risks of Header Protection for Legacy MUA Recipients	9
1.3. Motivation	10
1.3.1. Backward Compatibility	10
1.3.2. Deliverability	11
1.4. Other Protocols to Protect Email Header Fields	11
1.5. Applicability to PGP/MIME	12
1.6. Requirements Language	12
1.7. Terms	12
1.8. Document Scope	13
1.8.1. In Scope	14
1.8.2. Out of Scope	14
1.9. Example	14
2. Internet Message Format Extensions	16
2.1. Content-Type Parameters	16
2.1.1. Content-Type Parameter: hp	17
2.1.2. Content-Type Parameter: hp-legacy-display	17

2.2. HP-Outer Header Field	18
2.2.1. HP-Outer Header Field Definition	19
3. Header Confidentiality Policy	19
3.1. HCP Definition	20
3.1.1. HCP Avoids Changing addr-spec of From Header Field	21
3.2. Initial Registered HCPs	21
3.2.1. Baseline Header Confidentiality Policy	21
3.2.2. Shy Header Confidentiality Policy	22
3.2.3. No Header Confidentiality Policy	22
3.3. Default Header Confidentiality Policy	22
3.4. HCP Evolution	23
3.4.1. Offering More Ambitious Header Confidentiality	23
3.4.2. Expert Guidance for Registering Header Confidentiality Policies	23
4. Receiving Guidance	24
4.1. Identifying That a Message Has Header Protection	24
4.2. Extracting Protected and Unprotected ("Outer") Header Fields	25
4.2.1. HeaderSetsFromMessage	25
4.3. Updating the Cryptographic Summary	25
4.3.1. HeaderFieldProtection	26
4.4. Handling Mismatch of From Header Fields	27
4.4.1. Definitions	27
4.4.2. Warning for From Header Field Mismatch	28
4.4.3. From Header Field Rendering	28
4.4.4. Handling the Protected From Header Field When Responding	28
4.4.5. Matching addr-specs	29
4.5. Rendering a Message with Header Protection	29
4.5.1. Example Signed-Only Message	29
4.5.2. Example Signed-and-Encrypted Message	30
4.5.3. Do Not Render Legacy Display Elements	31

4.6. Implicitly Rendered Header Fields	32
4.7. Handling Undecryptable Messages	32
4.8. Guidance for Automated Message Handling	33
4.8.1. Only Interpret Protected Header Fields	33
4.8.2. Ignore Legacy Display Elements	34
4.9. Affordances for Debugging and Troubleshooting	34
4.10. Handling RFC8551HP Messages (Backward Compatibility)	34
4.10.1. Identifying an RFC8551HP Message	35
4.10.2. Rendering or Responding to an RFC8551HP Message	35
4.11. Rendering Other Schemes	36
5. Sending Guidance	36
5.1. Composing a Cryptographically Protected Message Without Header Protection	36
5.1.1. ComposeNoHeaderProtection	37
5.2. Composing a Message with Header Protection	37
5.2.1. Compose	38
5.2.2. Adding a Legacy Display Element to a text/plain Part	39
5.2.3. Adding a Legacy Display Element to a text/html Part	40
5.2.4. Only Add a Legacy Display Element to Main Body Parts	41
5.2.5. Do Not Add a Legacy Display Element to Other Content-Types	42
6. Replying and Forwarding Guidance	42
6.1. Avoid Leaking Encrypted Header Fields in Replies and Forwards	42
6.1.1. ReferenceHCP	43
6.2. Avoid Misdirected Replies	44
7. Unprotected Header Fields Added in Transit	45
7.1. Mailing List Header Fields: List-* and Archived-At	45
8. Email Ecosystem Evolution	46
8.1. Dropping Legacy Display Elements	46
8.2. More Ambitious Default HCP	46
8.3. Deprecation of Messages Without Header Protection	47

9. Usability Considerations	47
9.1. Mixed Protections Within a Message Are Hard to Understand	48
9.2. Users Should Not Have to Choose a Header Confidentiality Policy	48
10. Security Considerations	49
10.1. From Address Spoofing	49
10.1.1. From Rendering Reasoning	50
10.2. Avoid Cryptographic Summary Confusion from the hp Parameter	52
10.3. Caution About Composing with Legacy Display Elements	52
10.4. Plaintext Attacks	53
11. Privacy Considerations	53
11.1. Leaks When Replying	53
11.2. Encrypted Header Fields Are Not Always Private	54
11.2.1. Encrypted Header Fields Can Leak Unwanted Information to the Recipient	54
11.2.2. Encrypted Header Fields Can Be Inferred from External or Internal Metadata	55
11.2.3. Encrypted Header Fields May Not Be Fully Masked by HCP	55
11.3. A Naive Recipient May Overestimate the Cryptographic Status of a Header Field in an Encrypted Message	55
11.4. Privacy and Deliverability Risks with Bcc and Encrypted Messages	56
12. IANA Considerations	56
12.1. Registration of the HP-Outer Header Field	56
12.2. Reference Update for the Content-Type Header Field	57
12.3. New Mail Header Confidentiality Policies Registry	57
13. References	58
13.1. Normative References	58
13.2. Informative References	59
Appendix A. Table of Pseudocode Listings	61
Appendix B. Possible Problems with Legacy MUAs	62
B.1. Problems Viewing Messages in a List View	62
B.2. Problems When Rendering a Message	62
B.3. Problems When Replying to a Message	63

Appendix C. Test Vectors	63
C.1. Baseline Messages	64
C.1.1. No Cryptographic Protections over a Simple Message	64
C.1.2. S/MIME Signed-Only signedData over a Simple Message, No Header Protection	64
C.1.3. S/MIME Signed-Only multipart/signed over a Simple Message, No Header Protection	66
C.1.4. S/MIME Signed-and-Encrypted over a Simple Message, No Header Protection	68
C.1.5. No Cryptographic Protections over a Complex Message	72
C.1.6. S/MIME Signed-Only signedData over a Complex Message, No Header Protection	73
C.1.7. S/MIME Signed-Only multipart/signed over a Complex Message, No Header Protection	76
C.1.8. S/MIME Signed-and-Encrypted over a Complex Message, No Header Protection	79
C.2. Signed-Only Messages	85
C.2.1. S/MIME Signed-Only signedData over a Simple Message, Header Protection	85
C.2.2. S/MIME Signed-Only multipart/signed over a Simple Message, Header Protection	87
C.2.3. S/MIME Signed-Only signedData over a Complex Message, Header Protection	89
C.2.4. S/MIME Signed-Only multipart/signed over a Complex Message, Header Protection	92
C.2.5. S/MIME Signed-Only signedData over a Complex Message, Legacy RFC 8551 Header Protection	95
C.2.6. S/MIME Signed-Only multipart/signed over a Complex Message, Legacy RFC 8551 Header Protection	98
C.3. Signed-and-Encrypted Messages	101
C.3.1. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_baseline	101
C.3.2. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display)	106
C.3.3. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_shy	111
C.3.4. S/MIME Signed-and-Encrypted over a Simple Message, Header Protection with hcp_shy (+ Legacy Display)	116
C.3.5. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline	121
C.3.6. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_baseline (+ Legacy Display)	126

C.3.7. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy	132
C.3.8. S/MIME Signed-and-Encrypted Reply over a Simple Message, Header Protection with hcp_shy (+ Legacy Display)	137
C.3.9. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_baseline	142
C.3.10. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display)	149
C.3.11. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_shy	156
C.3.12. S/MIME Signed-and-Encrypted over a Complex Message, Header Protection with hcp_shy (+ Legacy Display)	162
C.3.13. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline	170
C.3.14. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_baseline (+ Legacy Display)	177
C.3.15. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy	184
C.3.16. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with hcp_shy (+ Legacy Display)	191
C.3.17. S/MIME Signed-and-Encrypted over a Complex Message, Legacy RFC 8551 Header Protection with hcp_baseline	199
Appendix D. Composition Examples	205
D.1. New Message Composition	205
D.1.1. Unprotected Message	206
D.1.2. Encrypted with hcp_baseline and Legacy Display	207
D.2. Composing a Reply	208
D.2.1. Unprotected Message	210
D.2.2. Encrypted with hcp_no_confidentiality and Legacy Display	211
Appendix E. Rendering Examples	214
E.1. Example text/plain Cryptographic Payload with Legacy Display Elements	214
E.2. Example text/html Cryptographic Payload with Legacy Display Elements	215
Appendix F. Other Header Protection Schemes	216
F.1. Original RFC 8551 Header Protection	216

F.2. Pretty Easy Privacy (pEp)	216
F.3. "draft-autocrypt" Protected Headers	217
Acknowledgements	217
Authors' Addresses	218

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]
   │
   ├── text/plain
   └── 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`) \rightarrow `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 `hcb_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

Header Confidentiality Policy Name	Description	Recommended	Reference
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

Method Name	Description	Reference
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.cmrq.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

MIILGQYJKoZIhvcNAQcCoIILCjCCCwYCAQEExDTALBg1ghkgBZQMEAgEwggFCBgkq
hkiG9w0BBWGgggEzBIIbL01JTUUtVmVyc2l1b2JogMS4wDQpDb250ZW50LVR5cGU6
IHRleHh0cGxhaW47IGNoYXJzZXQ9InV0Zi04Igc0KQ29udGVudC1UcmFuc2Zlci1F
bmNvZGluZz0gN2JpdA0KDQpUaGlzIGlzIHRoZQ0Kc21pbWUtb251LXBhcnQNCm1l
c3NhZ2UuDQoNClRoXMaXMGYYSBzaWduZWQtb25seSBTL01JTUUGbWVzc2FnZSB2
aWEgUEtDUyM3IHNPZ251ZERhdGEuICBUaGUNcNBheWxvYWQgaXMGYSB0ZXh0L3Bs
YWluIG1lc3NhZ2UuIEI0IHVzZXMGbm8gSGVhZGVyIFByb3RlY3Rpb24uDQoNCi0t
IA0KQWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUNCqCCB6YwggPPMIICt6ADAgEC
AhMPLSW9ETmXSs5CVIEh7j00Boq0MA0GCSqGSIb3DQEBAQUAMFUDALBgNVBAoT
BE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLWYDVQDEYhTYW1wbGUgTEFNUFMg
U1NBIEln1cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIw
NTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBX
RzEXBBUGA1UEAxMQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCAlSn6i8Gi44/oAVAn5Gnck4PHHNjrSfWUnne1N41KImVaTC3D
9zfCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs
165ernT905NLFf1HUjURca3ynqEBBv4DmhnZp8eDhv3t6dXyCjNHT82S6DgCreZu
TtMc1zy++MxQlqdn9WZLh0A0peNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCq1LqhBwDH
dZ5qDTII2PVX1X3K7/c0NxbvBbaU1/k1swdszUtjhflYFZ80RuQ3qFC6vL/PGeWy
6SCf58duq/A0EksCAW1b+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/
BAIwADAXBgNVHSAEEDAOMAawGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VA
c21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMC
BSAwHQYDVR00BBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEw
jnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQCBsXignLEynBak
DKU68ro0RsyXWAPkfxGQLgy7GrW7SrZeBc5IEcjoN9f/gs0x/Ht9Ii6zyBVjdao
x644DsiloQEP4YMS7y4q94RFFdmdzEbDLyX9sfUhdvTxDN00oHz53PYDBh4zE4Na
r2inC0D+VM6RGDy66K9l+D+b18Wj9CyGUc1ppMNURexTg+z3web/eD0du+F2Mvt1
uLihne0Bp1GUTkr0mJBol6dSYa18Hw8/ANHPyEx156BJABb744gqoeuD9YSHjKK
49+qYC9faFmQ+mK80l1h1M9RdNI7srjn0LKpuob6w06jaRzWdNeXz1Ec2tUpAr4vR
hZjVD6FYMIIDzzCCAREgAwIBAgITN0EFee11f0Kpolw69Phqzpq1zANBgkqhkiG
9w0BAQ0FAADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBXRzExMC8G
A1UEAxMoU2FtcGx1IEExBTvBTIFJTQSB0ZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAG
Fw0xOTExMjAwNjU0MTA8yMDUyMDkyNzA2NTQxOFowOzENMAsgA1UEChMESUVU
RjERMA8GA1UECXMITEFNUFMgV0cxZzAVBgNVBAMTDkFsaWNlIEExvdmVsYWNlMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTk
fCv4TfA/pd0/KLpZbJOAER0sI7Aja07B1GuMUFJeStulamNfCwDcDkY63PQWl+DI
Ls7GxVwXurhYdZlaV5hcUqVackPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TC
N012DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtwS1q7
ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTM
SiPR+peCrhJZwLSebwWXLJe3VMvbvQj0BMPeYlaJBUIKk01zQ1Pq90njlsJL0wID

```

```
AQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATAB
MB4GA1UdEQQXMBWBE2FsaWNlQHNTaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYB
BQUHAWQwDgYDVR0PAQH/BAQDAgBAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDT
IGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0B
AQ0FAAOCAQEAc4miNqf0qaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3Bj
J0d64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIj
So27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahixRn/C9
cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIAe6aCHHBh0iPU7IPkazgPYgkLD59fk4P
GHnYxs1Fhd06zZk9E8zwlc1ALgZa/iSbczsqckN3qGehD2s16jMhwFXLJtBiN+u
CDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMASGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFNgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydGlmawNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJc0vT4as6a
qdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCsGSIb3DQEHATAcBgkq
hkiG9w0BCCQUxDxcNMjEwMTUwMTAyWjAvBgkqhkiG9w0BCCQxIgQg+APzZJl4
pcksiF0YwAUqexbFmtnUdg8eCFIkLg8wDQYJKoZIhvcNAQEBBQAEggEARLZH
lu1QA7h4AzGUznSRv1TB3w2u4oXQBgxTTaUFXvezPsEacndc16K4ESz8IpjsLEqC
lhFU6haOKz30Znab6A8sCqozqAoCpJI35L3D0XwlqucQqRDMQoNDZf1AZw1/2rvhl
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"

MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMA5GA1UEChMESUVURjERMA8GA1UECzMITEFNUFNgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQUU1QUYBSU0EGQ2VydG1maWNhdGlvbiBBdXRob3Jp
dHkwIBcNMTEwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDALBgNVBAoT
BE1FVEYxETAPBgNVBAStCExBTVBTIFdHMRcwFQYDVQQDEw5BbGJjZSBMb3Z1bGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBABJqVKfQLwaLjj+gBUCfk
acKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID1B/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3i0x7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0a
Gdmnx40G/e3p1fIKM0dPzZLo0AJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC
N5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbG1jZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj
80e0r83zdw8wHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSH1NhpNHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCsTKcFqQMPTryujRGzJdYA+R9eBAuDLsatbtKt14F
zkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7PFB5v94M5274XYxW2W4uKGd7QGnUZROsVSykGiWdp1JhqXwfDz8
A0enITGXnoEkAFvviCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu0fQs
qm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBAQUAMFUDALBgNVBAoTBE1FVEYx
```

```

ETAPBgNVBAsTCExBTVBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUFMgU1NBIEN1
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLewhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWPK2af0+StijSNOR8K/hN8D+1078oullsk4ASvSwjsCNo7sHU
a4xQU15J06VqY18LANw0Rjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzyms02kaYWTut3
SryCqeHEFbZfKb4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfi0ucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9C0gE
ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEEDA0MAwGCMGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYD
VR00BBYEFV2zLItHQYSHJeuKWqQENMGZmZzMB8GA1UdIwQYMBaAFJEwjnWHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjD/4Kkk0H
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZL
RAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEnt1sRxlcvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JCKzP0Qhp
7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
0KypyQ3eoZ6EPazXqMyHAVcsM0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCafwCAQEwBDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLewhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGx1IExBTVBTIFJTSBDZXXJ0aWZpY2F0aW9uIEF1dGhv
cm10eQITN0EFee11f0Kpolw69Phqzpp1zALBglghkgBZQMEAgGaTAYBgkqhkiG
9w0BCQMxwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTBEPFw0yMTAyMjAxNTAyMDJa
MC8GCSqGSIb3DQEJBTBDEiBCAokSzA71kmv0yy0h+lr02jw3pvGhvgRnv/zTDC9IxD
UzANBgkqhkiG9w0BAQEFAASCAQBWLC6/VCYFv6ZiQR6JYBbLWiQJyAmNFrRhAbfi
w5bPndhDbJNSv3DXoUfCKd87pvD5Qr1PsH4WXDZ/iy95h3dD7k6oIIFXhPBtYYW7
Np+vrrVtS0sDKlr03+ebMBY6J0rEtNf5ZXCKQULTmvmmuKcg4S+5piNqhTnnE0en
IvICii8NgjP3VVPZmNpFmxwmztGWd04omYHbY4JY9C7yvuQ6SNEQm47bxnSIS5yH
sowWnDYqs2cMDLxZ7zy0cEyOpSy8oDfVde4Ty0ifqMT3VzSmlttDg1uDNE90ek3t
xJn9E+hE02sw0Mv1lLjNdrXviRsaMw33DxGbtoUSo2m0kpyb

```

--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

MIITXAYJKoZiHvcNAQcDoIITTTCCCE0kCAQAxggMQMIIBhAIBADBbMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIElcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIEh7j00
Boq0MA0GCSqSISb3DQEBAQUABIIBAFxh10X2qKJrCxxk4NBNVX/kprtr6yjMWM/1n
tepVdA0A/uf69sMzbyZhd8wF11eapv05Xp6+1Du0ZfqYgkbCJwD+ZtSL4MB7EBPM
ytXB42LTEC9f8Z/80L96/+nnDotKHxFSVZPXfmi+FKLLDlddH7bswV3GH/nozzY1
4wjesm/nvakHEv2CNJ2mh5XHq0ggNPDx5/20mxaU+x0biLPcGNzFob39ok+1rTbN
/9fIGDLKr1ENZQXW0vixcyAS/RB1Hw6WGby51EvV7F0bcdxsXkTI+vvHTcTGBPhi
54ShTTEocIj7mrXzHodVEy0pysuYCl2h0kqre9HSspAqw7s+/3wwggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EGQ2VydG1maWNhdG1vbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZiHvcNAQEBBQAEggEAbrrhe4bg9I4GbmhF5qn05kJXw
JTfpgB3iK+K+bIXh/gsZbLA0x2UR20HESrW2dqqjynuxZ+QE571NXQN7X7THo0aB
mhUPuBRPycw/orR2GR0KCYx4taATw9o2fK3Kss0+IAnNP10M7yUsgABZHT6BfvtC
qH7ZPBjaj73A9AyrxTNptJJHwueE3X5CPTODViasPRZrqIGB/WO/siuApdk0MPik
tp29bVqzQuD1tpDFb+aQyfggEnqGQn1ReZYhfBvub+AUr+001N0h57mob+eJwc0F
Snq9mljS3kgoXbh1DrV9S/seSdYZ7ieCiS3FYei8h7RsZTGCVMn/STxiq13X0DCC
EC4GCSqSISb3DQEhATAdbglghkgBZQMEAAIEEP3eQZI7xmdgaoaruEjNYuAghAA
mXWuV/HZ+MiCJTgt1RWzuHw8hnhLDxcY444IEB0M44fryhiuSkUKDdnvy6GDRiUF
ThwVs2iGhdCgvh/tJNaXmF9fa/Vi/aHq/oL3wJi+cS0qkeeq2kpGSMm82mNB1mgt
uhcwozIru+2n+L0xspYIUx0+dG59N1fB1a1RQJd7JmCUWF9AY/wVkGPKj5Vym+Vt
dRqGqcnJPM4Nq572bhxgLwD0CuoU+2rN5pdW1AT31odSdPtHoux3ysK+aMLcw3ch
mL+en9j/euq040Xr3Re0J/suSzHobI5I0bDtQwaEoXooz6aQIZrFE4TtZLCDzG7o
ZbMf3rkj1CIelKpbVhJRAjj4X+Mvkti0fxVV4K3GYAagHI5jp+4+MWz2yaQcAnRE
7SpHFxuFdmSYYYAq0yTgXkS9opoAwXPytKefqnnY62wAbug26ZCpSM03172cKopA
gkBqljwFE1+YeauN6206vZKu0hNuyQFbPe0+00qKeHw2bPM+PiKWdzAkQKz9N4C0
kFqz0gEHG5HnH8jx9PPuU57g8TmJccDFuUrZ4kZVcfWogH7gsNyW+A06BSu9Do/S
I7VxMwenuQLv1+W/tm+ZLqBLpksK0h81HVNvQ+4zEXx/jQBqM/Tv9BcetVdzGTIq
vCNn7KDLwLceNF7hgbNM4SfZZhg5hfV/xxeNpZx0tn86hHntN54FKym0/kXaFebr
W5yoXwvGHukCJJyI87NN7WIM12g5IHC829NIICAGIuZ/kxPb/A51WB8yr8748XXv
QcXKq70xTzkVgiACGDyS3ye+fZCncBZgfQ0jccipQU7jVYu7+UiUZDAvuQwae/RUD
CS0hdjwTBzMLIazVfbIaHPM5QKvB+MzbAKUMWza+XRpjLrDVdaSFR06V4r4SUMsi
AvKdd/1RFvSTEhtNj1Q0UKEa1DvnuRLvYsdjWLDf2TsBCjP4jdGKGG+PtfB4vcSU
NFJSJ5epaUIDxbFkgSolRF+1M8790Nd1gkhY6RbW3kXkA0T1CmKIYrN6poYxCSwU
Q+RzGurGDMQTGvfDgZr0bvde0haaNEdti/ci2EbcasYa3um7HCpt/bKDw5sivnh6
9P9E1WMvdAfeInppCZ08yRrkS116b9Jgk6ohJWftQMA20mpKGw6tRbb1H0tJ33JR
8ghApEJpSvtokGc46Nte1R6hBgxoaJCEbRpxJ9wrNp4EETj0/PbZDiDzNETWDZ4E
Bn74vJ2I3wCltkk16SmnEJadZovBlyqKYB6bmFvX9S00h0Bv8TZ4o//mY4nH57f0
5CmUM42ePRS0HMK9SrBjpouTIkw/tbDieZNB4tA09B/c3/s3qpZ2Bo0Bz7RVRI79
D2P8hnp+/7y74rqyUdRdQW6mFXjNojo1A+hsbXWqTfuMcSikbENC59pmhMDxdS4L
GxJCIVozmhbnjeEhIMqKwa0NtyLLG8uRLzdTF8g/I0I6UwCeFX1/d03tvLoEB/KA
D/n27IyDILDldYa1Em7I8jQmQghJ1IdMrUlr1n/mRB+sq12IDV1I95+r96IrFdmj
AWVMX+vbq6n/QNcaxfS5nL7ICgV9kQH09AtzJ4zXxLDj62nkIdoCRupF+I1HXL9G
OmgJJfj0uhgX067/2G0ct2JME1siW7/F6JHz1GAyeVSoPs2FAJKYMQvvrK6jbn3y
Huw3s9RS31co6D+nvxJHLvr/REVwiLk1xPqimC+2pmkUjRYyL/aXRV9pDuNJLTmu
XJxqwrYgwPw9mBXXaYLG08G+SSUfeBKvwuKa2kd0prB3cWwfIW1ZBgZvVGc7Uudz
QzxyMaDt8R7eVG6/CXUeG0MSWKbjzoZwkB/QCgZetV03YM7FqhEfvmg0tv1pS0c
nprxkkMurw1NGearPv+faBo09YSswF38o144A8hdpYIGc3LL4jj4wSPdS+1MVP84
nKWnZJ/asIS74bEH7TK3JK6tg0PEvh+GDM0DoXALsnH157oDi0GeN0kwcB7CeUT7
6zYaQT07Qcg0UyWME01Sc0i9zibws0ZKL3uNTwmF8p1Jv2TEvepZQil2/xbENTmf
H+47tdIPU1J0ePdJUGo6QTAaqSH5of0e/T/QENueeJ0JboPgbaV00qTF0VAMMhA
upadP8ROG6TalCP7X0gV9Yi60vd/WWWVTJPPLDf4+FJm7HmkzT515f0AuA+mYJUO
F+BPTUCKyeY9VypoXDV0VnTTpiB9jfy01PjBnZ/85BvfkT0eCW5rV7xeq7tgSJT
+L0KtFwDBql0Zt1hlvKe3SFHnsW9hdojLJz/sXw5FcFCxbxqfageVJ60uamEN0hB

```
j4Q2ZRvs1LXxpVME0ifG1CxpFAr2ZQsEormIu0zJeZjkDguwN1BInFKHFzvtSEJp
rP4hAqknbsV0qUdAFp9r1II2dYXI4xh3kV3ECvhvWft39PfVpGL97R92cTK9JCgq
p9IOJZv32FdhEsaHqQIRklw5xy96fTwbrho+LQSZIMUHTQ+hcqtcRX9cDPA+VZ0/
0vLgkF1R8rAWOTCxu3pHELjDq9nKKIzvX7tmyKapFgC38uotkvvKzpUzoA2xPoVH
ybrM09g9uJruzT/Oz02cDa9NWh2eYs1TWJvekeNftvakr6U9r7VYzUkmPCtfDDKC
oWSZHgwnU50Ps16UoTFaw1GuVn1C3cOREOUvFNbtV6R9Jdn3y0XJ0T4uZapFHPJf
naojAoE5iu3VXRMxVZB+4vZWfJoe4QNvc5t0kwUZVmE1nQWNkHuRyVnpfoLqaG1
1+5IpR6yIZDH1Wm75oc8hchG9PxrE002WUWqf+QSEdsT74cGTJVOZD16d4x/G5g4
97v1JaCSCgB/J9yrm4olsqgoYfWAbTcIBe0cUHnoNMAstKqH26jAf0Hz1l3V9D7M
zt3POMck+f3lLNUCqyNLcSASWc7jmB170/oF4vNP1EkGwWaz7yB1uTlS8sJCIViV
YYyZvj4du48h7lKaxeairWjcen+qeIS+Tn8VHqoJD6+QJinH5bXMKtxX00rvf69p
r0WjUctKikcJfJRbc6sQyMP6Y44+6/LyFmWILTav1WPoWLX5MYKOWP1s5GRneGWS
mZRztWt/CL/8DWjpPEG2siCSAs+1Bc1u/C5HkD1UVDjPmZTnvuFTHukaTKfteGz1
z0Bxuz9gQMMyAgU00My1+cGldHeR3HvIC9zUZ0qRj/d/20M8aQ+8NtVodadiMt29p
THvkr1oxuW6MVKXs0gZgdL72swDHTG3lKW1rrbufgjSr0UvSc8/MDgBPJVP2d6QX
P1IJvvBcr766DZ26j9/X0Is5cJjCN7Y0fIrS4RGU5aQR0w+d0ulK6v8q8reYzy0K
198CRs3prXRKRPIU0oM16oQdsV9T9LhfOnhWelil/HzetEltc0SiKgGKVYcArkZU
bzxsxUHF7q7qEzF2fVzWYBnM3qn8Shj3HH1PWYxW6uh5kI60+mV3Hs56KJjD9zsZ
ZIZTE/5agYXKplivRGScTUUGeDqrPPyEt0GRTmiQDLISHfW+nviZZcjC4XDxp04b
v6BH3EsSbXN4wJAXypDCY2kfL8wzqMh7qh/8Pk2AuodDtCJQJGsQPkgGwX21lSR2
4C1J1WJqDEaNHvmMf7B9nUu8unXYwwFe7FQN22CYZJQ0loj04T1Ukg7wRITeWwc6
xArdNOtn+XQuXfkxVEbiQRhiFt/47qAzoAjPRVr9r4P89Hz3wkTixirpAjTnKA5v
osv/7+28rRuYRYGu2yPwNeUPm00YHy3IeTVKcJ/Ucm03cXAe+Q+9ckmZ/MmxaxA1
zvJ2pH+INf3eBsQK77PxwsaGUFHqKWS1Wvk/FPsZkGEMX6QcD56sbGRbtsRRryXy
4L0U13Jc1P1jWmJhldGEqQohVfKYvHwdOdMaExZh/hhlpfxw1Cwh/d+uuP1Lko5
HTHxw1zQvRgzTlIdX78XIItFIYo+eMOB84xr8kAaXwHWpuZ06tymA59kD7LpvWVC6
r/OmqcnvAVDg/eiNh6Kru4BkIiTmtBs313ruZtSe8Hphvm80fYcelpfHs8Y1qrsS
EVohhfXl7073Td6jScN54FZU3dg0Efg97wyn+2DKeckNr5E/CgdD/FqhkH1IaE0
8wTbc9T/6XC+n27q/kQAMXzFnhn4Ec5E6uQb2MkCJEpW91eg9ZTDRYsZW1/r8yz+
QzbrSDSjVRvZ61FkGdh6m4i024ZtfcUV08AXo0hGKCh8fG/PKMcMzHvqQez07I8I
DfLTBhWBag9KcNljVFNBfYfL0e/hGnAZ6aDc6AQA0HdIZiAF49kEBhCLt0Tsa4UHT
npIjhKR6fi1RuiVnFkTqfCMgZawL1Z0kaQX2BdH1bsz2Q8wbu/DiNoyXdB/1k3Y2
9yLcVvGRCnyX0DjehyoLF/iJUzewsu8fz1TJfV/CCo07cDge2PdnDPVdE12nM+BH
Qo4scmT4cm1YYNGoecy9wGSgHE4fvhk0Szv0V2Fbt5HpJqsJvKH573A1CxR0pumw
r0ttrdRvke2vTw2nlw5iW1lPhcIpUQAEZfpxQ21hJfRvJiWDBvimAjVlHipTd0xA
oNZ383NE4SLWvNmjryk/uSvqoMXvof0Hatm67So0KMVDmBA5AMMq+9TBNBxaN1WW
FIuWMzmMWZYCMYm2Lmz2nU0dqVz95Y6rEsaMqQoft/UiteYyJdqawyMYKmwYzN
7yES4hRc3ee3JTyogrEtirg87pJ+RB7w0uI9FVjKKhjgVppGQVZAKcpeTRyrqjNU
oSycr2PbV3RPwzDRXX12PigHgX3suLehcc0WAMFvpQvgixXU/Ik5ScDcuLC4o/bs
juz0jy5END0jQldvC1bgfPfYUSZAvd/g0SYDc0xzC0Dm7dudNhuwSNDT7R39qh9t
eBZSOEI+1TKIxThFhHjKnWqxAJp9LJZbk7/L9QaKfQnDxQkPgwaFgskPTBflzgXd
4inGvpCfa03dHbhcb2EdF3jiIzHH84S0w5L1ZmXGgYUfNZHNkFf55VYzoTxNCIuA
Duc6jWMI+BXIXM1hJ0YYY90Y1jhT1vpv0VS6rj8zrr9y4xkH8dIdDvZh+OIqI5
jGmCCDFrCk03zHtLeYTWzQge5p2UPRRQWoxjKsjDHehxWdtHzfUsAAhx3f9USH3b
+nt2vLL2FuSjJMtqS9ACRFncGCQAPsdXjozm85raGnn8p4j9EbN2MFzQ1/mRA3XM
3mNpZ2/qT2GU0B2d49WLHJvesgKGBrIQBb0eM6//hH84BonFrSR6Sf0uUjTGiu2L
PXWkcsTORuAaaTzM330V0zQTAhBS27vhMr/kxMZSdTx/14phEaJ4zkYzzPb+T92G
CpiDpwEfU2akyZNa1Z9jTo28zq1gZENDRU6tYRsJrvPsDI3JN4702HZf80KFhd0/
ZgQ8eg079JS5iJASxu78DbC8Lo28DzDN7etUTCLKxBmz/IQFIHDDkxmzNfoF399J
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"
```

```
MIILPAYJKoZIhvcNAQcCoIILLTCCCykCAQExDTALBg1ghkgBZQMEAgEwggF1Bgkq
hkiG9w0BBWGgggFWBIIbUK1JTUUtVmVyc2lrbjogMS4wDQpDb250ZW50LVR5cGU6
IHRleHQCxGxhaW47IGNoYXJzZXQ9InV0Zi04Igt0KQ29udGVudC1UcmFuc2Z1ci1F
bmNvZGluZzZogN2JpdA0KDQpUaGlzIGlzIHRoZQ0Kc21pbWUtc2lbnbmVklWVuYw0K
bWVzc2FnZS4NCg0KVHpcyBpcyBhIHNpZ251ZC1hbmQtZW5jcn1wdGVkIFMvTU1N
RSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2ln
bmVkrGF0YS4gIFRoZSBwYXlsb2FkIGlzIGEgdGV4dC9wbGFpbG0KbWVzc2FnZS4g
SXQgdXNlcYBubyBIZWFKZXIgdGV4dGVjdGV4bWVzc2FnZS4gIHRoZQ0Kc21pbWUtc2lbnbmVklWVuYw0K
Y2VAc21pbWUuZXhhbXBsZQ0KoIIPjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU
h6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UE
CxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmawNh
dGlvbiBDbXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WHgPMjA1MjA5MjcWU0MTha
MDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAStCExBTVBTIFdHMRcwFQYDVQDEw5B
bG1jZSBMbzZlbnGfjZTCCASiDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqV
KfqLwLjJ+gBUCfkacKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID
lB/wlbdmadXPMrszyidmbuZmOpB5voVQfILYYy3i0x7Y0qzXr16udP07k0sV+UdS
NRFxrfKeoQEFXg0AGdmnx40G/e3p1fIKM0dPzLo0AJF5m500xzXPL74zFCWp2f1
ZkuE4A6141koaZXCN5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv
9w43GG8FtpSX+TWzB2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIB
aVv4wPxAf1iPsIVKarUCAwEAa0BrzCBrdAMBGNVHRMBAf8EAjAAMBcGA1UdIAQQ
MA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbG1jZUBzbWltZS5leGFtcGxl
MBMGA1UdJQOMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAWIFIDAdBgNVHQ4EFgQU
o1NB1UQ8gCkVfAEj80e0r83zdw8wHwYDVR0jBBBgwFoAukTC0fAcXDKfxCSH1Nhpn
HGh29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKcCsTKcFqQMPTryujRGzJdYA+R9
eBAuDLsatbtKt14FzkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLv
Lir3hEUVZ23MRsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLP5UzpEYPLro
r2X4P5uXxaP0LIZRzWmkw1RF7FOD7PFB5v94M5274XYxW2W4uKGd7QGnUZRSvSY
kGiWDp1JhqXwFdZ8A0enITGXnoEkAFvjjCqh64P1hIeMorj36pgL19oWZD6YrzS
WHUz1F00juyu0fQsqm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIIC
t6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUDTAL
BgNVBAoTBElFVEYxETAPBgNVBAStCExBTVBTIFdHMTewLwYDVQQDEyhTYW1wbGUg
TEFNUFMgU1NBIEIcnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQx
OFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEWRJRVRGMREwDwYDVQQLewhM
QU1QUyBXRzEXMBUGA1UEAxMQQWxpY2UgTG92ZWxhY2UwgGEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC09InoWDgWPK2af0+StijSNOR8K/hN8D+1078oulls
k4ASvSwjsCNo7sHUa4xQU15J06VqY18LANw0Rjrc9BaX4MguzsbFXBe6uFh1mVpX
mFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2
Gxzyms02kaYWTut3SryCqeHEfbZFKB4urMk4xrIJC3CzWruS2Q0FhbB1fkgKN5wX
VgkWFfi0ucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElNatJ7B
tZcs17dUy9u9C0gEyKriVokFQgqQ7XNDU+r3Se0Wwks7AgMBAAGjga8wgawwDAYD
VR0TAQH/BAIwADAXBgNVHSAEEDAOMAAGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYET
YWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8B
Af8EBAMCBsAwHQYDVR00BBYEFLv2zLiThQYSHJeuKWqQENMGZmZzMB8GA1UdIwQY
MBaAFJEwjnWHfyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2
p86poGkjD/4Kkk0HG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzh
W/JVdYn30UxfyrZ1RAZef7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEN
t1sRx1cVb7HVX524bKZa1oPTUNlm6QpivtqDIIdqGJdGf8L1zLfxBuo2zL3HR+M9C
Dr40pq2JCKzP0Qhp7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0T
zPCVzUAUblR+JJtz0KypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNTjh+Aq
J5QfH+0e7NSzNnEmMYICADCCAFwCAQEWBDBVMQ0wCwYDVQQKEWRJRVRGMREwDwYD
VQQLewhMQU1QUyBXRzEXMBUGA1UEAxMQU2FtcGx1IEExBTBTVBTIFJTQSBZDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69Phqzpq1zALBg1ghkgBZQME
AgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcCBMBwGCSqGSIb3DQEJBTEPFw0y
```

```
MTAyMjAxNTAzMDJaMC8GCSqGSIB3DQEBDEiBCCb47LkqJUmfPzt9bQAPoWpk+vy
9sGfzpOuEZf1V+goizANBgkqhkiG9w0BAQEFAASCAQCD+I+Tr7hDMV3VFvFGduS9
4ysR9dceBgPloLOH71fsoJUL508WspagFkqjkUGPipKfYVrssi8IHQM682HQqUk
jkB0UYx0hfEBVbsDvhYeJz0YfyLRQD6TYI3HTVFJIJIKV3JQUuQWzx+A5i14oHI
mCeH11FgRq6D1B3hjpWFFWI35pRZ1gSZ3tPryQwq1Y0bMkiF4CeuUYEKWIdFHZdo
u/IMfLJoJeYpy8cyv6FznuJzkAR9A1UIUw58zXCD0ipCfKH2w6vwqdoCo4V0+cZd
5cZ1YQSFab3fduU44viKaXf4V0pWK49oDeR/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

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAYAAACNiR0NAAAcE1EQVR42uVT0xbA
MAgS739nO3TpRw20dqpbfARQejOywiwYnCTkDKnbcLk66sq1T+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

```

```

MIIPiWYJKoZIhvcNAQcCoIIPFDCCDxACAQExDTALBg1ghkgBZQMEAgEwggVMBgkq
hkiG9w0BBwGgggU9BIIFOU1JTUUtVmVyc2ljbjogMS4wDQpDb250ZW50LVR5cGU6
IG11bHRpcGFydC9taXhlZDsgYm91bmRhcnc9ImRiMCINCg0KLS1kYjANCk1JTUUt
VmVyc2ljbjogMS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9hbHRlcm5hdG12
ZTsgYm91bmRhcnc9IjUxZCINCg0KLS01MWQNCkNvbnRlbnQtVHlwZTogdGV4dC9w
bGFpbjsgY2hhcnNldD0idXMtYXNjaWkiDQpNSU1FLVZlcnNpb246IDEuMA0KQ29u
dGVudC1UcmFuc2Zlci1FbmNvZGluZz0gN2JpdA0KDQpUaGlzIGlzIHRoZQ0Kc21p
bWUtb25lLXBhcnQtY29tcGxleA0KbWVzc2FnZS4NCg0KVGFhcyBpcyBhIHNpZ25l
ZC1vbmx5IFMvTULNRSBtZXNzYWdlIHZpYSBQSQ0NTIzcg02lnbmVkrGF0YS4gIFRo
ZQ0KcGF5bG9hZCBpcyBhIG11bHRpcGFydC9hbHRlcm5hdG12ZSBtZXNzYWdlIHdp
dGggYW4gaW5saW5lDQppbWFnZS9wbmcgYXR0YWNobWVudC4gSXQgdXNlcyBubyBI
ZWFkZXIgaUUhvdGVjdGlvbi4NCg0KLS0gDQpBbG1jZQ0KYWxpY2VAc21pbWUuZXhh
bXBsZQ0KLS01MWQNCkNvbnRlbnQtVHlwZTogdGV4dC9odG1s0YBjaGFyc2V0PSJ1
cy1hc2NpaSINCk1JTUUtVmVyc2ljbjogMS4wDQpDb250ZW50LVRyYW5zZmVyLUVu
Y29kaW5n0iA3Ym10DQoNCjxodG1sPjxoZWFKPjx0aXRzZT48L3RpdGx1PjwvaGVh
ZD48Ym9keT4NCjxwP1RoaXMgaXMGdGh1DQo8Yj5zbWltZS1vbWUtCgFydC1jb21w
bGV4PC9iPg0KbWVzc2FnZS48L3A+DQo8cD5UaGlzIGlzIGlzeGc2lnbmVklW9ubHkg
Uy9NSU1FIG1lc3NhZ2UgdmlhIFBLQ1MjNyBzaWduZWREYXRhLiAgVGh1DQpwYXls
b2FkIGlzIGlzeGc2lnbmVklW9ubHkgUy9NSU1FIG1lc3NhZ2UgdmlhIFBLQ1MjNy
bm9pbmUNCm1tYWdlL3BuZyBhdHRhY2htZW50LiBjdB1c2VzIG5vIEhlYWRLciBQ
cm90ZW50aW5uLjwvcD4NCjxwPjx0dD4tLSA8YnIvPkFsaWN1PGJyLz5hbG1jZUBz
bWltZS5leGFtcGxlPC90dD48L3A+PC9ib2R5PjwvaHRtbD4NCi0tNTFkLS0NCg0K
LS1kYjANCkNvbnRlbnQtVHlwZTogaW1hZ2UvcG5nDQpDb250ZW50LVRyYW5zZmVy
LUVuY29kaW5n0iBiYXNlNjQNCkNvbnRlbnQtRG1zcG9zaXRpb246IGlubGluZQ0K
DQppVkJPUnCwS0dnb0FBQUFOU1VoRVVnQUFBQ1FBQUFBVUNBWUFBUQUN0aWwTkbFB
QUFjRWxwFUVZSNDJ1V1RPeGJBBDQpNQWdTNzM5bk8zVHBSdzIwZHFwYmZBU1FFak95
d2l3WW5DdGtES25iY0xrNjZzcWxUK3p0OWNpZGtFKzZLD2taDQpzZ3J6ZmNkV1w
TDJqbzA0NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2loQWY1WUpydzd2anYwWldS
V00vdWxpDQp2ZFBmMVFaMmtERD14cHBkOHdBQUFBQkpSVTVFcmtKZ2dnPT0NCg0K
LS1kYjAtLQ0K0iIHpjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQw
DQYJKoZIhvcNAQENBQAwVTENMA8GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMg
V0cxMTAvBgNVBAMTKFNhbXBsZSBMU1QUyBSU0EGQ2VydGlmawNhdGlvbiBBdXR0
b3JpdHkwIBcNMTEwMDY1NDE4WHgPMjA1MjA5MjcwNjU0MTA0MDsxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExvbnRlbnQtVHlwZTogaW1hZ2UvcG5nDQpDb250
ZW50LVRyYW5zZmVyLUVuY29kaW5n0iBGFjZTCCASiWdQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAJqVKfQLwaLjj+gB

```

```
UCfkacKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID1B/wlbdmadXP
mrszyidmbuZm0pB5voVQfiLYYy3iOx7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEF
Xg0aGdmnx40G/e3p1fIKM0dPzZLo0AJF5m500xzXPL74zFCWp2f1ZkuE4A6141ko
aZXCN5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX
+TWzB2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iP
sIVKarUCAwEAAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZI
AWUDAgEwATAeBgNVHREEFzAVgRNhbG1jZUBzbW1tZS5leGFtcGxlMBMGA1UdJQQM
MAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkV
fAEj80eOr83zdw8wHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSHlNhpHGH29FkwDQYJ
KoZIhvcNAQENBQADggEBAIFJeKCCsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtK
t14FzkRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUVZ23M
RsMtjH2x9SG91PEM046gfPnc9gMGHjMtG1qvaKcLQP5UzpEYPLror2X4P5uXxaP0
LIZRzWmkw1RF7FOD7Pfb5v94M5274XYxW2W4uKgd7QGnUZROsvSYkGiWdp1JhqXw
fDz8A0enITGXnoEkAFvviCqh64P1hIeMorj36pgL19oWZD6YrzSWHuZ1F00juyu
0fQsqm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3
QQV57XV/QqmiXDr0+Gr0mqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElF
VEYxETAPBgNVBAStCEExBTBTIFdHMTExLWYDVQDEYhTYW1wbGUUgTEFNUFMgU1NB
IENlcncpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIw
OTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBXRzEX
MBUGA1UEAxMQWwY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC09InoWDgWPK2af0+StijSNOR8K/hN8D+1078oullsk4ASvSwjsCNo
7shUa4xQU15J06VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+95
0MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzyms02kaYW
Tut3SryCqeHEFbZfKB4urMk4xrIJC3CzWruS2Q0FHbB1fkgKN5wXVgkWFfi0ucfC
n+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9
C0gEyKriVokFQgqQ7XNDU+r3SeOWks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIw
ADAXBgNVHSAEEDA0MAwGCmCGSAF1AwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21p
bWUuZXBhXbXsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAw
HQYDVR00BBYEF1v2zLiThQYSHJeuKWqQENMGZmZMB8GA1UdIwQYMBaAFJEwjnwH
Fwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjD/4K
kkOHG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30Uxf
yrZ1RAZef7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENT1sRxlcvb7HV
X524bkZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JckzP
0Qhp7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+
JJtzOKypYQ3eoZ6EPazXqMyHAvCsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSz
NnEmMYICADCCafwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQLEwhMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTBTIFJTSBDZXXJ0aWZpY2F0aW9uIEF1
dGhvcml0eQITN0EFee11f0Kpolw69Phqzqp1zALBglghkgBZQMEAgGgATAYBgkq
hkiG9w0BCQMxwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzAx
MDJhMCA8GCSqGSIb3DQEJBDEiBCBkEM75wgxS0KXxqQLSNadhQ5kD10ABIYw030cj
kP4nsDANBgkqhkiG9w0BAQEFAASCAQA9zet9PbdeB0dT0TVjIwCXvUjnj1/UN22d
GV2Q1//QcTN3Z7wMvLilhcYHrL8S191Im2XYCV9r2yqvVyiB+qN+69y18HIzZ7ok
rgqQ8TDPt4IW2UXxyXrB0ItFirlKklntf4SafPq73ipeZLMc3x3jr84lr7psIknP
EEemNM+okG6FHduKq8nSvbAKlahOE9qvDGcBJBYXtn+/ijqA6Fxu+mJDshCz0Vvq4
uVxp0ZS3py0+Gg0JJnLD+z5+MPq08TrSTBhZYQauVQFji9Kjb2A8KZpLjEXvw/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

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAyAAACNiR0NAAAACe1EQVR42uVT0xbA
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
```

```
iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVTOxbA
MAgS739n03TPRw20dqpbfARQejOywiwYnCTkDKnbcLk66sqlT+zT9cidkE+6KwkZ
sgrzfcqVmpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRUErkJggg==
```

```
--757--
```

```
--872
```

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

```
MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCcC0CAQExDTALBg1ghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHjCCA88wggK3oAMCAQICEw8tJb0R0ZkZkJUUh6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMA5GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EGQ2VydG1maWNhdG1vbiBBdXRob3Jp
dHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MTAhaMDsxDTALBgNVBAoT
BE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMRcwFQYDVQDEw5BbGljZSBMb3Z1bGFj
ZTCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqlWALjj+gBUCfk
ackTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID1B/wlbdmadXPmrsz
yidmbuZm0pB5voVQfiLYYy3i0x7Y0qzXrL6udP07k0sV+UdSNRFxrfKeoQEFXg0a
Gdmnx40G/e3p1fIKM0dPzZLo0AJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC
N5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVGRNhbGljZUBzbWltZS5leGFtcGx1MBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj
80eOr83zdw8wHwYDVR0jBBgwFoAUKTCOfAcXDKfxCSHlNhpNHGH29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCCsTKCfQMPTryujRGzJdYA+R9eBAuDLsatbtKt14F
zkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUv2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKgd7QGnUZROsVSYkGiWdp1JhqXwFdZ8
A0enITGXnoEkaFvVjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu0fQs
qm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBAQUAMFUDTALBgNVBAoTBE1FVEYx
ETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQDEYhTYW1wbGUgTEFNUFMgU1NB1EN1
cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQLEWhMQU1QUyBXRzEXMBUG
A1UEAxMQQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWpK2af0+StijSNOR8K/hN8D+1078oullsk4ASvSwjsCNo7sHU
a4xQU15J06VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzyms02kaYWTut3
SryCqeHEFbZfKB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfi0ucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9C0gE
yKriVokFQgqQ7XNDU+r3Se0Wwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDA0MAwGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYD
```

```
VR00BBYEFLv2zLiHtHQYSHJeuKWqQENMGzZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEgBDQUAA4IBAQBziaI2p86poGkjD/4Kkk0H
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENT1sRxlcvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr40pq2JCKzP0Qhp
7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
0KypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCafwCAQEwbDBVMQ0wCwYDVQKKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGx1IExBTVBTIFJTSBDZXXJ0aWZpY2F0aW9uIEF1dGhv
cm10eQITN0EFee11f0Kpolw69Phqzpp1zALBglghkgBZQMEAgGgATAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMbWGCsGSIb3DQEJJBTEPFW0yMTAyMjAxNzAyMDJa
MC8GCSqGSIb3DQEJJBDEiBCC5KpxWrqp9lc/at0VVR0dHn83fXt5r6VC1EPizN3pz
YDANBgkqhkiG9w0BAQEFAASCAQCVWFu4+5JFFOLMcfSgjQsyxsRKPlmT35MrYT1
rZKzBqdb7BgsgtavL6xHs/GKGjbqHwrrPADgsnyeXwot0BZoFzxLxw9fQI7z7wH5
QbGLEj6hRHvrSdYzh1ptTnTqc4hXdyWh3jjNJlIf1D01EP9KySaLt3M/aGcNUKD0
z2ngLLtpOQULqGm/IxkIG+Rj9YHlktQVEiPxtT+TQ8q00eiHZVukT88BpG0BBpCs
9aLUH2JuEF6v6wKp9S+sWj4sx09bzYmNP0mi8WWyGYx5NVldgzeZxhISConuiji7
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

MIIZHAYJKoZIhvcNAQcDoIIZDTCCGQKCAQAxggMQMIIBhAIBADBbMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBTVBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
```

UFMgU1NBIEN1cnRpZm1jYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAgxvLw0XDh1LUZffbbDPPnrXQvEqUfaDKF
q/0tzSwKuX4GYXwI2srRxm04umoeqcyUdiaBx0Vu4R2mSCSUFspk+W9KACMLqpT0
hAheLj1B2C2Pu0t0Nbkb074Junxy4DM7epIDpMRqfDs78QSJtuLehkVZRSPbu+of
fdEjeihEluJrK171PW04zgCUajmHpT0QFkstBnP8sI631tIKutQ1tn7f7NbXFSkI
gnfZnp09osQpUI1hfDbKsPE4Lsv0p3R60Bhy3xK27qS53KMH4bzQrIN86FiGRgYL
25s003jCSDuNimD1q0Yq3ADJwiN8JE4vx17oh0vhqkV+cFfiA6MwggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1UyYBSU0EgQ2VydgLmaWNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAjofQnu1xr50wncKoCmExvdj5
eIbwYUuUrpfriURfX3dhMTAQ5jnQghbIi+zmTuraElTk6Vi65/rpDBz7a4YBAaeQ
jz3GH4ua8j5wrYe44ipXaZnHd2QkS5zYCER/1BD/lGrgewhy7Ef4QI03drzT3zF
rc2YozxaViKZ/KUaBn27B1IPZoXWtah1Sa8TnoZkCl4to5mI5K6vLuxAR7WgFC84
5vpnELyyiXcET0cjDnnvfx2wfUpBP04gx1S+VTzcCn9i/b35LiLoVWS1WabY62Zt
RR1NH2gtIqNKjw3X6XvSM63e6qilg7vxWf1wv6tS+m1gsVzxc58u1g0zCxCuUjCC
Fe4GCSqGSIb3DQEHAAdBg1ghkgBZQMEAAQIEEL40vXNKumsqJAgvAXypoaAghXA
WAvh2j69ZQKJIU7KRi1TU4RuE4uuPBn+QLa50YXocxAA8bN2x1BcW14DgR0hZ6mA
aNV6yzK+aNKypn1KLwo+Yww911hMLdjVBUJxZan9N7RvRTwxvBqxUFP56m/t4Nxx
lKkRICb2yt0+/RzMHAA4NqAnugmiOPs1Fcva2vXL5eRn0vrxQCTQ0kuPdRLNM1JX2
u1cT59pFStaxkPxEMEm9ES8+nuvJNX/a0mUrpvYQsED7vCvDlcmd/NlQ8fbTiMj
Alg20nrbCxBGk1RqpElmLP8t7ip1JX3Uqw7rB0zVoRpf4q4nMN+WIdSsJevnn
cyy09kTEhklwTmkldme2XSmuPukBjW1RghHV5hpWDMlssURpb4rMf79l/8mbuZbQ
juHI7gXVdudDH/VxeMx3fPYtYRrkXia6XHtHfOIFRuYuXeoX3uG36FDrCXUHTHQ
5TujlJkI2l8gYUsNU19JpFj5mauVn1LWHc1ZdgY7Lu2DCVooybBD4Zfe2laQK1+ZD
KiVi4yxFWMLbZzENMmwUXnrf12x18uEzNW63Ms573Cp6DgLj5acFSJPA7GuKT25Q
+C2lFp4o48hMdwqL7xZU1cxEjiUE8bhvBVQ7RNVWziANmI+vzAXyPmq+LNjeaig9
yzTEDRrcDISL61wVBf1cakbrDS/zitKy4WZta15pWLPXS5Nm0o/j78H424poEnkl
BLdn9VFjENNYqsZwXumTxMoGE9bMFA0Qny4FrMCyuFLVcu2ktQg6L2q8CSw98Eod
KAg1vyKIYUtnMghZpx2dSWaVV/0dFzgV9q3ezgKft3GrZ2MP/vdCfNB0+GM9yJ79
KJcgdsUv8GeIs0fkihsABdUMZn/kdFdDQIX4w9K5hmxWXEr37ancwRloBgC2Ke
5Ci/MtKsHtnaAMhAhwHDtaB2j1ITWQUvu3uBe4CffQaZblYhro1KedIcMco/Kw3Y
sQgE2SBhKTmiIQc/JPlnn350J93zVEzdouhzjX09NyJpQHX614iJs8V0GevTfcXN
0fsuT0XdX5ArjlFKB4Wv4G6jVf9lQqNHpr/fEnSeuz0bFnGrZetRYHlHu/gxsDDA
BHAIrmRhPNUJEMWkeC4t9MWfDMtI0EFb+80E8y27bYh3VlGxJS/Mvfw1sgRmp2+
17Gyny7MA9xMtIhetzG0pLb/8dwODdenv/Set1qJ3yDDS7S6UnNsbuK1/080AYBL
hNb05pGYiQohf1Hkq0Rrs1ps6lxdz5hk2fm44sgCKtTC3S7g50UbATSx3z11aEE0
bnTcNEoh+iHUj4YFRhz/sB8sqeodMJS1bU1A120gmF+cJyLT7+SdAR0/vJxjkgP
vVB1p5Eut27JGaACrXfWE/hGGriLgdiT4UgV9f5pru7w9TVM67jc59+7Flz4bSct
K+xUskePye1SN4DeaSD0m9hYUZMfKu9lCXAWRdGJd4zWdICBbWcfNvuaJuFZb0E8
16lmS61f7/6zhLSREt0xNP/hsJa2QpnDE5hQWql31kyC7k4T3bGzvYRK05D063kF
Mgo2aofZ4QdbS17P0iibSEj0KyxhXCDnJsybQ25g0ycg0VoshVZj1loxIDfMZzh
lRuA04q1dm9W3o/MXKLbhWhyFAEJswnz05VxrXyUQLL9mmcp8I8fN1YH9gd/DQQC
BQPkzzFs755rJpdPJ1KKoj8aKefDzNSBsZgHdwNUjbrGHRQAgqYg8QHxHzG5SNA+
xX1uvJv7gMcr1SFYTKKgWKM7tdBmD2dhxQL8FGI+Z1ZEF9GZ4UIVEMRVJqZ1kQ0k
qsR84dxCeJnALehDDAjsY11E2+0JA8D0+ddjdP1F3h5DNGs/GwJ0CkStf9mWt2LG
uwueWxdEeI3jphF75ttwJ4v81Dv4vEH0suzcQS701PZmLoqXu/h60SvKK4txEr20
60uc8un8a4//WcMotRQMfMmYmNomY/HaayEhbEPWofENsEgsa+70oHFggcM70Mts
TyW2MOXM7KEgUH8YRsHLx5a1V2TCqVeJmUcq/MeQZs30rxBywGNVRPijc8XSV9k0
fRI+h+d7c2YR0k8QLRumdZdKxg9229I40r5jwG0zwljFCYEsyWC8AEw5TKi0Y6mE
cdkY8viRK1ZkVtFR7od3xgfzjm0Woo1BW/Nj4Q3j9B7eR+Td0Zqq26/t7Xiqz1Mq
jor08wBhE4GtrxBHvIjgvArNiBe/z9s4p5ZT5sMWqm7YEzkaWeocT5cvJGZVdmC5
CtNUI1mmTIngy57sIx16rSXcdrS18qMvTc0/7D3mSChpj10QxhP95jtEkYMAyqsr
vJtZMCaumihR3BKbnsPkdpZeXb7VBGW08M1jv9dy2MucmTCyP8inDhMwPuj1sn2f
VRqgyqWcFLH1N47gXtNtKb0vzJ0NkHfJqpJRY6NtQ7mVHT9ZUjh6HjPVU47Tik0J
PU97IYvGhwGnKf6R0UXoUt0X4rba77kgBAA8NqtGFB007IZ1NzL7hb98TjMOM0pn
piWsihdkP50KgV9PTorlhmV/g1ZQ3Dli2oFBmdQrdM0fvqWZwTHf6qFXXasjgkKh
Rcr1o4TfRQT/WbHj4Mjcx9/govqtB2ssw30JTI2s6NxVt+0GKK798W4mAC1YqSDY
2nXBS00a7vr3MRzlmwMtFvLe5WIV4ojjvcjRmgFLVA9d33D0Cvb9h5tk8jch07H+

mhcXWhKq+UgmK1xjKiNqFOUmif6vr9lwv++RGJEuuJVVRgucfMuuQJmhOTBeuEHA
nTg3ILoJ5I9CFTBCr8w8CGfJsax1gmOpY39aXxgXNBWH8YhGPi9UYu/cUdiXyEQQ
kBmFWvaD45247R1ubkERejEd05z1/K+93KhZVDeoMow/Q0GGEEQ/SZ5als5NpyzJ
Q7qI5jDjSqreiRXRrX1WQTN/7aTaCnw1LwN05SNHVzZP1vAQIZQ1SYxMzrFPtuF2
5uiFKJrUpe48NkLni8bAKOb3Wc40vLlPhbBVQuRz01N8VE8gZMcZzQcdsFvorEor
+4+ABaHVsTbdrLGSgSpTcqGpTcd620H9JvrrNgfdv7eZ/ZD7TT9XG6coy4dz033
gaWIY+VZy/poMm+bFjYD8B7bc+qiTYQrIyBmFaC5haFgRnvN9nFq20mL40g5Q9Ur
eLfPwPc5aBgr+kKjebSM14ZLV7T21BPDBDZ8JWFWFutw/SUR/7a9S7G8YkztQPXh
/EMrFUsxK+eYu40CbTGM0dZOAvnL03Na3AjaSJGVdCKU50Yc4HxZ0dTOmm1tfrj3
PZIWjOp5LYue2SK/pqG1GeFztaZbGF19zkLmZMRr1K071RQeaI11wLkZYOLRonIS
qE7z6mj//Z5x6zP17i11LhWMIXZECpMFjKA4dkfXLPa+aMqd8Wc7p1F7UeJbu+x
K4kLfJdRf+YjIc6F+OtJClK98AKxjfx6Hs6AdTBT3SkKci4qPmN0slv+GgyUP4yf
MwXiTn3/Tv1rHARaEQrKCTUL6GnedTEFZIPy9UUCG82PerOeyitm6m4SmSo+VxSf
grQQP1rCjz0xxaz5PT0+6rdlki53T4rBUYzw3E11i5r7XA0Pw9+dLLZRLW514Dj
vr4XvuyhKu7PZahKtoYMBKVw423JxNpJkgP2DlHb78pUeNMaUuWgyxjSLX6mpf5
c4a5Q0+R9fw4Acs/QtdoX5ZMgMoSpdN8x7AdBtxolicWe/iQECurAnRYcrwKXo7+
WVURy5/cq6Z3STIHqdCcGBBJLX90sGIyBK80mgmhNDjbRe4fdeVXOSWQ0cdNQSXT
KFg5G75UuCkukly7e31XNBhhRQy58jbuhM4bptnxqM7cz++uC1Xfl+zm8TX+1gRM
B0DVg/e50pJT60BQv/V0aVChRu9pMa7B7Zi44iYzh4jAK2s86f7d7amLQZT+PtCY
g+Q+8Vxf+XUDs1wciqcBZA9Jo4Qk/1cb1DBmxj7Vh54liv/nHUEroh1UV6CVWOM
Jcb43KIuhkKooVG5e1/u/9SHRt4ne5WK9QQruL30V0hzfopc5UAV57ocQBMHdgqT
ezq+ntFTFlez7Loed/zUqInzWhE3I7ID+pJX6YK5ti4E5uq0zBYA8bj/a3PTWE2G
2PteVZgcMK3764MB/dRgSPZ8HdpsYcG685aCzs3zEiYVi/Q5Zp4q3UBzRy3TY0mh
djvDk1RCwkmKxZRQDEJV0cxz5GdMcUlt8WAB5pjK3LG3gIEbfd8h968U+D3+ufV
6KjRsh5cweupN51piLneBEg5TgjZzSMuYakrbezTRfyS09SFIj2JvLfWvuX8grEi
101qRGC8/07/I4L45Sb8diZaPsNI1/3kuqjGMASytneFYcrurCGlC1UweISh0rtS
deHjmBB0q+YyAYybF2ez6AVPr/SDfwxcK+cQB1wmpdfytyuLhY3uEQE53aPvxb9EW
RVGOKJv4fxq0gAt99XeXQvgfWWM/Kix/hI+zP5g0rzKW0i/T7wdJBQDBI0wqbauP
fepur9reL75ixWn7AR7iMaEZD6sCfEojPhozeFUZ6KZdGo1baG3bRW5IRq4g9rt8
Ypuj0Eo4dFtf1ECQHAsOJ6xiCHs4XLgB9iLJd4eMzHuZDaVdPRp4JQT9fi8/st3C
RfDkyIdFb1aAxX/D8xBykE1zwC4TR3ejTEVwpQUNz8GOW+npz/uTukjKxy0+P4qX
NSJap6dmxb341U0tE/OnuMFcy2IrvE5g+NzzqwcFG0E0pk+Ii6HVgmZDhMhzzYzF
eNArxRQP2YA+dnn10X4o3oB2gW47vZ+PF61r6DcUWlTCDaVDU5FvMEu5A0asuwp
/JSkBafZ0xup8QQHdhIQhuL99Y+CkNDGqh6d24L93bSRFiYu1k/sRO+QdWrNtyZ8
MY0oeEsVP/MDdi1anKE0Un1snSaGc08yaSmHqttLI85KnG0JCNsNvJ/qB7DQXXAd
gUWHM12x/dbbBwwh5cc281352crClDtdm21Vor//Jd8sz3o9dGIRyyf/NiEvuK9A
Y4JjMEHKZ6/XFgBxmgKAXnik642D6zCX7phGRgcVTJX54NhiJ17DT7sw/VIN91sY
GZoAWFjvu9wto1HADhz20Cftrm8bs/SYyf2hUma9DL8Ej11Qvtc0KHZxuKNXcqa
+srUomSq+HrGMBL5SmVdwvRptytopEKPvVMZDS27IacnioEljjCHzQdqFu6zmmwRu
5d3gmwV0zuubQPz5FXiuyQ0ombKR4G9MWSLsRwMiwMz5sDaNbSiAKRgLDfXbQmL5
qH1hHPTAZSD8r6BZTwHPsi+jfBH4lpgsdjHRYwk6ApX4lCdRa/q5SaubBZkJnxpE
0Tg0IXypGPWYPefHVv2aiy3oHs21k19YpokEe3askAcpmXFGSkf1Fzhac0ZalBR
cP8fapP8yJY8Ys/fZDHGKB4XL28JKfMUeb7+YwTAN+yoj3YsfdfsM5EL7oZHcb/H
JQhdvTLA5Iyi1IUdk/GUF+YYKuOMG50KC1qAX2fm2X9Um30HTCENRuLlbT71youR
ei6dhxqHMBcBoscqFLVbVu5ESGVyJYpML6EjzCrkTgJH+01CI3Zsu0y1JL+L2CN
0H5KQ2y7aMqbiq+122QrjICWNNWrA2qgB2x/NI/BiH5vGs5HDvKTDchafWQiDvJU
k4+CSSnxKs9AJ5VLStkLfEaxvtbBDt5KaLtmCE8yKKc6fGB4ji9CSSdWcfjCdd0K
i/DaW0xKcwwsknVaYbL6evqAk5wEZjacf7kudcYTKBuMdEmM7vKVluXwI671dDdL
BWFsXi2pTpFnppA90RBvNS7nDG0mKhXzTiQjEZx0uWT97yW2Dtoa106V1GLyC+wM
X5TlswenP+r79DxCmpzYk0GI9SGAG2gN0SWr10wy54M+ZnNynntc39wz355IzhDG
08DBoZVF69/RUGHVzJm65MMJjNEcv278QHTlyw4B1upA04CMchGYfFDsQP0297wd
6Ip8ScpKNx04amwDcK6y9E0tre3I3cW01Rr1Tt1tIW3bY3iTDjv5NStfZxAhZlpX
twb/BDabvjLDpfPVlRXB17iC7RfI1q9WdpV6Zam4aXjYlvpWREZ1WXuTpi1lxGxv
CMYbRfrgTT60ZRwNeiY12p0610DzwQTbVS5L0JE9NSr6Cx/lGQ1Y8wxbJ1A0FAzW
slLnMlk0FE2Qbfyz+6Yg33xD90m5LRnxBdd/zifczhV9+K1J2u1GvaUAN9CVHrhW
8M/ukjGWwxsq1adPx1BK60H/vAIhynbYio0lrVxi6xYHfnyjfhAb4aFozE98X2hH
UFUFdY2qn8CT5say+QEyiA319gtZ6U1rqGpLD0KVNeIuaJXLZBst8sY/Dzvdyf1K
N+nGUR0grmuZZMIdkZTL1IHGtKlDTRfTzdT4qPz0M30xDw+DjPE6n3C8vxgWWH7A

QUFBQUJKU1U1RXJrSmdnZz09DQoNCi0tMzYzLS0NCqCCB6YwggPPMIICt6ADAgEC
AhMPLSW9ETmXSs5CVIEh7j00Boq0MA0GCSqGSIB3DQEBDQUAMFUXDTALBgNVBAoT
BE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUFMg
U1NBIEU1cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIw
NTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLewhMQU1QUyBX
RzEXMBUGA1UEAxM0QWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIB3DQEBQUAA4IB
DwAwggEKAoIBAQCalsn6i8Gi44/oAVAn5GnCK4PHHNjrsfWUnne1N41KImVaTC3D
9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2Gmt4jse2Dqs
165ernT905NLFf1HUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZu
TtMc1zy++MxQlqdn9WZLh0A0peNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCq1LqhBwDH
dZ5qDTII2PVX1X3K7/c0NxbvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGewy
6SCf58duq/A0EksCAW1b+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/
BAIwADAXBgNVHSAEEDAOMAawGCMGSAF1AwIBMAEwHgYDVR0RBBCwFYETYWxpY2VA
c21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMC
BSAwHQYDVR00BBYEFKJtQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEW
jnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIB3DQEBDQUAA4IBAQCBSXignLEynBak
DKU68roRsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsox/Ht9Ii6zyBZVjdao
x644DsiloQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhdTxDN00oHz53PYDBh4zE4Na
r2inC0D+VM6RGDy66K9l+D+b18Wj9CyGUc1ppMNURexTg+z3web/eD0du+F2MVt1
uLihne0Bp1GUTkr0mJBol6dSYa18Hw8/ANHPyEx156BJABb744gqoeuD9YSHjKK
49+qYC9faFmQ+mK80l1h1M9RdNI7srjn0LKpuob6w06jaRzWdNeXz1Ec2tUpAr4vR
hZjVD6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpq1zANBgkqhkiG
9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLewhMQU1QUyBXRzExMC8G
A1UEAxMoU2FtcGx1IEExBTvBTIFJtQSBdZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAq
Fw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOZENMASGA1UEChMESUVU
RjERMA8GA1UECXMITEFNUFMgV0cxZAVBgNVBAMTDkFsaWN1IEExvdmVsYWN1MIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PKrYo0jTk
fCv4TfA/pd0/KLPzBJ0AEr0sI7Aja07B1GuMUFJeStu1amNfCwDcDkY63PQW1+DI
Ls7GxVwXurhYdZ1aV5hcUqVackPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TC
N012DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8ggnhxBW2RZAeLqzJOMayCQtwS1q7
ktkNBR2wZX5ICjecF1YJfHx4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPpDfTM
SiPR+peCrhJZwLSebwWXLJe3VMvbvQj0BmpEYlaJBUIKk01zQ1Pq90njlSjL0wID
AQAB04GvMIGsMAwGA1UdEwEB/wQCAAAwFwYDVR0gBBawDjAMBgpghkgBZQMCAATAB
MB4GA1UdEQQXMBWBE2FsaWN1QHNTaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYB
BQUHAWQwDgYDVR0PAQH/BAQDAgBAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDT
IGZmczAFBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0B
AQ0FAAOCAQEAc4miNqf0qaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3Bj
J0d64roAKHap+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIj
So27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahixRn/C9
cy31wbqNsy9x0fjPQg6+DqatiQpMz9Eiae6aCHHBh0iPU7IPkazgPYgkLD59fk4P
GHnYxs1Fhd06zZk9E8zwlc1ALgZa/iSbczsqckN3qGehD2s16jMhwFXLJtBiN+u
CDgNG/D0qyTbY4fgKieUHx/tHuzUzZxJjGCAgAwggH8AgEBMGwwVTENMASGA1UE
ChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydgGlmawNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJc0vT4as6a
qdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCsGSIb3DQEHATAcBgkq
hkiG9w0BCQUxXdcNMjEwMjIwMTcwMzAyWjAvBgkqhkiG9w0BCQQxIgQgup+VC4mf
BVNHPJS0b9oKX/dVMKiR3JOz5AXfqv/YG0AwDQYJKoZIhvcNAQEBBQAEggEAJ2XX
xojAdRnBTRahPos057TnArr1wju76pnJSWXX1f1GWjEsSphVro2t9LRKALqWtnX
YLM1PbrPoMyivqfHf1k1h1dR9J2aXisS4FfZB3jj1c8Xkd1yZb8qTBBRQ4v17MFS
1bEKW4ecopbd67f73QhUvk3NGJ8Aq8JPY8yxKGgGH9bucecSGYAHC1745wosTs81
aaY3k5UwyHNxRjFkkQAsnMe7HAiVnwsDLYCD0XACbg/D0w0CFK9vzDYkD5HjnkK2
wrhKts1R4QZW+gWXPfYCY1f3fMvrGZvr9rCwgjnwMvrPjugZi5QGoi/sEdH05T5
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

iVBORw0KGgoAAAANSUUEUgAAABQAAAAUCAyAAACNiR0NAAAAcELEQVR42uVT0xbA
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
hkiG9w0BBwGgggIpBIICJU1JTUUtVmVyc2lrbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVYLUVuY29kaW5nOiaA3Yml0DQpTdWJqZWNo0iBzbWltZS1vbWUtcGFydC1ocA0K
TWVzc2FnZS1JRDogPHNtaW11LW9uZS1wYXJ0LWhwQGV4YW1wbGU+DQpGcm9t0iBB
bGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NC1Rv0iBCb2IcPGJvYkZzbWltZS5l
eGFTcGx1Pg0KRGF0ZTogU2F0LCAyMCAyMCAyMCAyMCAyMCAyMCAyMCAyMCAyMCAy
VXN1ci1BZ2VudDogU2FtcGx1IE1VQSBWZXJzaW9uIDEuMA0KQ29udGVudC1UeXB1
0iB0ZXh0L3BsYWlu0yBjaGFyc2V0PSJ1dGYt0CI7IGhwPSJjbGVhciINCg0KVGHp
cyBpcyB0aGUNCnNtaW11LW9uZS1wYXJ0LWhwDQptZXNzYWdlLlg0KDQpUaGlzIGlz
IGlzeG90LmVkbW9ubHkgUy9NSU1FIG1lc3NhZ2UgdmlhIFBLQ1MjNyBzaWduZWRE
YXRhLiAgVGhlDQpwYX1sb2FkIGlzIGlzeG90LmVkbW9ubHkgUy9NSU1FIG1lc3NhZ2U
c2VzIHRoZSBIZWFKZXIgaG90LmVkbW9ubHkgUy9NSU1FIG1lc3NhZ2UgdmlhIFBLQ1
DQp0NCi0tIA0KQWxpY2UNCmFsaWNlQHNtaW11LmV4YW1wbGUNCqCCB6YwggPPMIIC
t6ADAgECAhMPLSW9ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUDTAL
BgNVBAoTBElFVEYxETAPBgNVBAsTCExBTUVTIFdHMTExLW9uZS1wYXJ0LWhwDQpt
TEFNUFMgU1NBIElcnRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQx
OFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLewhM
QU1UyYXRzEXMBUGA1UEAxMQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCalsn6i8Gi44/oAVAn5Gnck4PHHNjrSfWUnne1N41K
ImVaTC3D9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMT
4jse2Dqs165ernT905NLFf1HUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S
6DgCReZuTtMc1zy++MxQlqdn9WZLhOA0peNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCq
lLqhBwDhdZ5qDTII2PVX1X3K7/cONxhvBbaU1/k1swdszUtjhflYFZ80RuQ3qFC6
```

```
vL/PGeWy6SCf58duq/AOEksCAW1b+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYD
VR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAF1AwIBMAEwHgYDVR0RBBCwFYET
YWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8B
Af8EBAMCBSAwHQYDVR00BBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQY
MBaAFJEwjnwHFwYn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQCBSXig
nLEynBakDKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gs0x/Ht9Ii6z
yBZVjdaox644DsiloQEP4YMS7y4q94RFFdmdzEbDLyX9sfUhvdTxDN00oHz53PYD
Bh4zE4Nar2inC0D+VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eD0d
u+F2MVtluLihne0Bp1GUTkr0mJBolG6dSYal8Hw8/ANHPyExl56BJABb744gqoeu
D9YSHjKK49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzLEc2
tUpAr4vRhZjVD6FYMIIDzzCCAREgAwIBAgITN0EFee11f0Kpolw69Phqzpq1zAN
BgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGx1IExBTVBTIFJTQSBDDXJ0aWZpY2F0aW9uIEF1dGhv
cm10eTAqFw0xOTExMjAwNjU0MTA4ODUyMDUyMDkxNzA2NTQxOFowOzENMAsGA1UE
ChMESUVURjERMA8GA1UECXMITEFNUFNgV0cxZAVBgNVBAMTDkFsaWN1IExvdmVs
YWN1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9P
krYo0jTkfCv4TfA/pd0/KLpZbJOAer0sI7Aja07B1GuMUFJeSTulamNfCwDcDkY6
3PQWl+DILs7GxVwXurhYdZlaV5hcUqVackPvedDBc/3rz4D/esFfs+E7QMftmd+K
04s+A8TCN012DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJ0May
CQts1q7ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN783
6IPPdfTMSiPR+peCrhJZwLSebwXLJe3VMvbvQj0BMpEYlaJBUIKk01zQ1Pq90nj
lsJLOwIDAQABo4GvMIGsMAWGA1UdEwEB/wQCMAAwFwYDVR0gBBawDjAMBgpghkgB
ZQMCAATABMB4GA1UdEQQXMBWBE2FsaWN1QHNtaW1lLmV4YW1wbGUwEwYDVR0lBAww
CgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgBAMB0GA1UdDgQWBBS79syyLR0GEhyX
rilqkBDTIGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkq
hkiG9w0BAQ0FAAOCAQEAc4miNqf0QaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ1
9naIs3BjJ0d64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaV
WHg4eHjSo27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHa
hiXRn/C9cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIAe6aCHHBh0iPU7IPkazgPYgk
LD59fk4PGHnYxs1Fhd06zZk9E8zwlclALgZa/iSbczisqckN3qGehD2s16jMhwFX
LJtBiN+uCDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTEN
MASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFNgV0cxMTAvBgNVBAMTKFNhbXBs
ZSBMQU1QUyBSU0EgQ2VydG1maWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJc
Ovt4as6aqdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCsGSIb3DQEH
ATAcBgkqhkiG9w0BCQUxDxcNMjEwMTUwNjAyWjAvBgkqhkiG9w0BCQUxIgQg
K3l0LqVxzKfZTCjC4/0WD1ui0JZ/y8y2mKLDM5P/bj0wDQYJKoZIhvcNAQEBBQAE
ggEAIWwXPK/j2eujwSbftm7fHd+LZyXyhUhfzGhxdPZyunkZmQ+N4ARXGv0zqr
y0gKhBdbd0pF08sIfqRGvU2eQdvfFWTKz1Nt1UMGMUtTTA2Iua4+QcPdJX6At6k/
pp/OdEIuSLQHW89UkUfNEqYc8Sjnh0aTMz7glWEM9jIXuWcmhtRqqsg+yYItvSbd
eXktWzBWuVCzvs04Q3oR4B0Aohdf+qCeT0wP5grdU4oIadD4eq1o+0EZfmlin2N
3dNYgd65gF0IXek3a1MMFh6AQF9aJz6451Gq01fwwwX2TtRnjXBY0ucY2Rn6h3PB
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"
```

```
MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCcC0CAQExDTALBgIghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMA5GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGhmaWNhdGlvbiBBdXRob3Jp
dHkwIBcNMkxMTiMDY1NDE4WhgPMjA1MjA5MjcwNjU0MTAhaMDsxDTALBgNVBAoT
BE1FVEYxETAPBgNVBAStCEExBTBVTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3Z1bGFj
ZTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAJqVKfqlWALjj+gBUCfk
acKTg8cc20tJ9ZSed6U3jUoiZvPMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYy3i0x7Y0qzXr16udP07k0sV+UdSNRFXrfKeoQEFXg0a
Gdmnx40G/e3p1fIKM0dPzZLoAJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC
N5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAa0BrzCBrdAMBGNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYZIAWUD
AgEwATAeBgNVHREEFzAVGRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj
80eOr83zdW8wHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSH1NhpHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCCsTKcFqQMPTryuJRgzJdYA+R9eBAuDLsatbtKt14F
zkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUVZ2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7Pfb5v94M5274XYxW2W4uKGd7QGnUZR0SvSYkGiWdp1JhqXwfDz8
A0enITGXnoEkAFvviCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juy0fQs
qm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+Gr0mqnXMA0GCSqGSIb3DQEBAQUAMFUDTALBgNVBAoTBE1FVEYx
ETAPBgNVBAStCEExBTBVTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUFMgU1NB1EN1
cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMQQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWPK2af0+StijSNOR8K/hN8D+1078oullsk4ASvSwjsCNo7sHU
a4xQU15J06VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2GxzYms02kaYWTut3
SryCqeHEFbZfKb4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfi0ucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9C0gE
ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEADAOMAAGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYD
VR00BBYEFV2zLlItHQYSHJeuKWqQENMgZmZmB8GA1UdIwQYMBaAFJEwjnWHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQBziaI2p86poGkjd/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZL
```



```
RAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEnt1sRx1cvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr40pq2JckzP0Qhp
7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsM0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfWCAQEwbDBVMQ0wCwYDVQKKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGx1IExBTVBTIFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhv
cm10eQITN0EFee11f0Kpolw69Phqzpp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNTA3MDJa
MC8GCSqGSIb3DQEJBDEiBCAfybSsej+1D6r16hb18FcqV4ucPU0CgwMlVVH7gTaP
3TANBgkqhkiG9w0BAQEFAASCAQBw1RSGR80ZHF+8cUc5th58+DiNkwKWqz4pWWW
0QP9uuxRzjE8Dt97b88d0HtZWL98qAp+bjFK8ElktpuBiS5Nuiy+Zm3XnMU5GhCM
ywIPUAPJA6jvibT5fzYvMGV11RBmrTFNBZxxrJOAwfGf96vx9VajBVbyXdXnV7
hnQCx8wsbIOrbRUUVJHBGqpx+j+bIoUmg3uKx0YkZFz9IShmq8fzsw/CVTBMLfoT
qle2y+4H+R1G1oqz8Mvs+XXbL5MG1r5PGjgpa9hHxPKdbFQCoWIJMA6xJNKgeuN
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

MIIQWYJKoZIhvcNAQcCoIIQNDCCEdACAQExDTALBglghkgBZQMEAgEwggZsBgkq
hkiG9w0BBwGgggZdBIIGWU1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWNoBzBwL1t
ZS1vbWUtcGFydC1jb21wbGV4LWhwdQpNZXNzYWdlL1U1E0iA8c21pbWUtb251LXBh
cnQtY29tcGxleC1ocEBleGFtcGx1Pg0KRnJvbTogQWxpY2UgPGFsaWNlQHNtaW1l
LmV4YW1wbGU+DQpUbzogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4NCkRhZGU6IFNh
dCwgMjAgRmViIDYwMjE1MDY6MDIyLTA1MDANC1VzZXItQWdlbnQ6IFNhbXBs
ZSBNUUEgVmVyc2lvbiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdG1wYXJ0L21peGVk
```

Page 90

```
n+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcs17dUy9u9
C0gEyKriVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIw
ADAXBgNVHSAEEDA0MAwGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYETWxpY2VAc21p
bWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAw
HQYDVR00BBYEFv2zLItHQYSHJeuKWQqENMgZmZzMB8GA1UdIwQYMBaAFJewjnwH
Fwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjD/4K
kk0HG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30Uxf
yrZlRAZef7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENT1sRx1cvb7HV
X524bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JckzP
0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+
JJtz0KypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSz
NnEmMYICADCCafwCAQEwDBVMQ0wCwYDVQKQEWJRVRGMREwDwYDVQQLLEwhMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTBVTIFJTQSBdZXJ0aWZpY2F0aW9uIEF1
dGhvcml0eQITN0EFee11f0Kpolw69Phqzpp1zALBglghkgBZQMEAgGgaTAYBgkq
hkiG9w0BCQMxCwYJKoZIhvcNAQcBMbWGCsQSIb3DQEJBTEPFw0yMTAyMjAxNzA2
MDJhMC8GCSqGSIb3DQEJBDEiBCAXURNXz0Mn71PPDM1oQHd1876V7RbyfNsR/srF
sVvmLDANBgkqhkiG9w0BAQEFAASCAQAJKgdecJe4TqYBPZ1hQzaeCGP+Y8k8B5byd
wtkUDh91bAPCGiA7YzRjyWG/Yq4soSb/bRSpPR3Jyzubwq5oBsnH9k1L2hVDinF
Yeot2E1Aga50ZTjfs8URVY4IEKKI9hNNUpdnqoehQqm54D4LFnJiujiVrS2C0HSj
Z3Nr9SjeZ7ymKzThhsHaZTRJaLoCxauGkf8EpeNJeoeNzae2Pvcgomr01aLW3M1o
Q3Vqls0fVsLElms8hL0Mo08XXVs9KRWuBiuXR+fsX10D1VHwqWJVBR/5w0GLgfn9
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

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAyAAACNiR0NAAAcE1EQVR42uVT0xbA
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

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAyAAACNiR0NAAAAcE1EQVR42uVT0xbA

```

```
MAGS739n03TpRw20dqpbfARQeJ0ywiwYnCtkDKnbcLk66sqlT+zT9cidkE+6KwkZ
sgrzfcqVmpL2jo0447gYDpeArk+OnJHkIHafTPRicIHaf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRUErkJggg==
```

```
--550--
```

```
--a64
```

```
Content-Transfer-Encoding: base64
```

```
Content-Type: application/pkcs7-signature; name="smime.p7s"
```

```
MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCcC0CAQExDTALBg1ghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMA5GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMU1QyYBSU0EgQ2VydG1maWNhdGlvbiBBdXR0b3Jp
dHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAOT
BE1FVEYxETAPBgNVBAsTCExBTBVTIFdHMRcwFQYDVQQDEw5BbG1jZSBMb3Z1bGFj
ZTCCASIdDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqlWALjj+gBUCfk
acKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID1B/wlbdmadXPmrsz
yidmbuZm0pB5voVQfiLYy3i0x7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0a
Gdmnx40G/e3p1fIKM0dPzZLo0AJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC
N5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAaA0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbG1jZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj
80eOr83zdw8wHwYDVR0jBBgwFoAUKTCOfAcXDKfxCSHlnhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCCsTKcFqQMPTryujRGzJdYA+R9eBAuDLsatbtKt14F
zkgRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUVZ23MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7Pfb5v94M5274XYxW2W4uKgd7QGnUZROsvSYkGiWdp1JhqXwfDz8
A0enITGXnoEkaFvviCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu0fQs
qm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBAQUAMFUXDTALBgNVBAOTBE1FVEYx
ETAPBgNVBAsTCExBTBVTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUFMgU1NB1EN1
cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOjFoYDZlWNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEWhMQU1QyYBXRzEXMBUG
A1UEAxMQQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWpK2af0+StijSNOR8K/hN8D+1078oullsk4ASvSwjsCNo7sHU
a4xQU15J06VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW234rTiz4DxmI07XYNFUE0ls/gkUP2Gxzyms02kaYWTut3
SryCqeHEFbZfKB4xrIMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfi0ucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElNAtJ7BtZcs17dUy9u9C0gE
yKriVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEADA0MAwGCMGSAFlAwIBMAEwHgYDVRR0BBcWYETYWxpY2VAc21pbWUu
ZXhhbXBsZSBZTATBgNVHSEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYD
VR00BBYEF1v2zLiThQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnWHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQBziaI2p86poGkjd/4Kkk0H
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZ1
RAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENT1sRx1cvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JckzP0Qhp
7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfWCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEWhMQU1QyYBXR
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTSBDZlXJ0aWZpY2F0aW9uIEF1dGhv
cm10eQITN0EFee11f0Kpolw69Phqzppp1zALBg1ghkgBZQMEAgGgaTAYBgkqhkiG
9w0BQCMxwYJKoZIhvcNAQcBMbWGCsGSIb3DQEJBTEPFw0yMTAyMjA5MjA3MDJa
MC8GCSqGSIb3DQEJBDEiBCAHedgXF/1PPCnjTbv4CNkH16SU0FJSW9ykndUZcVnS
czANBgkqhkiG9w0BAQEFAASCAQCYePlJ3K4FtJC/4snTs081+p0qEkpFh4swjQTG
```

```

WUhZHrdzb4kvHTCaoH5ShpVxZ4F0p1InabzulsB1P9m5xDvZveUMaCiC/qgSS+st
Kdk1sWANOtTgT1AAGs9og6Wp5Nq/evf8XIYdQV0ZXavzASl/yylz2uHTpW1ETxT1Z
fkgSqb8X/zRaVGoai20aVbmsIJFrVPIlkpgh+r8tbJ0m4791cCU/8lIdreynoUKq
Bsa2Y/uhoez/pldX/5A7Rv+JX2vdt71C2BZAk4166wvDhh1Hf9pVCWXdKXSh99c6
Do1Tzpnak0m4bKSzPMXTrz1p5GcfDz094kbNImkcd8yAdcB

```

```
--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
hkiG9w0BBwGgggaDBIIIGf01JTUUtVmVyc2lvcjogMS4wDQpDb250ZW50LVR5cGU6
IG1lc3NhZ2UvcmlkLW1lc3R5bGU6YXNjaW50LW1lc3R5bGU6YXNjaW50LW1lc3R5bGU6
ZTogbXVsdG1wYXJ0L21peGVkOyBib3VudGFueSB0eXNjaW50LW1lc3R5bGU6YXNjaW50LW1lc3R5bGU6
ZS1vbmUtcGFydC1jb21wbGV4LXJmYz1NTFocApNZXNzYWdlL1U1E0iA8c21pbWUt
b251LXBhcnQtY29tcGxleC1yZmM4NTUxaHBAZXhhbXBsZT4KRnJvbTogQWxpY2Ug
PGFsaWNlQHNtaW1lMv4YW1wbGU+ClRvO1BCb2I0ZXB0eXNjaW50LW1lc3R5bGU6YXNjaW50LW1lc3R5bGU6
PgpEYXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEyOjAyIC0wNTAwClVzZXItQWdl
bnQ6IFNhbXBsZSBnbVUEgVmVyc2lvcjogMS4wDQpDb250ZW50LVR5cGU6
b251LXBhcnQtY29tcGxleC1yZmM4NTUxaHBAZXhhbXBsZT4KRnJvbTogQWxpY2Ug
PGFsaWNlQHNtaW1lMv4YW1wbGU+ClRvO1BCb2I0ZXB0eXNjaW50LW1lc3R5bGU6YXNjaW50LW1lc3R5bGU6
PSJ1cy1hc2NpaSIKTU1NRS1WZXJzaW9uOiAxLjAKQ29udGVudC1UcmFuc2Zlci1F
bmNvZGluZz02NjpdAoKVhpcyBpcyB0aGUk21pbWUtb251LXBhcnQtY29tcGxleC1yZmM4NTUxaHBAZXhhbXBsZT4KRnJvbTogQWxpY2Ug
PGFsaWNlQHNtaW1lMv4YW1wbGU+ClRvO1BCb2I0ZXB0eXNjaW50LW1lc3R5bGU6YXNjaW50LW1lc3R5bGU6
TUUgbWVzc2FnZSB2aWUgUETDUyM3IHNpZ251ZERhdGEuICBUaGUk21pbWUtb251LXBhcnQtY29tcGxleC1yZmM4NTUxaHBAZXhhbXBsZT4KRnJvbTogQWxpY2Ug
PGFsaWNlQHNtaW1lMv4YW1wbGU+ClRvO1BCb2I0ZXB0eXNjaW50LW1lc3R5bGU6YXNjaW50LW1lc3R5bGU6

```

cyBhIG11bHRpcGFydC9hbHRlcm5hdG12ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5l
CmltYWdlL3BuZyBhdHRhY2htZW50L1BjdB1c2VzIHRoZSBsZWdhY3kgUkZDIDg1
NTEgSGVhZGVyC1Byb3RlY3Rpb24gKFJGQzgz1NTFIUCkgc2NoZW1lLgoKLS0gCkFs
aWNlCmFsaWNlQHNtaW1lLmV4YW1wbGUkLS0wZjgKQ29udGVudC1UeXB10iB0ZXh0
L2h0bWw7IGNoYXJzZXQ9InVzLWFzY21pIgpNSU1FLVZlcnNpb246IDEuMapDb250
ZW50LVRYW5zZmVyLUVuY29kaW5nOIA3Ym10Cgo8aHRtbd48aGVhZD48dG10bGU+
PC90aXR5ZT48L2h1YWQ+PGJvZHK+CjxwPlRoXMGaXMGdGh1CjxiPnNtaW1lLW9u
ZS1wYXJ0LWNvbXBsZXgtcmZjODU1MWhwPC9iPgptZXNzYWdlLjwvcD4KPHA+VGhp
cyBpcyBhIHNpZ25lZC1vbmx5IFMvTU1NRSBtZXNzYWdlIHZpYSBQS0NTIzcg21n
bmVkrGF0YS4gIFRoZQpwYX1sb2FkIGlzIGEgbXVsdG1wYXJ0L2FsdGVybmF0aXZl
IG1lc3NhZ2Ugd2l0aCBhbiBpbmxbpmUKaW1hZ2UvcG5nIGF0dGFjaG1lbnQuIEl0
IHVzZXMGdGh1IGx1Z2FjeSBSRkMgODU1MSBIZWFkZXIKUHJvdGVjdGlvbiAoUkZD
ODU1MUhQKSBzY2h1bWUuPC9wPgo8cD48dHQ+LS0gPGJyLz5BbG1jZTxici8+YWxp
Y2VAc21pbWUuZXhhbXBsZTWvdHQ+PC9wPjwvYm9keT48L2h0bWw+Ci0tMGY4LS0K
Ci0tZmNjCkNvbnRlbnQtVHlwZTogaW1hZ2UvcG5nCkNvbnRlbnQtVHJhbnNmZXIt
RW5jb2Rpbmc6IGJhc2U2NApDb250ZW50LURpc3Bvc2l0aW9u0iBpbmxbpmUKCm1W
Qk9SdzBLR2dvQUFBQU5TVWhFVWdBQUFCUUFBUQFVQ0FZQUFBQ05pUjBOQUFBQWNF
bEVVRVl0MnVWVE94YkEKTUFnUzczOW5PM1RwUncyMGRxcGJmQVJRRWpPeXdpd1lu
Q3RrREtuYmNMazY2c3FsVCT6dD1jaWRrRSs2S3drWgpzZ3J6ZmNxVk1wTDJqbzA0
NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2loQWY1WUpydzd2anYwWldSV00vdWxp
CnZkUGYxUVoya0REOXhwGQ4d0FBQUFCs1JVNUVya0pnZ2c9PQoKLS1mY2MtLQqg
ggemMIIDzzCCAregAwIBAgITDy0lvRE5l0rOQ1SHoe49NAaKtDANBgqhkiG9w0B
AQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBXRzExMC8GA1UE
AxMoU2FtcGx1IEExBTBTBTFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgaW50x
OTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjER
MA8GA1UECXMITEFNUFMgV0cxZzAVBgNVBAMTDkFsaWNlIEExvdmVsYWNlMIIBIjAN
BgkqhkiG9w0BAQEFAAOCQAQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQJ+RpwP0DxxzY
60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8g0UH/Cvt2Zp1c+auzPKJ2Zu5mY6
kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b9
7enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMs
wt41/0HJvmswqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5
chWfNEbkN6hQury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/WI+whUpqtQIDAQAB
o4GvMIGsMAwGA1UdEwEB/wQCAAwFwYDVR0gBBawDjAMBgpghkgBZQMCAATABMB4G
A1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUH
AwQwDgYDVR0PAQH/BAQDAgUGMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3
DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0F
AAOCAQEAgU14oJyxMpwWpAyl0vK6NEbM1gD5H14EC4Muxq1u0q2XgX0SBHI6DfX
/4LDsfX7fSiUs8gWVY3WqMeu0A7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U
8QzTjqB8+dz2AwYeMxODWq9opwta/ltOkRg8uuiVZfg/m5fFo/QshlHNaaTDVEXs
U4Ps98Hm/3gznbvhdJfBzbi4oZ3tAadRLE5K9JiQaJYOnUmGpfb8PPwDR6chMZee
gSQAww++0IKgHrg/WEh4yiuPfqaAvX2hZkPpivNJYdTPUXTS07K459CyqbqG+sN0o
2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJc
Ovt4as6aqdcwDQYJKoZIhvcNAQENBQAwwVTENMAsGA1UEChMESUVURjERMA8GA1UE
CxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZXsZSBMQU1QUyBSU0EgQ2VydG1maWNh
dG1vbiBBdXRob3JpdHkwIBcMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MTha
MDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTBTBTFdHMRcwFQYDVQQDEw5B
bG1jZSBMb3ZlZGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALt0
iehY0BY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LC0wI2juwdRrjFBSXkk7
pWpjXwsA3A5G0tz0FpfgyC70xsVcF7q4WHWZwleYXFKlQHJD73nQwXP968+A/3rB
X7Ph00DBBznfit0LPgPEwjTtdg0VQ6Wz+CRQ/YbHPKaw7aRphZ063dKvIKp4cQV
tkWQH16syTjGsgkLcLNaU5LZDQUdsGV+Sao3nBdWCRYV+I65x8Kf4hCxqqmjV3d/
2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGIWQVC
CpDtc0NT6vdJ45bCSzsCAwEAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQ
MA4wDAYKYZIAWUDAgEwATAeBgNVHREEFzAVgRNhbG1jZUBzbWltZS5leGFtcGx1
MBMGA1UdJQMMAAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAWIGwDAdBgNVHQ4EFgQU
u/bMsi0dBhIc164papAQ0yBmZnMwHwYDVR0jBBgwFoAukTCOfAcXDKfxCSHlNhp
HGh29FkwDQYJKoZIhvcNAQENBQADggEBAH0JoJanzqmgasN3/gqSQ4cbbmdj/R40
BEPr+gXT+xiidfZ2iLWYyTneuK6AchwkfnNv0Fb81V1iffRTF/KtmVEDMR/sYeq


```
AH83KM5p3e12lVh40HhyI0qNuz5oShNaACSioQ23WxHGvy9vsdVfnbhsplrWg9NQ
2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4z0I0vg6mrYkKTM/RCGnumghxwYTo
j10yD5Gs4D2IJCw+fx50Dxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDd6h
noQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk220H4ConlB8f7R7s1LM2cSYxggIAMIIB
/AIBATBsMFUxDtALBgNVBAoTBE1FVEYxETAPBgNVBAStCEExBTvBTIFdHMTewLwYD
VQQDEyhTYW1wbGUgTEFNUFMgU1NBIE1cnRpb24gQXV0aG9yaXR5AhM3
QQV57XV/QqmiXDr0+GrOmqnXMASGCWCGSAFlAwQCAaBpMBGCSqGSIb3DQEJAzEL
BgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDITxMDIyMDE3MjYwMlowLwYJKoZI
hvcNAQkEMSIEIJaCe/AYALXLZ8GDGBx2yVvHB9b3uwnKNIvWM0h3y2s3MA0GCSqG
SIb3DQEBAQUABIIBADrTK0kKM1vxG/qmdbFxdKDBjyUXGDa0WqjCmq810fRF88aY
37JerJhyUUsUPVCd73r1sjskMrxsA53c6oj0cSqj5PM7ZDhXCnGdEg4CiKj0An1l
C84LXG485qDgCJiQ0hMF/p/V2UguVdfVzPrCLPP2SCDP5BWfCLMII3k4sRVayUt4
FwlyLvsXcRUBt1LZBoJrYvfn6sNOAfcBNwAMTu0rx1A8ZAoNBtAbpn/UiTd6Av
YFcisTSEIuZ+oGRyvU3n/wBHp9bUonKVHuNYGYKgycuXowwVx3D3j6+h+XEB0FJE
KTaTKY4sz4qH+3UWjytqrEisWQW0JkuzV0a0dg4=
```

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

iVBORw0KGGoAAAANSUHEUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVT0xbA
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

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAyAAACNiR0NAAAAcE1EQVR42uVTOxbA
MAgS739nO3TPRw20dqpbfARQejOywiwYnCTkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVmpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--cf8--

--740

Content-Transfer-Encoding: base64

Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQCoIIJ0TCCc0CAQExDTALBg1ghkgBZQMEAgEwCwYJKoZI
hvcNAQCoBoIIHjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMA5GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydG1maWNhdG1vbiBBdXRob3Jp
dHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDALBgNVBAoT
BE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMRcwFQYDVQDEw5BbGljZSBMb3Z1bGFj
ZTCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqlWaLjj+gBUCfk
ackTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID1B/wlbdmadXPMrsz
yidmbuZmOpB5voVQfiLYYy3i0x7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0a
Gdmnx40G/e3p1fIKM0dPzZLo0AJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC
N5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAaA0BrzCBrdAMBgNVHRMBAf8EAjAAMBCGA1UdIAQQMA4wDAYKYZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGx1MBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDADBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj
80eOr83zdw8wHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSHlnhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCCsTKCfQqMPtryujRGzJdYA+R9eBAuDLsatbtKt14F
zkgRyOg31/+Cw7H8e30iLrPIFLWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTgt1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7Pfb5v94M5274XYxW2W4uKgd7QGnUZROsVSYkGiWdp1JhqXwfdz8
A0enITGXnoEkaFvVjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu0fQs
qm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+Gr0mqnXMA0GCSqGSIb3DQEBAQUAMFUDALBgNVBAoTBE1FVEYx
ETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQDEYhTYW1wbGUgTEFNUFMgU1NB1E1
cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOfoYDzIwNTIwOTI3
MDY1NDE4WjA7M0Q0wCwYDVQKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMQQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWpk2af0+StijSNOR8K/hN8D+1078oullsk4ASvSwjsCNo7sHU
a4xQU15JO6VqY18LANwOrjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzyms02kaYWTut3
SryCqHEfbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfi0ucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9C0gE
yKriVokFQgqQ7XNDU+r3Se0Wwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDA0MAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYD
VR00BBYEFV2zLzLIThQYSHJeuKWqQENMGZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQBziaI2p86poGkjd/4Kkk0H
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZ1
RAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEnt1sRx1cvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JckzP0Qhp
7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzuUaUblr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsM0GI364IOA0b8PSrJntjh+AjQ5QfH+0e7NSzNnEm
MYICADCCAFwCAQEwBDBVMQ0wCwYDVQKKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGx1IEExBTvBTIFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhv

```
cm10eQITN0EFee11f0Kpolw69Phqzppp1zALBg1ghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzI3MDJa
MC8GCSqGSIb3DQEJBDEiBCA9qnCv8hrAl02HDX00fVNCH7ucDtJ3vYdKv0vdCnWz
SDANBgkqhkiG9w0BAQEFAASCAQBP4hNammJHK5hpd7ha61zKahf9hoZZS6TPNUCD
p1GKSjV4XN7pLxDu3wXAuzon2zV0FxeA1MG6gZgdSBY/5nGivTc/NB0mXJt1NOUV
6b+IiQ1ZgJcWG6R2Pi0bE+NfadPhxvekmgCNTNl0jHQkXn+ABsto10Z+0QnY7Tpe
6JoT6HHamKbV0L1/gkEEQtSv0kaDaZ1lA+if+Qkb6xus1QA3FGzScPpcryTvups0
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

MIIWjAYJKoZIhvcNAQcDoIIWfTCCFnkCAQAxggMQMIIBhAIBADBsmFUxDALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBtIFdHMTewLwYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAERACKkMFfCQBEXqsSFRAOfaa0UcrVI6fcuB
nsfnksstYg/+DabeHHBueVpIuTr5Zqtj8kQMK8hWRoA+yVhA85aZaRadcywsEn30
oTc5vD6m9DBV0IpK2vhT+aYWJr67cfzlxJgVdRi6Pf+8g3c0oi05fMA17pPCUHYe
//VSeW3cdaMGgaqFamqL+p0i222Hp19p+3Q6zYRUJ5Y1cvD4aOKzaxw0RcWvFg//
KYuy1q6Fn0utZAhoEfnBtEp71fSI5LugUdj3tx3NDfrG1MLJHbBsELqawuWrcvmv
```

BbewMWR5BYc11/DQgbGFSbB/yoqBPkpC54A7PP2MXfb97SEquY0wggGEAgEAMGww
VTENMA5GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGhmaWNhdGlvbiBBdXR0b3JpdHkCEZB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAL7P01rb8J7CwZ+vEvIROxpiz
on8lc1VRHaE2tthLu8W0ekoAyQtPv11edZgydCRbXr++xY2Cv0iaE3+jdWrn11am
khzFkHpFEna4o91BHoNoipvl4vuLp7B+s2Dxymwctv1sZYkcHjVC8EH1SH/43JMY
0TJkBtk01nLDWTVfVePC/ydbFaXqtgN69SiN03GjaczHUTuZbKJX41SbGqk3XhH
iscSiRS/QIDk9arBEP7V1r7WdvVdFAfPEYZvRRrogzZJ5TE95Aes78+kaQ05wJRq
xScdSgw1M9jchURUtZ0kk/pGvs2aa3oNtkKj/70MDi64SsWwEdiTVsHob5foyjCC
E14GCSqGSib3DQEHATAdBglgHkgBZQMEAQIEEGYCTS4JhiRx+ufWgp0a1QiAghMw
GgBNjWrIh5GY9E1Dx5GWJxbUaCm77I6Q/NAYPVQaM73L5yCBHNEekbAFMFmZF8k2
bYgLyBCp2PcL6BhSAQIFAvDUN8KYTKHYqaz0cwK2C9EgUi1dBtQ7VB+xPvTXZwSx
0sP0iv6ke02FYeIDEnT56jnD2b+JkW4/dwsqBGvju3dtPsVR6bIRHICTrk0thCphg
0kUPnjefDmQh0kCkp8XuN6M9ZTwamzR1gn4ZLXw5LArZ9h7P1yNKZvdoR6D+510
qo6IhBR1fmi+uF60m8b1LN8TBJ9y8dt+UPQE3XD2d/r8YHvritCJD1hse56J3WqG
AAU3dlks76PcxUzECQPmVgdzFWYmQ+ygCnxqIWanRbDs0Y9DG0F0ozWLBrg0yTsT
awwlH8si81FJPUyqiKRSdhufVMHIQT/rySSmfB2o6r6Z5p60x2sqY5csYemPrFq2
YWp5wCv/nLTkcAbvuCohR22XSlz9n0ihuTQBh3d2vDsUQzbX/7RrPNPOKYLPNZXu
00XEK1YC0IwMMJ4CUGtjg0Ma10EpeePuURmXzQHg3704w4ESSiCnmVEVQCLEwgQu
8A1r9P97aQaVV4vvKEtLv2/RpRr5BXy28Kcer/2HQFUJ9nBpkJf+ItZBic02cab5
o0JelZdoPL6aDwy4eDLVS+SMaj05bQLYMkaTYfcP+nUdYZ5gLU9qBcqRtIjQ5qdB
WH8XhEEiBPZYHHvBidaK9EovTOJ4touEg0G0iaWoRa8crQgryKR/cnInZ1pWpfd
kmeJ0+NJSfst0LaHhk2x1fiq0KklryMAF90RN2iZvtb0dr6zv2iR54801XuN0Q52
ZmLQnWdqj2CSXvXi2kPHz+/1dn/iQl4oXAnDMbvm0QcJxvflFg1zQzRsTwvoyiRn
RBUdbsbGBziZGqg/vMaVnZF8yU16ADxzqIf5rM/iV76g7sscLhX5Ewcj618QK0gq
n3nGxBd2xuEuX0pv9tS0mRi81qELRUboHV3/HhRn1TLs699fLFOAJMcke43a0jHF
NOECszVjwdXfn9Jw1S6ZwWGqtDuCB4qPGjVttiPMn3iWiBWC6y5mtgaJBBacGMaT
DXcojNrR3mUEwFmWZKb/3cn2mzmB26JU9qbfyZrFxxvXFPF0EYzqREhSkQLvwnqu
IqWm1ILBuIsLICSURJw64e+k+qBgqg7lKhTywECC/0D1bjKntE7R7eeUn5IGs4Xd
dLdr0f/UkDhIqIAkn67CnIZi+miCszlk+l8uzIAIM6Vux3a7rXYVcJdSQg59tWfN
mmqdx9BT/bZok1Ijo2qG6JI2EIIjuvD8ufW9LY12QCNuZ+Qn8S5b4gbRDKZGf9fG
vD2G96t0C8QpnUmVn4dI5B4pLXYo77SrvMAY85G0tzha6HCJdIA+5SMxxIF/Qpba
TBin02Z+4dxTJvbIJpQzZfMUQP4DCJxphpaALMiBxgVMM7FxPn4hpwUUAiu8juQP
GRh/PRKTb+ZjdzysiCYBPULvd5B0/aM8uhu0Cq0a19oA7b0Xznd5PyJ0Brkac94x
qXCwhwu72jYrt0YFmL9RbpXMZSh/fTGq68NY7j7NOMd1FS8P7Si1Tdfc7Q8fh4MW
w/ODenQPXTRKJ8NTYk7LntGM2NKRUS+e1kjaAwCk/F5fRieF6AkBvKp/vFDQYTui
oQM9LlGW85TIih0/WDWJYzRQCoigVVErwppjuwSDztFtQrtfCFb0Vx4sAfbYoEt7
NTVg9V/elgTgAwrzowT9jMmZIDnkAZQ1Y46sD20BhjgXU1YwWSIhKyo7EP0xsxPX
DTo9fY5ybayhKQ59gQcb0mrwZ8qC95FFxpxA0S9Yee5++j5+RCSosvYIHw5Piv
Rge1Wm1U3SG0BYQENLqYB+G39va0T5yy9lusVMiFnJ6CVGGNufLXNjpCXANQLFRX
shYBUoUMwt0R9kpBDDg1tOwqHWoh0iG4X8Iy+cLvna2thFv8u94/Riq5pUn1sbC6
wxu6y0vBdMLx0fm0fP8xyPnBCiG/5WeziARqdAaH8sGp3Q7qc/YAprlIQevCU2b
01Iz6t7dLve9HyY1vIv4pC1PWi6AZg/un4Rtas2HuLAndrNV7s55s0FH4BvdGP58
3fR/M9ITOVjyiT3bUit+5qE7MvpUqdxfsdC3SUApxFJ17khGiimV0gC+x+8YTicE
JebKrihVAosyVWVZpjCIa4hjdMpVgUutyEgVNov9XFoWcNxMb8f5IAgXvNKMsvpN
FMoAfeT1MSj3tM5jdWliV0P5tU8Wt1Fj3hxixZPaz+w2Syk0rHoyoDjCWpXifZ3K
CVgGghueWgLGlwuja0FSkvZbq1AiVy6ebtbkx/q5o/jh91oTa0SM2MupcHrHg3Z6
SB6ujw7B1BXWqcNlMMJQS6npXCWslleg8iHQRdTuDGabxuBJmVf6I2mg8Ev+Ki7C1
KAHfAAhHp1E13DXf+E8eHVEPIemv3YeY3ldBVI93+T5V823yYwqwk5PfWZ+fPo+7
lBoq8IuHDu0fPwH21b6iNKE0DvokX0PwkixLB7KpMp19niCkdVwtj8CJJZLD6CSR
ctVnGtFua77w0MEu1wv1XWuWz2IT9a3aKGyciLrgz/CsTmJKWSIoc/f+u6EnPf23
hYmPMxLI46I9VQVcxaX5YD20ywMxTmN2fkGQdoxya5pAhN75+iBeYH9J0+B+bYHo
HJX9UiEs5Ja6vu37SVje6RqchkLrrXLyock/utB0pCqsqJaZoFaVC8M1T+jTw8ro
+mioqKVi0JeH/Wn3yhCEHQ5AY5n5dB20MdPe9BZQ9zzr/WdNx1/xs/FpRj+ggpq1
1nEerBbzG9uJQ0neKqRLYActvZ3zhe9X7S1/jS9+pFLLt02tnRNe/ed0unZhrJVt
pb19s+WtaDvez/eRUBjkgdj1BFtfYtFtcldKJBjL09KiIkLecj49cfZhr2pcXeZS
pnMu3vv1mjapHABqIvnEnf/jGxGFIiWKP3jeKjgjuv7580R3YpNQ62upOe2MP+HAW
3nhYYNrlXLD1eFT/TTiFw0fVpvrVuL3vFfJBXVFWyaokM4/sLN4E2EfJ9KdgbVBS2Y

RmgXH3/EBYjJzicoVcvb799rXkbFu5LymXGteMZ+XeTDeYkLrx490E4FYmnQF1QX
Grx2cqtzLPe4aVFekZndq0zDenNibLpv2PGL1cJy3mL/FEM85phjxe16wXM/aPcD
2ScKzC7eSfUj01K27nswJ0FogQQv4Q81apSqaVt3884uQfpz8j07Nxr7ZfknpnwF
AR208udTix02yEQc01YEI+vTo48DiI7bHVOXB441M7hSCaFyqAMuyb9JXyZGVvdc
v9+mxvNg60bXh0kLwPxBVfQ+TraGKGvXMBI29/Lzfgssb6k8JoxiBy/qQnBcLZfs
bCqggRM2WDy0mApeyAHBwmybYS111nosIGHntnpaPgSRMIcMENNZEpVdWLZ0cmwh
fEX++diQFQ9AwzW3zygnYAk/tZSXVe2wUL9ojMRr7kLwUz9n30ZLF3u/4UEra7bD
XRmtTO/UmuN/d16EqBN10gKY96buiRcgAAigMzj+D5VRqXzgj0I0Qq+gu/eXkzr0
tONfZfuovND1+q6H//f2kDRHbj0SXz90SWH0txaJ6SJBdX60MQFb6mEWJm8kno/e
UpEXjHzTU2xyum8qoN8XdaRBevrBhyPXFpb8QEVD1BXR6ehFockfbnaRqHVastva
Df6/nos9E7ViCGW8R3YoJ+2qfWTk7RXjmq1ykrdbQxMyc0XyRTbLB5ur0ynIif15
oQyz3SiQGSLOaSD1Z501Yty3zTen8jMlpB0r9KXFkgbbxNY1X6nn3vZ5ZuAl1M/
iwtapGThkj2RnM0ATEWG9SQua8FaH8zUv3fGepJ37VMP1Q43eWhZavwZi1/fs5vG
UYCyqxjhNXtwSnhEGHI2F4LaffYeim20Wt9HiXZON15vRpSeTWvTGOUGVZWR0zx7
0gIeKe/ksjcILJuzy9fKQ1JjsmURWQfuKM2vfrFGAom3jxKBNDDFzinkL2/kVpoz
rn8LpukKE0ZNB++ALIGV0B8L4zNDluePDTYlojthvjJUN0+oU60B/iYvcnH0KXin
PKmeDe7g5Ywjx0Uj0nuZEwa4L7ALCG2WpmnpMOT1RkHVpqN+29PPQ/Cx+JpGmX0+
uFiHQN+L3uk74rQwJ+LUQBGDrRE94GobEN/sWgk416bQrf7S13Af0QaXDCN9d2Nn
ebzYvxhxEkpqVnvjvd1Vr3ZT7ECz0FEA2hjK8L12oJz/zF8DXUhSLXxXAER3Nf5n
VzM+OfCpigIUezk5QN3r0sHD1mWemOe6JgXnDu8BIbBN6NnxFXE+rbRV71vd0APE
q5F0T9a0o95/cVYBcLvHw3QQcp6yP1Xhulaq1zZc/N1482qDNddYDPtUDaa+g7/X
m1+3tK1myLIBhvx80RgdyVQiXmHmvjWVv8qqSmwrNM7rZNkWo4FZFOYALreVhXHZ
T1bgmQZQ/0ydwRhfpWT1HK1AH4UzUTWKjFDH0j1pZGqtDuc+ghEboZxHdAI/xrvy
ypU3OnP5a9Dvdx4B2GuKHbPpN/yY+jbvJdbb1DX0NR0cVqC7JU+mMXyFRkKg6yga
L2KDhI0VChXtzGUGSR7wnfVCPBW0pmi959NSoSRdVnVI6hrCqNopVPvRh9bAtdor
+MoGi2gxmKCLhxY0A9/6VjZnBF498RrKSAh9EkHZp3Wtiy5T5779j8gHRLwIpeL
YnORqbFW0gcWhjKwL8BoXT95S7rvHWUJbwFXMmZFD7fVJqD11auaeS8QNFPxE0IW
91Z+2yidE0MdkfTWWS3WTFy3N4DBYP6JJRIzHV9bYk18ASxvNR7sGjKTsaioRble
3WaKwI7eszBNvgEsRntJP9PYD31eXc0XXbsZZmUgbu+Q0zIYfrmJwo0wA/4p0jtm
VpF0dAW0vwOMygs1jd0H8MFBbVMsu95DiM5Qx7JTXNaPAkxKSVrvmPCP11yH6s
82Tkf9D7MC91Ty0V5g5wqR/aNXfHFk31+8tRi/jhDAGcyY+s1AUONPaNCIm0jfe1
oRPRpw6noLVW+0X6JuZ+hFoIvOv5oY4mhvXmtm0rxG1/bI+5WFHRfqD3rQNX/RW0
WMepPlKnRq1yNCzwKNrdPf7sus1MHSDCYCuGFUawRBZnPtd0wM7G4kPiVh6rm0W
EQji3yT1bDp61yVbw6TN0SAhcAzkDwrBNiGyDCda5naYnnYRNE2j5KkAcFtZv32Q
KFVEAl8dP3+qeuGiNJVpiTNaQMtMT+Zm4IwgHHn7aHKW6su/jjc48gxLU+IHSR6
iW9IwZxRvCWkHLLKmUutBN/WkNMgpt/Wmc3waY7LZiFhK+LCXHK1dLbyrkCdSD8DB
iYxV6+MFG9huPj1JtuonFt6DX/PE2S7pgLeTFWDwKxaeNSd6WGVU6KiEpeEgDPmJ
GpLAv1ow/G3Vmv0GHm/oxKd76uY61CosCH1EV6KqSX/c2YA1IVcxu6v8kaPXd2B9
mbafIPVDfEr8ZOD8SswA9jxaf3ZCmrYHhwyV9FSuQn8BNBpYqaa1++YOeOWPj9tA
7qTDNUJNgc0vKa/nVWPuSVogfaVn5gw/byuN1PHmdLEdHUMyOca14UyJ28nQrvYR
23WPQKmRT90ASsEMm2UZzB4+yf4/lzt3p2auEks2s3GM1fdyUm7PHu6tz/Kvpvy3
xE6G04qV/cEK9600jwfonvNgf+LV/06GV262QvbVj6eKnNVoe/7qws+QJNuwjqmE
xyOt/dRjTFLomTXFAKWpnXNTPnzUTyM4GG31We+a0k0zvjhC4dAL7lf4JKYqP6WW
wKxjK46KQuew81k08Wwk1VHW+D4D1N2ynIbDM+q8rkr1JNNvIHxw5BA5CSWpsxnu
oYR/fpw6kSbCPG07b2tWVGmTw3S/Vwy960Lwunw4oYyaaBgenFFBgDzicgiyExtP
K00PIr3LjEXyo131cLwSbjCNUMt7FwPiB5/TFQwVmtGq5t3uYL3ei5IgTaozbk7p
04bVa2QJQxK4bHHbsgZ8/Vd2JXJJdQ+I1rfC0F6PKFqrfhDeujsF8QzZhvn8M2qJ
y1NPENK9Q4zb77dYvDUXBss4+erFM0wPesScHEbQPh9yyu2zqskpYQMrOqMPCjb6
y7yKppG1p0IrMzpJQkt7WP6n68nhZAlkEoCu7XchopEq1TmlzFVJ0F48ijIXWHMJ
PjsMWj2eh6goyFaAl2tovcyH114j8vY3J09ACyLytyns+PzdrqjuZxJQt8wZmd84
axs1klG02AEuAehpsf7ypMKCB032kirOMQSYZc4QridRDU5J5TTxMsxz8vXtc748
8fDkhFFq5Bqf6Weo8YiFvspF/Vvow6xjGpcNK6DMgxwwwUb92bxHwhdlyVa90lho
B1fxiQkaA+0iy4bdYXuDoLHd5p+T8SipMorXJrHe/blq0wNaHrbGSCje2SXQBqB
+cMVUyvTtEsA+hpI6hI1AZutT7ZqrviMGafD5C0078+8okboTHysqAIH8WAdDwkv
aXylZnqk5KEiW3eNjoh0Q==


```
3A5G0tz0FpfgyC70xsVcF7q4WHWZW1eYXFK1QHJD73nQwXP968+A/3rBX7Ph00DB
bZnfit0LPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZ063dKvIKp4cQVtkWQH6s
yTjGsgkLcLNaU5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKRu0BX
nDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1llyXt1TL270I6ATKRGJWiQVCCpDtc0NT
6vdJ45bCSzsCAwEAAa0BrzCBrdAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYK
YIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGx1MBMGA1Ud
JQQMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQUu/bMsi0d
BhIc164papAQ0yBmZnMwHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSH1NhpHGH29Fkw
DQYJKoZIhvcNAQENBQADggEBAH0JoJanzqmgaSN3/gqSQ4cbbmdj/R40BEPr+gXT
+xiidfZ2iLNwYyTneuK6AChwKfnNvOFb81V1iffRTF/KtmVEDMR/sYeqAH83KM5p
3e121Vh40HhyI0qNuz5oShNaACSioQ23WxHGvy9vsdVfnbhsplrWg9NQ2WbpCmK+
2oMh2oYl0Z/wvXmT9cG6jbMvcdH4z0I0vg6mrYkKTM/RCGnumghxwYToj10yD5Gs
4D2IJCw+fx50Dxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJdD6hnoQ9rNeo
zIcBVyybQYjfrgg4DRvw9Ksk220H4ConlB8f7R7s1LM2cSYxggIAMIIB/AIBATBs
MFUxDtALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEyhT
YW1wbGUgTEFNUFMgU1NBIElncnRpZm1jYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/
QqmiXDr0+Gr0mqnXMAsgCWCGSAFlAwQCAaBpMBgGCSqGSIb3DQEJAzELBgkqhkiG
9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE1MDkwMlowLwYJKoZIhvcNAQkE
MSIEIPc7Pk9KNPXYMYThSP1PWV2Qm8CR4vwcxnqIo0jkdUtMMA0GCSqGSIb3DQEB
AQUABIIBAA4QYIyZPmQpKWNUHu2nJc7Fr10h66z992rzH20TpxSHehRBo5dJYSqm
9p/EOWB0XL0uJ8s97cVbdY11EqEjx9zvp1kdLtvosuonNGHmQ1CPVKSFfpBvq4DV
L7YcZkAQgXujN2Z1F+MD1UTYo6reDa2K21zPqa6CJX75zersFb1xS3raFRaNAspW
URatTpJpgf2E7F39o78kRGsbUxurtzm5QTNHIVAqjv4LudNSGV0H++VTmkMR5gLJ
3Xm2E7tz/TLd1GDi+167tYni3f+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

MIIXTAYJKoZIhvcNAQcDoIIXPTCCFzKCAQAxggMQMIIBhAIBADBbMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUjNBIEIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIEh7j00
Boq0MA0GCSqSISb3DQEBAQUABIIBAHafgwK5Dq1Mk+/BfVcTHIE/bWks0Cdg0uo1
pp13Qdi238REiGs0NqPHaLjK9xhjvTS4pSV3NHEbKTVZpQurzaUqIXL/sA12kkn
TQgbJiemZq2HXKI1feGM86z13FYWPe4g42nffZNi5kErmPI/IZX4CuJ2+6Wy8Io0
tZ3C1vLg6z4V9mialF6IyVDYw2VZUIb/r3I4SKINANa1t6wKHeHTX6TEJx0v3P6W
kWUwpPHGzYXPNVKX+NSLxGqX68vTYOhg86Q+FeKLNHkutnQD1fNU/ZBn/iidZt3u
aUbDpByaxv79j8QpvCHUXbygTIYENnc11+RcJ3WmkCKVkwXG2fswggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQUU1QUYBSU0EGQ2VydG1maWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEGgEARW1p7eiEdi69X6DKW+FXzEoc
E8KIzTvIpU++vNLVzq+29VTzdjvBVcg/8F8L4BNCIPWSgz5i7Z0o9LjMCw/mHo20
XL074me2zAv3HeGZ85i7gIiA/lsgIb3f2Qw/+8gQVAIKoY01BmpocBF6EGyEciU
SWfwp1qJE6/YWhiFbjcTIZYj6UqGy72AkiqGKgCZ/tFWWhMJ2KKZbm8t5rG8oC8bD
dgjT2PYo5by8brJohF/zTS5CucfLqqWpA7QtHLHcAeU3NXqVc5tHyGZy89KDPeii
xVCxdE9Rs2AurTjT2/98WF5tTEFOR6LeEdG3sv0zmMd0xWEdwP47BA/ePsS53jCC
FB4GCSqSISb3DQEHATAAdBglgkbgBZQMEAQIEEILWJEheEd6fWe0TTJf9Jz0AghPw
6igc/NoE/0kf7HXkehS4/7Vs85BKRQ5mdxGN1WfY4nFcchHVWVUCrPXyC9mUC6hW
12YunKd+i/LBUN0Yunvny5igqNHEUBzMQbJmPRxcgClqS8zMokqB0+kzGJMK0nC
0DVfneVaPAldMvZhw3BsbJfGaeDVTthp8IuR4PgDCUEBL4QWCvkgD1NquACVYAD3
MD7PSziVb2tAvVBBpX0Z0kRGc3bQm+IhZWRA65313297+eYKfmInlt+j/K57UBC
i3tnWaNei+ftFBPVpbnMqXm3TbBBKzuWtV8Qs0KZFddCtgoZmjpeNPAYMUGtn79c
3eq6ftZQPaMKCY8Z3aEFev7YfvcDCWRmsbtGndyoQAr0nc8BU7geuHD+MoVIVu07
F6x/hxZyJdEh1vfLP8hPKq9X11gwa8+qq1M92oBxT4hY96rMOMu2dBNvF3g9T16v
g1LE2PJs62m402XEYd05F1WzYzXjP4EzF3u171duDsdyrbwZBq0JvMXVffqEmfd7
YfiLMvfUihHpNBFSktgPeSqjVZ7WN2M902CzFa85Z1CcCTrqtXTbVksUYBfixU5
mCkZimMFvH9iwnSxxqdovNq60ojFiVNUH4SCKBXDHhwBrHR0UqZ7Jap3xQp1Yp0P
2q9owbJ9irL/2oX9QGRG/g2W9P0Q2L7+S912QWWpn3hJZwZimG2LebRrIHEVsHhV
nQdEst7LZ8iDw2fDTd9cpSxUjV24LauODLxLHf02NWNtttdykv4RZhrhAY00IE0H1
YuEhPD7m8rYvhr5X16pDEFVGPjKAE0VK9CQKdmYxjF3nJhL9EBzozTWWkRsiNgyU
DJUKaikV/smnYcwU/0Y4Ug+AZdLhx9fCK5Crv2MjXaB/8btXoutyKU3o04ABVtQ
KFt3r/CkYJvyfZQTm1hDLdxry1L/yX78+pFmnsLRSKdNp+W1hz3GeeI/bDZzR5L3
ETECwXcPjh9uqrgM3HUvKC9HHc+fUXKRQXqGMXR1tvA117yW90N0dBZBW+Aa552x
cSSr/z+jQJy6WSIXiPN/Lme8SyK8cSMUGRW44x08jZ17FRcmJwbmET6n/AxX4XFM
MBAJ/Cln9kM0cnC1Aw52X0571xKOS1MNQb5LRr/a6RnpVTTTJpp1BQgjc8tjQfA1
bL510dPFKq2o0p90C3xjVa0Gvi3Qp8BBR9LKfwTUZSEsrcNhYm05+0iDfKMaD4nX
PJPd47XBR+MuYHRVU/7LYFv9KmhxDsemLmq+8W23AYuPXGoodQDB5upJSoVj2gJw
j/Aa6n7J8NIoNr0omfsavqZBiAiNSKRBNaQZ45h7hkYB400e13dMgJNATAE8/5d2
gXV6RkhCxtFQp0ykzbSdrLCVUSW35TtiCzGzEsVUQdJ6ZBy02a2mXIwWDt98Hf3x
Z1pHjfiX1FKG+h9f2S61xkNZjIATawIwY1+yN246yvdfX4TugEtISyyeu8mGlnkk
md6BJL1fGCapQ8B2u/KFswjNqC9orJAs4PZAYwAMJqZ14j0PbcwjD4yVwxwdgu5W
uQZguFHVQnig4jT35svTsNmMei//0WYrESkOLT+8I64TuBpP9Nt8kwFbfrJA3MAS
mmLKVZ2t/U5Ff0u8hemprMntiAhNGBLUKwwbg2q8cQfZ1XNGyZv006s/9dVX2aTG
ExNCEsfprvsXrgHNT2gFGEbvLDJFEHCW1ozu2GucDVo/AH5FAcwSMcyWtFvTkXHV
W2gGKYQd6Ap9f1py4B2PGQHdlinMADUxmaFRsD3fYbG2Jkh0aSzAfJ0wjXMMu1dF
AYyUmSj/hCCmosqR0QG7UJWQ4QK2S7dMFSnNt9zaPvKJMwPmAc80TzaxrJxJ716H
DJ5HHAztZm52fGYRrUyXEWYSzIjqPkQF09pwFhn1MNDLZ99D43VFUkoBeHHQ0Aswh
d+Xp+jGDwEMR62xQhIdRCuR8i7Wy13+tCdZpfQSvMcFTPU2G3/xdvhDVJ3sDjcIf
7gLQG6/uQmevrL6XdUNW7zI4a09e/knL+trM/847NLjN0RRTABLkTx1TxgJ9ELcw
yx2gvuhvKSt414/1NcnbBZaW3yfa6132X5t5jY9djW8M6EYLN5HSjy3aIJ8fiaZt
T9kKm5uSsz+7bb8TSc8uQ51HzAvctgM2k56zGVQnzWkXR/ghaIJnp4ekLG1GZeWv
Wa51KqMyvIM511VRL5Uvu0AA2T99A0Bic0qWjuXpAjXHRDUMKfR1vSJMcxim228V
d6MfqcXjJEFsH1SLDA02jSafk2jAAPBZe6Dwx42bw1/w3MOGJv+rPAI7tVyRBqD4

LqD4sgT7R1N4z1CPuxWdRTCmsSN8rqK11pzawJy0wElyimrqjP1GLFGuoG/s+VIH
gsRZGGeL1X90eyfgFeFb8EAiQ8VcCr5yzQNL8l+E7CJYCbqFH1HK3+aGqYhg2G1
kYEgcMGS2JVQTioPlohPB9ZVLPmcaCAzsPeZ1qAgkc4FAMHNh60ad8/ELCt1p8Mf
+ttz3HVZVZkIHbqjag/LVgAGbi2WMvsb1WmtRCEAxzQwuuxvdQ3SrqiJ9QTP0DUR
hpyIzIP7G61EDnI2HPEq0G4L9LspOf/MUZTtYhnjKxRrsqUDVJ4UhWWVeL/rzEOI
/mflTQ+f2odEY0WLYHomhyd23SnWnq86P28wVgEhXBTNFeo+BkXnoenaJyLmjJi2
7Hx0EXM6gc00Y98wt9NQxaLvJ3DPtCQpJf4vQE2fs0b1Y4YLM5z/sEQSmNhxjRFr
RT014S6ng0cH5iqdrw0+e9P7HXZahp5c6IuD0gG36DEM6NFxzy7mSDUsKRtStZKk
TQXe1W9LeUo4Vn/oHiR4cijQJ65j4k90FTgfBMKL58z0H82fZUcXZIHJnkMhvjmQ
m8LZLU7n46KC3sAzVJg+Uh374iwqsrNYXqr/IjYyheXLHxbFV76a7RbknTFx376z
Y84Q7NTD+HoydTwtFd7WyaJy8lfcJIdMi7tQtKvrrSZXGWQEHKTA4TmCgVCYRks
Oo4RynbaFbX7Xb50No8CUtSsD+fVyIlq/fS1hs8cdpxzfQH2K75CdIQ2DacPTVmh
o6MIBVAmDy8y1DAw8zJUPH5p8mS0vbxRX0y5Bs5dRM7PT9A+Nf67f+RF5xfJNSi4
Gwj6cU1hBN4Uxi8Yre/ze8DgaTb+5b5vt8pTiNpSvqqa0iY1o4TQjQVA+wZ9FZpF
ha48nC9hmp0IEAH3e10Dip2kuAXx1J8tUCJ6xvWHBfxhYjZZoZfkW5ANh7YRNDmV
cKjdpWyLak62aERncU351xpg/0HM7fTlChFB10PBPIownbpWSzuzPFKslu4Maf9h
PLO3jTcKPlw5Yp7JL4ChSqCLcf9KK7ava11UHj4oNgnphej18ncFAWHvrB3CykN9
xD3IPjQmpH1woMkNspkFHKlfq6jiFcuVBPPJ1AFawpKMwrf46MHOFqr85BE5JLXo
ez/pM19tItZy0sm6XU1ITumIX0EL1kiVr5WQaC4eC8FEd8KDJfD+sOq7RGaRoIQZ
D8vGB5QrdLbB2aNNKxwyTbK+P7p+F3Qy0BVidoGk1J16sEep2Sko70oVdJCFd4bm
dUwBlvwXc006z821QkfmdLWpuIEIiqB19bEtxyEXyVnt0QG10hrzJqjY0Q8cFhMs
exyW0aak/pOSPd7f81azE/UmX5U7b8s1LwA54N7tqqjoMCLXyQqqaGndgfU6S5Hd
CIGHA7KT1t1r64H1zhQ0A/iqCrv3/mOdJtx5voztQSqlZqlVs86ZhvW6BigqxyL
oqI52yFPMmk1oR+QkPrwC17EiSQSLRjv06KgdYDRjBqr2mgIOuZy0UrZ0LDSSJv7
hdV+TYLwYxb4h/q6sxtQH5vvyzBshNBof84PK7/xMMw3hASQLEpVZJCv0k/0pFuB
adCXsux6Op8nSYcmfyN8b1vIAPFP4b/s6uE+R9beTss6tWzZrk4rx77qjB0dApIA
PdbtndybZvktflfSq7ftwgiKERN8qT/FRQZVU9Z58MnVCTb3ep3MxTEoiVE47/sg
V5WZsly6Pm87XFCZxGCfZvyePGPU6iEPcbi07zfHqk+tH/D7ccd4x03kSVF5S+qX
V9DC5/eiKXDaWV0f+KyhJVuoNztErEvDfuPIqBr8gL85kpcqi4fvPrP4xziKK0HJ
X7hoc5psA27J00FbvPPPwNCWBcQmjZswIqt/s4JwiKGApZetv1za18qHieiLS51F
CJGyeQvjdSm99fRGf+d0rypeMGoTPKBL5KjTF6ezt/H3b+BN2A7600tphv8YHsa/
GhYwxmbjLnwCNL8bKrLzR211n8XPZcHcZTOKwvuT3/jImgTW47T8tBjP+uzsp6PX
a+I5HTxkw8hhLIN7sqfkzp+zupKLHjHG8AayROtkW8yFNViDZfxWI7shsj0HJApf
6Nkaauz0bUXYuxGdobMWAy/50ggA5CKS+SEXRyrmLL017NAEWBCqIODK26zZPQk
TABDscOSDevdMXiAKcfUcIJCwZpjUQ42x9yJ0Byd5ood2+489nfz+GJC2y09ZgZe
SWP1uUUs8maUPglQA8IVik6Jh7hijmoKu6ZMxM0Vg64bkiAMpNxFcZnYQsr1W4nY
6LsHstDs2z6+8oz/1ff68Ig1i8i1EzTXLRF5rKofQNMtBruuxD507tpeXDhJ2EmA
mxkU5ubRf6Ab0QbAJ/FMB32VXpZnJHt8dIQZJ2HN3dq1H5I8PDw1D/kFuLE6xyYY
PMC3an5+q5VrrLzqaZ5w5uZAupJ+1dHmT2TxuySkUJuwf0HL20d2JVOHmtpJmuZ1
SEUU4EOIwDzS/NlqAVWE1N4r5MPWotZ52pzvd2MiTMwrtNDE9wZd+WDOX9evTr6Y
pYOS7XW+NYEz/jABEWJb+Vw9gOL0DOKhwBjYdnUnD5io7LkQsRfvcun1vHIWv7f
Mn7MdSgnmTu7+advjf0sv+SdHYOMPdCML/QbNQU7d1DP6gv8/WeDoGFvInNRidBg
Ftwm8ChrZXPiEP2/3GPxWh8SS1FyafBKwtpUWZV3pb01+9Uh1DBGX/ysIKFD1/Xd
iSt6B6ZZARes07sxeSED/7yTHfEb9kAw16Z4d1XIyZ9y8QNRATI8IC2T9PHt2qVb
DDNR7JU+UH+XsPUvqo1v0vDCkk6KfrRKiugEfgKZHPC0YQsVwh0+Nych47I7DxJe
AHJUdjh03KjBHa1hbT2EZexcDPCmbiQ0dQsVKyGSMFTbupZ4jGN2qMu1/2nfB5Ed
/1EK3At02aFzS12eIEeEs/kyL8yJB9g3MAae5hcH67tvQ1YIpZvRtKHbaF5n0r6
CxznHv2Iuui39a/FE+tpzeutxSg8gSmu7RuyYtILhNRJgKhYfBQFqJKJZzLSbgP
MZBPEEymba113dmAajow3trFz33Uy8nw1/bQvWLMX9qoJM2FK/CFwTvNeW4+ixWB
IHovEiv2Z+0eSS0JcBXAfWadTha0593PiJ0aMWPwHfa0smahNmBqQ/XYnKGS0tsd
/ijY0m0YoNyjwS36gRn19BMJ8BXKraxlQirjLM2zcuAXh1/wieahb8N12oPgooNc
Yn1rgcc3V3Ua0jW6qjypkNJ0aY9zQ1TNPf//Dv1Vi3Ut5niLMmroucYho9Cs81z3
IpKi/dvP7nEtfxuyQwTNHhJnDELPBuAQ3BBEptVYZufT6dtCIGeLZoLALShvEgrW
TI7HtAcgdBI5+52yCJLhFg/Gkg08BtztAW3XJyfx0j7RH64ijCKpNzW+aBSMDPCx
bPvLjzQzVqTuCpr1VF+uY28NLFfXdcKfOVIvH746nt7f1S4UUUP2h/6ISIE/NWSf
IiAL5Pd3zpdCzT2w0hrztHYzFgVM0m8LSATm7Lfvay9j8G92qnzD2kge0J1uApgw
SMJCY6wQ1EubvxywxML4JZzkDZMwtfTmujaGLNZm1J9wOW8ZR1et6Oy39326n34
Fv+Jx1ZaLC0WY6Ap/01YDeQ4ebCqhRJBli2e54AeNfFntNmFtxvkl6/ZLvEi3fHC

```

iijh24iHVLQNKjACp+Ez8/rjWaqA1MEBXhAJShT7pTKTL5KtfnOujP6Jd2REI5jD
UTmbwOzdEap3xT8pVBLWrJr9D4Me4vu+htyqxdNYtS7M7LP3AaWN+XNbtVszES80
u1gFNKCytaVwX3lVtFuMCwT98e3qxhE5WLENxSsHYWUSoYCF0IureNIbmLeYxrCE
gKJ/vYEI5EGYWBXAYRs96Klx3zfmMCgBv7Fi+U+Z6zlh2nhJo4AF9G+DiifeRVTK
syESFZSFYDrRFIQR4M1Hig/yGxZIBSD73Q779Q5x1T3/u5pYwP2Sb0I/45csIWvS
zK1cdjVDwEOGnjLHP3E4z6Dvp58Er8zHkWPPhH5bvEzyP5ga14huQ8UgrVrVm66/N9
Ob/Rh3iwS4fk4dSQkqBxZ+W8QifsXkWW0jIhjbDjtmj1r/1azJJSvMkXf25ocTjT
3x1o1oRlCHuXa2yPY0He8uzx6ikrBHmaIWtN0RvUIXA5Bqfk6xsDwfsWfTsgNUxp
pUVgQawrq5bwFOD6C9Ee756QXp9DGmW4PW176u5qcnKYeG7JHud+JLRjcxVvxh0g
mayCxEsRoCZiePnRjSUWTUiFd7SQ3C2/3hRpC7aeH4rEZJ00W9cFBgRzHsZhghjK
IWEt5kqpX4C7HAhEHmk8NztZRoMXMLEK/yAj6btTt7aRgPtjkISQ3ZDU66C4MUr
uj2B1Z1HBLVFZsk79z/yzHQarFYooGUJEsOmJ6VDjGj10h3kHR72BDLspScxUqe4
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"

MII0GwYJKoZIhvcNAQcCoIIODDCCDggCAQExDTALBg1ghkgBZQMEAgEwggREBqkq
hkiG9w0BBwGgggQ1BIIEMU1JTUUtVmVyc2lrbjogMS4wDQpDb250ZW50LVRYW5z
ZmVyLUVUy29kaW5nOiaA3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwh
LWJhc2VsaW5lLWx1Z2FjeQ0KTWVzc2FnZS1JRDogPHNtaW1lLXNpZ25lZC1lbmMt
aHAtYmFzZWxpbmUtbgVnYWN5QGv4YW1wbGU+DQpGcm9tOibBbG1jZSA8YWxpY2VA
c21pbWUuZXhhbXBsZT4NC1RvOiBCb2IgpGJvYkZbWltZS5leGFtcGxlPg0KRGF0
ZTogU2F0LCAyMCGZWIgMjAyMSAxMDxMDowMiAtMDUwMA0KvXNlci1BZ2VudDog
U2FtcGx1IE1VQSBWZXJzaW9uIDEuMA0KSFAAtT3V0ZXI6IFN1YmplY3Q6IFsuLi5d
DQpIUC1PdXRlcj0NCiBNZXNzYWdlLU1EOiA8c21pbWUtc2lnbmVklWVUyY1ocC1i
YXNlbGluZS1sZWdhY3lAZXhhbXBsZT4NCkhQLU91dGVyOiBGM9tOibBbG1jZSA8
YWxpY2VAc21pbWUuZXhhbXBsZT4NCkhQLU91dGVyOiBUb2ogQm9iIDxib2JAc21p
bWUuZXhhbXBsZT4NCkhQLU91dGVyOiBEYXR10iBTYXQsIDIwIEZlYiAyMDIxIDEw
OjEwOjAyIC0wNTAwDQpIUC1PdXRlcjogVXNlci1BZ2VudDogU2FtcGx1IE1VQSBW
ZXJzaW9uIDEuMA0KQ29udGVudC1UeXB10iB0ZXh0L3BsYWlu0yBjaGFyc2V0PSJ1
dGYtOC17DQogaHAtbgVnYWN5LWRpc3BsYXk9IjEiOyBocD0iY2lwaGvYig0KDQpT
dWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLWx1Z2FjeQ0KDQpU
aGlzIGlzIHROZQ0Kc21pbWUtc2lnbmVklWVUyY1ocC1iYXNlbGluZS1sZWdhY3kN
Cm1lc3NhZ2UuDQoNC1RoaxMgaXMGYSBzaWduZWQtYW5kLWVUyY3J5cHRlZCBTL01J
TUUgbWVzc2FnZSB1c2luZyBQS0NTIzcnCmVudmVsb3B1ZERhdGEgYXJvdW5kIHNP
Z25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhIHRleHQvcGxhaW4NCm1lc3NhZ2Uu
IE10IHVzZXMGdGhlIEh1YWRlcjBQcm90ZWNoaW9uIHNaGVtZSBmcm9tIFJGQyA5
Nzg4IHdpdGgNCnRoZSBGaGNwX2Jhc2VsaW5lYCBIZWfkZXIqQ29uZmlkZW50aWFs
aXR5IFBvbG1jZSB3aXRoIGEGIkx1Z2FjeQ0KRG1zcGxheSIgZWxlbWVudC4NCg0K
LS0gDQpBbG1jZQ0KYWxpY2VAc21pbWUuZXhhbXBsZQ0KoIIHpjCCA88wggK3oAMC
AQICEw8tJb0R0ZdKzkJU6HuPTQgIRQwDQYJKoZIhvcNAQENBQAuVTENMASGA1UE
ChMESUVURjERMA8GA1UECzMITEFNUFmgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkwIBcNMtKxMTIwMDY1NDE4WhgP
MjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFEYxETAPBgNVBAstCExBTVBT
IFdHMRcwFQYDVQDEw5BbG1jZSBMb3Z1bGFjZTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBABJqVKfLwLjj+gBUCfkacKTg8cc20tJ9ZSed6U3jUoiZVpM
LcP3MUKtLeLg9r1mAfID1B/wlbmadXPmrszyidmbuZm0pB5voVQfiLYy3i0x7Y
OqzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0aGdmnx40G/e3p1fIKM0dPzZLo0AJF
5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXCn5XL7wWTLMLenF9Byb5ksKqUuqEH

```

```
AMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWzB2zNS20F+XIVnzRG5DeoULq8v88Z
5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAAa0BrzCBrDAMBgNVHRMB
Af8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEWATAEgBNVHREEFzAVgRNhBgIj
ZUBzbWltZS5leGFtcGx1MBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQE
AwIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj80e0r83zdw8wHwYDVR0jBBgwFoAU
kTCOfAcXDKfxCSHlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCcsTKc
FqQMPTryujRGzJdYA+R9eBAuDLsatbtKt14FzkgRy0g31/+Cw7H8e30iLrPIF1WN
1qjHrjg0yIs5AQ/hgxLvLir3hEUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMT
g1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7FOD7Pfb5v94M5274XYx
W2W4uKGd7QGnUZROsvSYkGiWDp1JhqXwfDz8A0enITGXnoEkAFvviCqh64P1hIe
Morj36pgL19oWZD6YrzSWHUz1F00juyu0fQsqm6hvrDTqNpHNZ015f0URza1SkCv
i9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmgnXMA0GCSqG
SIb3DQEBAQUAMFUDALBgNVBAoTBE1FVEYxETAPBgNVBAStCExBTVBTIFdHMTew
LwYDVQQDEyhTYW1wbGUgUGUfNFUfMgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5
MCAXDTE5MTEyMDA2NTQxOFOyDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQKKEwRj
RVRGMREwDwYDVQKLEwhMQU1QUyBXRzEXMBUGA1UEAxMQQWxpY2UgTG92ZWxhY2Uw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgWPK2af0+StijS
NOR8K/hN8D+1078oullsk4ASvSwjsCNo7sHUA4xQU15J06VqY18LANwORjrc9BaX
4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4D
xMI07XYNFUE0ls/gkUP2Gxzyms02kaYWTut3SryCqeHEFbZFk4B4urMk4xrIJC3Cz
WruS2Q0FHbBlfkgKN5wXVgkWffioUcfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog891
9MxKI9H614KuElNAtJ7BtZcs17dUy9u9C0gEyKriVokFQgqQ7XNDU+r3Se0Wwks7
AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDA0MAwGCmCGSAFLawIB
MAEWHgYDVR0RBBCwFYETWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggr
BgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYDVR00BBYEFLv2zLItHQYSHJeuKWqQ
ENMgZmZzMB8GA1UdIwQYMBaAFJEwnwHFWyn8QkoZTYaZxxodvRZMA0GCSqGSIb3
DQEBAQUAA4IBAQBziaI2p86poGkjD/4Kkk0HG25nY/0eNARD6/0F0/sYonX2doiz
cGmk53riugAocCn5zbzhW/JVdYn30UxfyrZlRAZef7GHqgB/Nyj0ad3pdpVYedH4
ciNkKjbs+aEoTWgAkoqEnt1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqGJdGf
8L1zLfXBuo2zL3HR+M9CDr40pq2JCKzP0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+
Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz0KypyQ3eoZ6EPazXqMyHAVcsm0GI
364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCafwCAQEwbDBVMQ0wCwYD
VQKKEwRjRVRGMREwDwYDVQKLEwhMQU1QUyBXRzEXMC8GA1UEAxMoU2FtcGx1IEExB
TVBTIFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69Phq
zpqP1zALBg1ghkgBZQMEAgGgATAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwG
CSqGSIb3DQEBJTEPFw0yMTAyMjAxNTEwMDY1NDE4WjA7MQ0wCwYDVQKKEwRjRj
9zozFh95Jb3qN55AtQaDyR811KUu+Kt9v5+b9zANBqkqhkiG9w0BAQEFAASCAQAv
syHys6s15UETHDVuQ8xBKoZ0ktYzIMuwy9TPtVJ0rX1vG4iXMBE+px8wWoyqlypv
KkM+bN307AfxMENsBsWfm9vEzPAC3WjgX1/6T5vhgxWb+Cb0Zn+uaYGkxa43vsS6
fUonAiKB2QTuG4LgHxD11xsK0YvUx8DcNcS/I4y9Xw+rm74LTjyrGISWmq7qec+s
duAWjkLU50250pkh86yjSI0L89x0XEqcKeKoxp4071xt3LZ6rHC3pr2zHhgGo3uc
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
BAoTBElFVEYxETAPBgNVBAsTCExBTBVBtIFdHMTewLwYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIElcnRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqSISb3DQEBQUABIIIBAC7eDC6qLlW6dni6Tl1jF0JWAP5P9RzVjPRjs
gJJJeEWxC4ddrf6UUR/HNSIEz0R+QFrBuzM45aZZdGpQ8WEyRdhfho9R6hHdaDhbL
FWpH5K5KNWVaUbmZkzvhhXAS6/ac9p9prd+0D71LPZySqV7sL43jFS72bx1jTF704
Zfd+IoGg5mjroPVQBpP3K6oG/10QydggnimBy5ISWRYtsHizfrFawj07V6I8f7sa
e0f6jFB9t1SVbjNzuGSZ8R9hg3nVHjNsQ2x9YTHDzaJoMlvGwDFP0ouo2MHEirAK
It62HCddq0tB6fGTUoxztrqPoNNTiZIN1Zb4eXp0JtpnXKMC5nQwggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFUMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydgGlmawNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64Mv1sDXhpQwDQYJKoZIhvcNAQEBBQAEggEAWMK/5bj6qVYBipvgvm/QX0qT
7iH7R7z8RC0jLU/k/G2Vgcl+9Lk83z46Las0vkn7xgUJCwbFhw+hgd/rBZ0uDJPt
Zhrx0G2rIU0aR8dH2YjithPi12yNGWgxddaGAFD07GU5Sbi2Q/R1jDoVXuYRGIZW
EGoatToIrQLmfKMoF0d2EbS0I6ic+jHNUD0NSzstRdsoqIDKM0PWcb7ap+uNsi2h
eJemWXQ5xwQuMCDNxicyWcZV9TjfaixZV2EaJjtgsB0YbTxSu3AlpYRIx+Ao1+58
TlK0bdrv8EUqxb3ehR7B/y15GoM7PtF1MbKF5m08JQCLUVULY41BLMEs6JTijjCC
Ey4GCSqSISb3DQEHATAAdBglgkGZQMEAAQIEEFcKhjcQbc7Lfa9Sm6HsEH0AghMA
Xv//vkE9RSpfziFKfS2N/SASzPEdcNE1ByKrDHpehYSwXT3s/V+JqxyfxW0dBgR
hrdQ/dw74DBv/Yk/q5auISAwC3ChtX0sgA5p2oMN0cDw1z+ZtniVHSYoDRRq5fnj
1YLZ8yNrziZW2XF6gVlnsCE7mIjuCzliUxpSr3PS1VLTXRgqeXvrzEijprArIh8P
SyoZ4Kd8js+N85yl1Lrh+EERevf184tTeRTjVdP4c6G2b5yPIwPqABM7B4EP5DLR
AWaqEXr4g7xWkiuZLYjJVdTfh0I6oiKVkVoP7X8hMi0E0M4Sx9UG6FGUz7mvuraR
az3wcYWNKhf80XoLZM64on9t2700RT16NOPMi7Ik8nM/Soo9lPm7RxHGN0bzNba3
eVgBV6iDn5bZgMxwocdY/A2b/kM0WReApCXNhckJo301q0RrCaTIKAMDx6lyUI5
bpE+3Bj+S7WYEB1QvXs3iAcDqEtA6zLy/A8eCJdgy86i8QS2PKRb81+3496ogtRQ
a3cNoxBQ1nzxS0jnzgVIPi9wTSysSVbtSAZJxeGoDUk3T/pyTki90DL4GsINGTew
WUuUEHNUlCYy7jRN6cDU/IV3ucww4WWvxos/npcQar994ycE+qCob3FE5GUMQ5t
ESN0rYoHkKhqlc/eNJs4HmICbJnq3YbXYsa3y0QHYYrCAMvtXW4zuwng6nh9tM5f
YseP0A9ztik1y9PWDUfP1pZBPwYIN+RnDRsj3JGIjPy5Eu+vPyELGzSSm4iMD9f
7LUWuSQAchF2ffKJZNItmT/HKXB8MIRnowdBfhLIyNy+hv8JX7B78ixpsvsjTsFD
DsqC0IV01Zf+/M/h7+RmV4tozt52KvU8jr1j0Io1PCBvp7QSj0L9M0u/M+2gXd0B
4kB9zNL1Byy9zla1HiIEuu1LVZ4zmxw19RtZCB0sgeAquCDBta3Qg1/pMhL9jQRw
wEQTBgoH5Ibs819g/R6LKy7hHv14Ea/a+b+LVT8Lz9/dCjY6orXgu/8ePcoiAKmY
MFPXLoSHnH9LF8104UB/Lejo3M4VUftZzZFs/bVQK8pmzx9bb0MFoKlM5LsgE+RJ
W/oeLsJfF3iVWnvHmVgDTZ6S70lhfL6ZJtnziwkq3Ub3MjhlhgiaS1dzihWXv+m
k/U8mMu7t7033YW999w9R8G2jpxU5Sp2GzEuAzzqfEL7eKnBRQJD93dOrwUmY6RY
HzUGJbfm56J8+Uc4GpGmgRqnx96aodf/McUB/NCLD5DVJ3aPvktHrhyB3M2V4jq4
RT/xXUvq+FLqK0nR3XwQicLcc1YREa3jbrf5zHJmcITdQTuZmgPXL2UAPzbdzm/e
sRK6o7b3TQIhwgyEWOAVrf91aDuBi0cw9/IaLDU0wy9moQJHb8g5HH1+XVhYwqfJ
pV0LNGSSxSu7abtgmmd02QC9mTXxh99lcE+z7SJXYjkNevf/SRzIyUIwtXD/Se0M
2LYYArUnty0QmBVzUREV9wkZXCR5cRYS9az+nBjUEmLL0CBcPPl/ar8m/qzoWm9s
Jnn1NQQVP7F8EVOuXyPDchk820ZVJ/WcLpGPoPWQlCfKbGwK0ftL8DQPFnZssBeQ
cNxihr1y2iDFGib8vt9vr10hR0XP0zMruXz2CukMILTV1je+UPV1uh41YVKJ0sS4
tFyWcVQXxfUZtCELQlaPu00FVvpzLqOmzRTd6os/zCGCo8lJ5VXeuQdEo9lPMebu
FygtuUJBh4WchNieVjoAafg3+51+IY5Ft5qpHUFbQOWQwskA2Ly4KGVKu9XFrUS0
rAPLk3CkPYxKA0AJlwdoc5CI3jE3IWWQf2DTFYQqzDE4/omkFCB3j7uIQVRYXD3I
```


1ncWsYa+0Ih7r6kLdEWWXBHSAZcMCAwBNK8+7JYtb3tQj0aUaOid6OT02R0ozwuG
90AKLcYfI6z/z8ETf4UNQ2UxgoXGEMr2puKx+3+R1BZiIdk8VHb0ZQDcW6qNEHdN
5Aq841xFOkdjg0AGt3WmUPXI4at4gxLMDYdqK+KtL+JuBBjqaR2ctC6Lpd3VC9jw
io+WNCfLvvbhw2MtFms0vGjBDUxnNkyhmNochTMsVv2IkxqJofjaGJ3cjFmU3Qi4
ARyuB6tFgtw5pMqw72Hci63gv8pRrmlyEIL6i0XhHvaqc/xz1PPrb5z/o9X3iv3N
etY4PhNF3FKaTmeFGPwGd9czdUUVBphb/zph+xzzA8rE1ItCHwNyy7JLX3veILUj
dyeKEDqSp1CIx9+HqYhZkCE9XiRfp5UgGJ2uFKgiP3gKHHn1eeLotKASZbaz02fw
M9k5xIom9wHVHnnnPvTz0CI7iswvP7am7moWkMwAzmxEUhVyWTSCvE7Pdn+XbNA
wcMSf4AzEILXMSuX0C876naz6LBZDdMQAaSRRjDab3YilCrVEMj4BMDmniPJ/r7I
IBiNCt0JjScR0IpTL9ASJqsBf/HbvQo5LVieTwVZUGZrCViT6LbLmT8/tBV3Y8Vw
9Y9LbombG3TXMWEgtylKxYDvJ2z0Bx1pspXnsGzB2QKxduinTDb6N3PBWR8Yb1u1
lcWEyZx16n9g9DqN0pi8cmVrd5f5bBMOD8CnPK4mWKKvpoQ0IX1NIDOQpjDZGgPl
eYQBlnT0j0qJG10m4X/qv+1yzTltsYnjWzER/teKsjGXUvMHZnwx6iFdU0KQ/JjV
A419ox0SiwS0N2/1ZgAosqw/N3oDuPEgFFYKsoCMFjn/WCX8LBdd3CsznKhvfsRN
qgNHEVGzQoVT70qWhnNb5F/8tGuQZ3aX2PirQT/S8+e4sPdgt00e4AZrmCC02wmw
kWyTPNtflN4GcmZmPjCAIqirm7ohaTdUSLfDKb2qBL/80UFQqyL7loJnYnIEguLa
/tNLfWUamgZ0Ets4ebaa559S6UbINlhwKdpvuoh+XgloNRfxtLsszAmQUJfC2GM
dWnOeKwMaIntPz5YucKa7nUYQHxzU930t9d15WhoqnEi4Fqgo15gJJq9AmODHDXr
+SsBc7mpuE/sJBCIrn9XiVU3QxXniAXx8agQHwaKc4YYXu1EB+pium01HqXtqcCG
iE9NDZRYTb315an7cPnC+674y3A3X6EivFJAQ7yabMIXG7IZc+gdk4CwkG+XoG9R
5zSOjFGt+x6FaWL0s0AbcZtX7htR6R4fnB5thsJ0u5U00jvj3Ub7cSF4I2Gqf2u1
HA19GZ5cC4906jABUxQBhexoaI+ywQOXVRYcQ2CGrZkjy1yC/EmH0w+sAmrn95f
wWDDz6izT00VNsazPzKTSuLV6R+a1EjilQh6AgsYSqzCRTum8dRRf1S6KxA6gKAA
6c+XVZje9A2szgblxHfcs/FC3hs7veBPSbgCeA5nSHTk2LjmExQX5n6qsavHqUba
gi01+X0792Ji/dPMNi1U0dN1PJ/LIHPioNcG7oBmF+AjVE64fe8G7Rxpum8JebfT
sv1Pgq/aUsLb2adv/Glye7vbuLQ0yeUJfGcNHCEWxfh+weJHXilxxxZr5wjIkee
2+yK7sHFJoY0VT+dFFdg2MU11hjz5VhE9vQRcwF142XKJqI842xdCvjAeXGDWC8
BIqhNJD185nJT6RddqoAylb1R2AqmebZ78E1LVsfUJ2MBUcWH260Ky1oWp7Rudwz
rKwxbHjoadueEom2DhdBsCl+AiaOW2S6iq7bBffqZTFdM30XsXsdy6nNaWSvi0oX
DgXLK0Kq4uh6SRD17tKFPoa7rIb0B5n7r82vWKYAc6FchTQGU2f/lXXnQuoycDM
HssIDRpSxzMB56ecSBQrApjWS/NXUpAunJr0zW4FNWQIEd143VTFJEg7tgk2/0ln
PG6fzK0iuJdqyCLXhx0sfy/64JAXbA1exyp9B++ZUq6pMZFewPpkqRH17L8EJ2NJ
62jYABnH4S1uiyY5rfTeY+Sz6gwlD+fshZSWF1a6D6wqKBT83I7gpvhbGgzctRpB
Uycd/IRV9NG0zF8RjpPtNOYUKV4C6/5cTMnT1NK0J7qvYdEQRSLCDVDpd7Z1ptw
Fjth5QEXqDA8w/B1UzdVKhvefN5ZQ33bs43/4A42US1EMFsPlntMQa5gibVLVaMj
fZofDE/NoQUUjC8zpqoHXrPnLvnmZQoiJsrV08/HEfBBo7N1TQXNmAdfVbVv7L/w
MJziZBEE9ux2rTilRpINcNbG1TTMkaTZMkv9EbiHHQwbujiDjyQ8/3/rmgmsigjKc
UpcUX8vL/R6BcRjau9v52ISAMIRu0v2yeiyUT5PyjUdbSABZ4ApgHPjkIusTtGzE
KNut5dmX+YsLQofapHwh84xvr0xBGfFNTpnEHnj+sIYjEiHVxWXbeFPnk/Arshq7
UjOu57IQwtaB18t002017HRxYO+PnjH1qLrvWSYVa4FX7BERCdZQsGDx0BeHdcmM
sLiri6xgXET27TkSculjVYQKMZ6fTXhf+MJUYWlWatAgoW6YegwnfCw5zZgLDsxs
f79eYUy7eePwko6a8jgFucRHRWCjmpCiCarLTbpIeMGMq1IBM15D1gKKDVmmwmS+
gm4n2XZ4dyrqzJMJHaSGX23gXq1S82rx2B9082uWKOTrHAgUhDd5qfp63rGZJ/KX
RwfPdJHy4ITGCPsi9sVo/Gt40+PhaH/F+156N6+YlmZ4NemtfxWRotBR1a3B0bLA
CTw2+T+Nus171wJu3q0nW2aSfHrF8laYCNkKUMqQ4Ju7Yf3c12B8a0EXYamiAvD1
EijcTPQe9VexCXX8zSzk+A20dSxtAr9QhRAAao9ewV0oDbs07G9dBGqjnAph30Ly
0DY0a9ylz1DwJWeSAZvsQYJ4dCGJlOBXHHB8VWjkdKe6751F7eDcvaN882M1jqpb
edoV2QrdqKjITiw+jSMKalldsV1f/WaIZ7CB+aq0mupKUdK75NJ0GiUBRb7L3zT
Ja9ryWZ05VVTvypRWPsd4m1wLS64GT0ZpSPNwa8FHeKYif3lVPoA6CpDvcL5AtEx
WpwsE4+rSGqMFFvk2MtJswUFVoJYKMxEVHDqYUz9c3Xati/wDDpmUuSeZ+V5yujj
BmWTLKH5jX8gCyhHDWZpRWStMxxIo8KHtcR/q9yf6Fgp30cN188Tx4hVqDFbDeJo
iEqy27D1SK6zBtSRLaFeZ+t5E9degiG24xufCyXwg5o/Zoh9+J3opef4Hr9qfBk8
GVsg169pNQsvqeAyI4pwlqvNLz1/B72TyRk/0/PibKICikUI/UrOkSKsyNBCj8Ns
N6PN0+KxNIsoCuHdPc7MKnMU4W5d51RES3SmQI2wKBiq++V02zz7G5Toi+69YuXE
eTwn3a6+7MxG2NDsxu/YaR2ghqm+a7PN++WtpyLSw2rsdHR1TrOQ6FZBBuuLR7z
L17pEtN4k2p43DURAWr3jQL9/iRdqYaBXMxdL3HKMiD4XTvaNw7vXs/rR77skc7h
lFb0vFIk8FahdGHAXY2/uJUuI/RA9dKD7IizDtuVel9n8gsxfPE68Pm7y2ZT9fBe
FXe0N1SnRCXwKPaBc/C+cErJbSx6/F0aWpraenLxA6bdKnA0dznNotzxZj1J5eky


```

AQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCAATAB
MB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYB
BQUHAWQwDgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546v
zfN3DzAfBgNVHSMEGDAWGBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgqhkiG9w0B
AQ0FAAOCAQEAgUl4oJyxMpwWpAy10vK6NEbM11gD5H14EC4Muxq1u0q2XgX0SBHI
6DfX/4LDsfx7fSIus8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1
Ib3U8QzTjqB8+dz2AwYeMx0DWq9opwtA/1T0kRg8uuiVZfg/m5fFo/QshlHNaaTD
VEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadR1E5K9JiQaJYOnUmGpFb8PPwDR6ch
MZeegSQAW++0IKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTS07K459CyqbqG+
sNOo2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9C
qaJcOvT4as6aqdcwDQYJKoZIhvcNAQENBQAwwTENMAAsGA1UEChMESUVURjERMA8G
A1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBzS2SBMQU1QUyBSU0EgQ2VydGlm
aWNhdGlvbiBBdXRob3JpdHkwIBcNMtkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0
MThaMDsxDTALBgNVBAoTBE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMRcwFQYDVRQD
Ew5BbGljZSBmb3ZlZGFjZTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ALT0iehY0BY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LC0wI2juwdRrjFBS
Xkk7pWpjXwsA3A5G0tz0FpfgyC70xsVcF7q4WHWZWleYXFKlQHJD73nQwXP968+A
/3rBX7Ph00DBbZnfit0LPgPEwjTtdg0VQ06Wz+CRQ/YbHPKaw7aRphZ063dKvIKp
4cQVtkWQH16syTjGsgkLcLNU5LZDQUDsGV+SAo3nBdWCRYV+I65x8Kf4hCxxqmqj
V3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG11yyXt1TL270I6ATKRGJW
iQVCcPdtc0NT6vdJ45bCSzsCAwEAAoBrzCBrdAMBgnVHRMBAf8EAjAAMBcGA1Ud
IAQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFt
cGx1MBMGA1UdJQMMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4E
FgQUu/bMsi0dBhIcl64papAQ0yBmZnMwHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSHl
NhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAH0JoJanzqmgasN3/ggSQ4cbbmdj
/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AchWkfnNv0Fb8lV1iffRTF/KtmVEDMR/
sYeqAH83KM5p3el2lVh40HhyI0qNuz5oShNaACSioQ23WxHGvy9vsdVfnbhsplrW
g9NQ2WbpCmK+2oMh2oYl0Z/wvXmt9cG6jbMvcdH4z0I0vg6mrYkKTM/RCGnumghx
wYToj10yD5Gs4D2IJCw+fx50Dxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJ
Dd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk220H4ConlB8f7R7s1LM2cSYxggIA
MIIB/AIBATBsMFUxDTALBgNVBAoTBE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMTew
LwYDVRQDEyhTYW1wbGUgTEFNUFMgU1NBIENlcnRpZm1jYXRpb24gQXV0aG9yaXR5
AhM3QQV57XV/QqmiXDr0+Gr0mqnXMAsgCWCsAF1AwQCAaBpMBgGCsGSIb3DQEJ
AzELBgqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDITxMDIyMDE1MTIwMlowLwYJ
KoZIhvcNAQkEMSIEIMF0xgjxvsd60/C92x9Wv+OPyqNJRSBwoMdr0B1V5Y6iMA0G
CSqGSIb3DQEBAAQIAIBACBPs5toz4DA/xDj8t/B3f8YR7Rhxf+607P29Qd71vc
c+PRfV9P+SEw1HgLTRvm242i5hDk0jWzwsZFTT9JfJa3fKMGM8ZpSnQQq8Q255PY
0003qh5xOpUT8KEoKQduLQbEdtUAzndZgfsNBbnw1buT7kaWqhK5ExB4qm+fPyfI
+ZRng4B+PI8l9YpcuzybR10CylZLzJdB2EfHcXFDt91nA+iouUNCpN0ddLENJ6gZ
2338fhZ1xokMqSXo88sEjh9KBr//UMLxsWUJ5rM1DBGs4ysMfmuoz0rAnh5U95NZ
fTDI2hVSCHWx/92NDZXQl7Te6MFwPluHV8QLwn/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

MIIxNAYJKoZIhvcNAQcDoIIXjTCCF4kCAQAxggMQMIIBhAIBADBzMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIElcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIEh7j00
Boq0MA0GCSqSgSIb3DQEBAQUABIIBACAu90H5PSuN9tLWwz3pZCIjfuHDPvElwIWM
FLLaSLuRC5cnMq1xagX4RJaKeAhI+WZQzinX0SRGWosV1ixjq1RhgoLsdnQhXh1S
G3HHd1ke+bhxqlyfAx0xozsKYybrkx+dHIhZk0tG9XrEfUC/4QCEAy6pQz1M15i8
N00xXi7UaEHo7qwyW7NJ5wWe9QrDi8G3nazLEAWEro6kimhdSKiVvGi+7KCjLQpz
HM/BY/ydpgLZ3BiM00ALCK8BiZlMhy//jp6Z8638UmjKDika8ExU3EH024yBT3y
TVBCVx99bq1FwP1jnBBKg5VjeFpFA4JnUge5J66YI0R7DVeGglowggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EGQ2VydGlmawWNhdGlvb1BbdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEGgEAAZ+0cEKyP/cfIy34M7u7ZUcdR
HK/hm2UHK1cS1xxIDvVZADtdSzJ5qE6gzeRtCzVgIXEWPzuru6ADSPFUNDzV+R9E
G8pDkwsZzzQ4QY37hxx6/bWDBcBBjF4/hVe4ubxGEvJ9QxixB2B34m0nCwxD6LY
EN2g88Pc9KSSRbduGq4LRfyrVQEG+WpKXzjHQSpzqiDXuMBDDW/+dMHaGKsR24oZ
Ne0Z0U/i0nU0J0VuuJbnPkgYUJXQvafZSJGIfhpocMMPD9L142XkMLIOJvDsGqVk
qkp2uEUJ3tzd4Nsg5UAWIrMnWQRdWbdqLcuMfoabNck1l0rJritHc65jA9jv5TCC
FG4GCSqSgSIb3DQEhATAAdBg1ghkgBZQMEAAIEEIP1SKNdHDNw0Ia57jzQav6AghRA
SnD0DeMznPKqrErin0IkCd2tCYouj0vON90o6QkuEMX0SsEL/+9c6JQRVAVxcxip
a/FpEnBMRBGdfeujUTFp/AM89QL0TVc6jdjFRD5XbDsd4VS1k/HTDar0zv8YEZ0u
FCHit1AoN04WgyDK2A016XPazZN+IZMmh7pWRWS7k4IgWfuo6tcd0Vo0TEtZH1Dp
oJkxgSgg2bZwSXq31b1sTDS1Cs/rG9h3GD6uBATdRKBD0+DRRX+Z/yPM96aFoX+0
+DqPvun7amo+2xeTgJgkchz2XK1sK80G0vb6aMv3PwK3p0KDVCLNAzkaz0B0QvdX
UFng8/sNnu/P9+WBelewVfGDTdCocA6+9vQa6Gx1RzJz0js2Gt4MhH/MfsSbapjc
omaveE6ba0DAHMcBqH4r77Qrg0RmUfBNQC0AsnC5zdm1+w5UL0t9YkKUWWw4F9sB
0+2UeQpe0y+mtYQatJvjT0cLEcAzRmV6Moaq+ETHHfeSoyfJbIUqt7K8epNbhKws
QC1Kd118++t2+Gx0jK4vuU0r3YF12kHhDJIf5H/FJNR4YS+ZZ3S4IRky3HeSx0p
CmJE5x5wbXLvLf6+NTcF1yzYjASQvwqmPSAjHMYzD3t8SDrK0/cJGNdud84FaWfx
zf+0YyRu1v7pPvmIK7U11Nh4T2We1ecF070N5qVLMeH5I+Zc/YwXRkyJGSgaAXHQ
cgh5Bt0QqnsstX+nYofSceGgn/Vpop52pwWCf0/KnRi6C4Ih8o1naJOSEcU8Ucxh
D+gg0Avy/gLeag6G1DL4IzxqNHh7Qr9IZfk4doNyumkc0vMz7gSZGFxHo0PdH61S
/ndqe8D1C0zFj446GIpj8hfhVLf8+7eVGK5GPcfAiM/fSjfe6ZVqn5zX398YjHGB
H0HTyp/ZvWwNNMfdeJgG6ukdhqhx/NqK3/Dl0crpCbdGqQThj14UDfmM1UEt255N
Mp24Qd+rUe0tj+vGComumU23UueJz9/VDhQFf0PMnhLnqxNhC55R00CzXBla3f0Z
6t40yRo0JCT9fkGfHFgYxmFLfTXkpHK3HBpP/tu9rFL19nc8KTo0guY6N+c5T9Rq
cpCyRj5yQIwks5sLREYyNlnVQXBK8jESSQE0uJ0p3pHUGNKMnWwfp1kuBVK1pAtt
GUUFXZEz24T9urWaJHXFsikB33aks59HrNddwamv2wpgadmt2e5zDZWKGtB3p89L
oIPbM5X0W2RsTAZwPgbjNqs4y7YZNT+CerPoocgI226Jyhxi6e7dYGrOmpavgyHB
ieale2z0tZdY0yNBS3FspCQWTXOUtte8220FuVu5xF4G0m/11zYRLt85SuAxTsNr
DwrBfLvuxwpX56GPgp0C42qyLbeuw19iTFs8kMXJxoSnfdJq59AwUqwdeFFxm8dj
TL8eCsyyfUoscvZLCD78mHMvB8IRzIQ/iCMESPfeAig5pZoeMMx2gVJF0ZKEWqcW
OC7Icm+qKPX6tjSi+EnUASKldfrRhUQ+BdVYXdEhwf6UUG4HZ60Ea+MxpFUC2u1D
3kKddnMJZaDuvr3k23Nh1BVhS0t7Uo6Soi/Sz1aow07d25JbLv5AVJJJeE+cWP1SI
DQTALPuYtx6oMVn51TjLw3KaF/Y5i+RQbvJ/HeNfrstrelx7brLHiHoCf1wZkgJ
EaQUTt/GZlnKv7xeKleBvJI1mCdy16NZrk1HMnPUgj1ZxEwBJ17M23B3hAkYLF00
EYtKUNushATxhMptM0sWQffDWROKD8c612WrbYo/zz+ApnNRUzEs20+cgvlT14d9
N6/untoFR0mPe+0ZuZ3iCKmGdw+LNwR3jBeLd0YxYw1QrRBWja400ofswqddQ9Iu
99+ksCTch4n4BSDNQV0VLQ7dX9uWSgnno6fD3gpmIJxrNuAMfBavXqsP1Gtj18uB
wBXn//0iMIOgHYvLMEj+A0Q3/D/6sB7Mki15spxF3KDI+60iFQJkrTu0F+f/SaG
uGAYgEjANuOLCVu6aQZPF9lu5SV1MJ3VjXzS2obkkk21b6aNckXG8jZPzHwCoPJ
XDTwP8sM9VKbwMiv4wA/pxKjGEtJq4ss1D2L5CaZBUakhIJtXSaTc93qkH3o7up4
qyChBX3sm2aJPvw8s5fktLaubyBrUwV18/naaCNJq5QXhcfbGxoBaoDaDAZ1au0xa
F802tAr1Dy3/c8KAcguiZhJtNpdtC//v8AyMYXbocb1LoCb1M8a2QTmif7LUcXZM
CMiLgynIMMTQA7gfkN9uvAR+Yibh358h6vupmu1dW0LsCb9KYtuNWEIL5CM2sw8P

1hGKrAxJrbQX3WWJIn1d+nv+ldqk3U0lwoKUTcxq4q7DYG9WjOev6LDGQyzAojrT
10b+fAR50Q5ssBnmN8xgw2zk/1VZH69Iaq18vG+zhNJRbSox5hRrovJWyA9Xt1UG
9oVWLhg0aqd3FbTv1Nth3S17zp2BLvA0fCctyoHHGCEzU/Bx5Sj55RvT1v15KyUd
KPU21Vox7C+ueMwzG3zwYHFud9YhmI2114KfjHfaYICjqNY9QX15kJa6oxJKGi68
meRATnQOm811f1+p2PVcmqB7Z1qkQwX7Fpjx2r3oJK0X0+s0du4rEvwlggqHbCaH
YzZGHJM0CfI1zIo/BEkG/JkMrZ1AT41o7KIykGGVoE3420VvohXWqH6DyI+4Q0zm
CM/MYhcZwdeb2ucEeS1GheMzcksS+x/8h1uAhguFEf+y2+qcAuYCIUYuVPFn+T30
ee2vdXag6JYUzaRGsxfL7cCATB508d24HfiwGiyH/mQzuhk9CnK3IAkbdAcrkrOd
zhbPrJzG5eqohCnarEwsE5cpfTrCveft+qxqE/5nhM0zmgvXr6ZZ/+Cc2e//FUw6
9jdtZsKMHqTZUx5o0DaoBTAKXS81PW5pChQGNTCP9k1M0nFspLEg7jsDnZm5EXHU
q0fDCPdSvDGg9UkmiYrGuJfL0ywYn1Q+ai6Z045ILD23Ha//+yHZAms20A8NWcA/
UU+2kYwS5gYilvGDV7T11vnfLiL6puNP3Uk0N1HTG/UWQIBhYbtVfmGWnprz2SX
uWQfrvgkCisjHqTrJ8UzaQaX0iPEewQZzqVoMIo1xsnu73MqncRwDTbQv5UWj8zU
UL6I33gCd5v+SLSUfAXZq3YpiMNku+93VL8PnSh7d/fSD32N7/pBOewxANOR1Je
pV5xHCFtKoAvIgfNJVgOvPmXTLU7RD0/0ceGbIxDD6kEle8rFe3PQqYBZGjIHm
l+1Mf4XPHUu2IdQB1L9XJTAfGu7kYxNBfdvf0rx7vFjTwG4neNsgaG9X0tRIWcq
9LODeZuSP/Nnc+M2GcxMjJGLk+c9pFtoXYvgKA77ULIC84FdcNUiAYx14CYStMtI
Smi5MMf71uGRy8JDjmHgUfn3e93nCABa+76VYAxCbp1svkGJsUBC17xSB1E0xVu
Qi1hHs6a4yL8STkLyDYkBA5iBxWo4kKJ0gd1JL/lfscCUZW/90jb0JBLF9NhWn+o
SCVG+e0JbdN8nbIVgVhd/I33bJMV0k+RyfY04BU0BCGoV6r40CJtMFKq3SZIdnG
0GfXjGMxoty3mKYrOAGui1+JMxyzabqRQTxc/k/HyPHuNCr6UNGLL+UXyfWAZSSh
di+mVcsZ7yGWUz/sxLT19NFmv4hq1e8sBtdTF/Ws8SmEVLsmBRhokNkk0+rbm6gP
pdCsZ6rcv7d4mmhCx+A7kN10A0KPenHr18coLapibfWmqliBwNqk+SR5ZYdLAAPc
Us7xikmqXd+AIPfIeigGck+7fTvKf/c6tSG3JMUbxLnYH+18swncr1F4/Jswv1wM
IZ4wCCYSwaAyX/CuIyUGah20tPsOmg78hLQ0VCETt7Md1wld6NFWhiEGQt96wKL0
215fiLORCfeitnK2Rdj40GnGUpQ2P6aXYJEa6TJ0EMKMFKeaoIwB9fiCEhVJhUu
ejUAAh01aciU11MT0ZjyfvQZIBv5GyFsQ0jSVY047x0Y08Tfg5ZVKn1Zq+XVe5qa
g3t11aLrcEtAhhgpugHX+bAiwo0eP0QAeRpoIA5swsvkyy6ou6VaB6+a5Xp3fcQC
4gsr55CoYynF14/xD8obq+o6XzR0JQ71kA0KYTnBRZirNnctTurdbb0HgyKyie5a
+0HhGoa9JI3MpfIWku/RKn0VSwJk93SJww4Xi36ifBJjWHW/534W+62DrOnoss4wT
smdYBy00xrQ11yeBNb1yV5/ehfRdAY2dRhOgv9ZQtutFdLopZAai7MZkh63P8PSy
PvBV1pXrx1ZxCruBeafxJfU+rWSS2x2Bep3rDKtdBLM/816NUvMprDeR75QIEszu
byynANxocATJEkP0h2uGQ1RM1B1Fz8dFLgVIRQ7MloIEiEyzdkta2XDKZ67X0F6u
warivnsUCeT/h9SeIg3C3tpxgBpb9NppMY+UVb46HB7XpzjHQ0bDAwC3VEizrKVm
a/6SynuNH5n/zNU0/MSY5M3GQL4xSfXq8AEId5UhuPiFwmD+sQ+G4Vvm7d2HbXbL
9D/NkDep0zvdqbnB1ygTnlnRf/N15uFsdu+/1iKOMP5guzqCj0bKh+521QTBHPD0
nZVM6Xvr+hWZPEZ7auSUqgeBR3DBXiwwrL5sxNysL6wRu/TXVV1ZiEw+EiJJ9uZa
f0f+vvd6CeF72Syt7ceE5vs0i7M7z7dHMXiBsskpgQbx/AtTxGQyMU3Ki4DtmnnJ
gYBnIR7n6Ywu33dIEivQwZVYwdnwHo6/SujaAX0bEBcPALQqcZLouNtFB+0KbdQt
jG8wMLs8eV/cdGiniwDXtStP4VZw8lQNIIdiGtgWAt/k11zFfn7A/YF0QfC8e1k9s
oLhZTic6SY33HLDJX5/Iq2b3Iw6ijzH8kkgTRCdtoJx+EqRIiV6ybT040cRgVCKp
FSZyuTeJXKDGWFDpbhz/PD4Np+dzp0tVUWw0M8pFy3erWmKPqu5Q4lbwinZPwtUD
PpP8CBKRWXanaqy558CIyJKzhkgGXR2z60r0XSQtVDbcbQtixidjV91GP2qP25t8
PCshvBNGSvBlmIUWPFn4iQ9T7wnDMtxPDzBb0k6KXWi1IxxC97pfFwt7kVjGT7St
6amDsHEfCqLLCwCN6Aa31KfP58FewuEoHoG5xFaT1+l0W/U6n9F6T2+CUM/3Y0xN
kq1oI9e2dCDvz9ND813U9Y8HGHqGQqjSQteWt49xRXqvMi7gurrNz6i2fe0mCvI
GMI snp2rCDyIfmadJam0ElyYnSHbL+PyjhMt8883j+N3m5IKUfA1wo3KbI2zWa2w
mP6rImkJ2WemM2Z5gIQWJ1DOKt3M9fUxwcoX8W8EXEiRVJg0Tp00xn+fqXqItZDJ
qkdgt7h7bVnhQbV6fvOCSSwU1ta+bjVGFgHPE1C6+Z6UrHQwn3iM9ZE7A+ytZz2D
CikVVFZANawbp9M5mM7PVPEY69n3WQ3VqpB0rZbCYFgNB0IyUu2yg06sH2wrKYE4
pfMbmLOUyFTbfs8ChQioVcmtZHux/wOL52MGfYBJkupHwhZ1bBSjZocuXx7pxe5L
5EFMWtj6IQvQtE6XB7Nm5xcKty9EW/eIkd1aUXXRnzRK0Zb7eWnRnqe21iVwL3e1
R26HfqfCDnt0CSSkYd0meOu/mD4oZoqT/PRcR5i9b6jQUtZyymbFBG7ZdIuavn5a
orjJCN2i02T7v2zN0aYTnMX+3fue/Ekgdvw7EfuBp73JaySDVByciSQkzDyJnWEB
fw5dEF/Zx17KhnMud0ZIOZkdaAWyF36jVUg2znIA2cjVqd9P+CfH9YI6vXPefgE
rWUbg1ijrufE26Yd40Hj7hMVXdeIwDuhZe8AdSmovaqK06N0eBRiyCzznmma09ae
VVdLoHyY5l/95Pc4c0ZoeFWJ83agzcOrtSHWgAkVsycW9xg+g/oHBu3VoA8rlcs8
Djv73184caZKdwiQ9sHvsvBBMIT50zz9uts+STb4e/h3ELAAkddl7eFowqlV0GIN

X3zSdDv1sT4D82oAeMDxeCAXG18Bn03Vd8dt/zA8FvV1uUuLmcBHVvGy6pPqdiit
buR6Saa08RusmygTIjzbc10ZUD/bLB7Y1CWS6mWwriVXBg2ThitwQJL3vXfEWHF
mHiGR5uc8dVhU9CmzqwQiiFFA9W0E8wg0udV419m6RbmW3grmVC8xsk0YK7EzX7s
Mhv6dvIiY6in5dYp6hEcQY0sdxekS1ltHUVIaij0+z9zx0RP4XA2tkyU0ndXUwKg
kivonLqcBxja07NlCtbpWLKDk/N1JE+nKZLU9510Xig3obIe5C6oALyC50s56zw9q
5opiXEKZBhcieBdzTfBpYRE6dZfqbacTyDSgBzHo/84wY7fhNqR3Y8t8bZZJcA
STWQVzhjszD1i+WRnJJ09fc9htipj7I7Sec9nMvrWh+sCeF1/QY+rEqbhQWajyUi
NTnIwHeuYIqtP8xi0vxqmBFe/t/WPrd+r53Y010bp6lJWPk8bnxA+5v76gjHAIHt
utp3kvykjCbJizw0WfU6du/jgCXzaYFWK88smgM1xAJ9dXUkkMekx/kJwUr/5Dfd
eWMMKT42eG/JxFMeauRs0wMIXuAj+AJU3IHej9oYBZWUEmqid5ZvL05ZY07IaDo0
O/pfhG0YQ1mE8mCwlVqggUYfGvNfxBpAi5yikLMkTKP1YmKqfDDC3PvpDrqlp9Pc
rSMAnsYdq1H3K3JGoFdv4RxCuIhn65Lqz1s9YepmHnff1AZxEPHC5MJLIXAT3Vv
imEYmLUHbb4QskWX/KR/FuZ00zPGHzPIdtiS6TdIRd9yZwPFvF7J36zDVfEP6mm
kE7FrgI4Wo5aiz0FA4GZFXN6h9IlsFiv9izXUOmJfJwR6Kp/QF1ikD0Pf/aPiUq

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"
```

MII0VAYJKoZiHvcNAQcCoIIORTCCDKECAQExDTALBg1ghkgBZQMEAgEwggR9Bgkq
 hkiG9w0BBwGgggRuBIIIEak1JTUUtVmVyc2lrbjogMS4wDQpDb250ZW50LVRyYW5z
 ZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtdW5jLWwh
 LXNoeS1sZWdhY3kNck1lc3NhZ2UtsUQ6IDxzbWltZS1zaWduZWQtdW5jLWwhLXNo
 eS1sZWdhY3lAZXhhbXBsZT4NckZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFt
 cGxlPg0KVGV86IEJvYiA8Ym9iQHNtaW1lMv4YW1wbGU+DQpEYXR0iBTYXQsIDIw
 IEZlYiAYMDIeXDIeW0eJez0jAyIC0wNTAwDQpVc2VyLUFnZW500iBTYw1wbGUgTVVB
 IFZlcnNpb24gMS4wDQpIUC1PdXRlcjogUjV3iamVjdDogWdy4u1l0NckhQLU91dGVy
 OiBNZXNzYWdlLlULE0ia8c21pbWUtc2lbnmVklWVuYy1ocC1zaHktbGVnYWN5QGv4
 YW1wbGU+DQpIUC1PdXRlcjogRnJvbTogYWxpY2Vac21pbWUuZXhhbXBsZQ0KSFA
 tT3V0ZXI6IFRvOiBib2JAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNh
 dCwgMjAgRmViIDIwMjEgMTU6MTM6MDIIGkZAwMDANCkhQLU91dGVyOiBVc2VyLUFn
 ZW500iBTYw1wbGUgTVVBIFZlcnNpb24gMS4wDQpDb250ZW50LVR5cGU6IHRleHQv
 cGxhaW47IGN0YXJzZXQ9InV0Zi04IjIsNCiBocC1sZWdhY3ktZGZlcGxheT0iMSI7
 IGhwPSJjaXB0ZXIiIDQoNCNlN1YmYy1YpYy3Q6IHNtaW1lLXNpZ25lZC1lbmMtaHtc2h5
 LWxlZ2FjeQ0KRnJvbTogQWxpY2UyUGPFAWNlQHNtaW1lMv4YW1wbGU+DQpUbzog
 Qm9iIDxib2JAc21pbWUuZXhhbXBsZT4NckRhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTU6MTM6MDIIGkZAwMDANCg0KVGHpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMt
 aHtc2h5LWxlZ2FjeQ0KbWVzc2FnZS4NCg0KVGHpcyBpcyBhIHNpZ25lZC1hbmQt
 ZW5jcn1wdGVkIFMvTUlnRSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVk
 RGF0YSBhcm91bmQgc2lbnmVkrGF0YS4gIFRoZSBWYXlsb2FkIGZlZGEgZGV4dC9w
 bGFpbG0KbWVzc2FnZS4gSXQgdXNlcYB0aGUGSGVhZGVyIFByb3RlY3Rpb24gc2No
 ZW1lIGZyb20kZ2IDdk3ODgdd210a0KdGhlIGBoZS4Bfc2h5YCBIZGFkZXIeQ29u
 Zm1kZ250aWFAW5aXRSIFBvbG1jeSB3aXRoIGEGIkx1Z2FjeQ0KYGZlcGxheSIEgZWx1
 bWVudC4NCg0KLS0gDQpBbG1jZQ0KYWxpY2Vac21pbWUuZXhhbXBsZQ0KIHPjCC
 A88wggK3oAMCAQICEw8tJb0ROZdKzkJUH6HuPTQGirQwDQYJKoZiHvcNAQENBQAw
 VTENMA8GA1UEChMESUVURjERMA8GA1UECzMITEFNUFNGv0cMTAvBgNVBAMTKFNh
 bXBsZSBMQU1QuYBSU0EgQ2VydGlmaWNhdGlvb1BBdXR0b3JpdHkwIBcNMtKxMTIw
 MDY1NDE4WhgPMjA1MjA5MjcWnJlU0MTdMdsxDTALBgNVBAoTBElFVEYxETAPBgNI
 BAsTCEXEBTBdIFdHMRcFAQYDQGEw5BbG1jZSBmb3ZlbnGjZTCCAS1DQYJKoZI
 hvcNAQEBBQADggEPADCCAQoCQgEBAJqVKfjLwAljj+gBUCfjactKg8cc20tYJ9ZSe
 d6U3iUoiZVPmLcP3MUKtLeLq9r1mAfID1B/wlbdmadXPmrszyidmbuZm0pB5voVQ

```

fiLYy3i0x7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0aGdmnx40G/e3p1fIK
M0dPzZLo0AJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXCN5XL7wWTLMLNf9B
yb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWzB2zNS20F+XIVnzRG
5DeoULq8v88Z5bLpIJ/nx26r8A4SSWIBaVv4wPxAf1iPsIVKarUCAwEAa0BrzCB
rDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREE
FzAVgRNhbG1jZUBzbWltZS5leGFtcGx1MBMGA1UdJQQMMAAoGCCsGAQUFBwMEMA4G
A1UdDwEB/wQEAWIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj80eOr83zdw8wHwYD
VR0jBBgwFoAUKTC0fAcXDKfxCSHlNhpHGH29FkWDQYJKoZIhvcNAQENBQADggEB
AIFJeKCsTKcFqQMPTryujRGzJdYA+R9eBAuDLsatbtKt14FzkgRyOg31/+Cw7H8
e30iLrPIF1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUV2Z3MRsMtjH2x9SG91PEM046g
fPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7F0D7PfB
5v94M5274XYxW2W4uKGd7QGnUZROsVsYkGiWDP1JhqXwfDz8A0enITGXnoEkAFv
jiCqh64P1hIeMorj36pgL19oWZD6YrZSWHUz1F00juyu0fQsqm6hvrDTqNpHNZ01
5f0URza1SkCvi9GfMNUPoVgwgGPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+Gr0
mqnXMA0GCSqSgSIb3DQEBDQUAMFUXDTALBgNVBAoTBELFVEYxETAPBgNVBAsTCExB
TVBTIFdHMTEwLWYDVQQLZyY1wGUgTEFNUFMGU1NBIEIENlcnRpZmljYXRpb24g
QXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0w
CwYDVQKKEwRJRVRGMREwDwYDVQQLZyY1wGUgTEFNUFMGU1NBIEIENlcnRpZmljYXR
TG92ZWxhY2UwggEiMA0GCSqSgSIb3DQEBDAQUAA4IBDwAwggEKAoIBAQC09InoWDgW
Pk2af0+StijSN0R8K/hN8D+l078oullsk4ASvSwjsCNo7sHUA4xQU15J06VqY18L
ANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxpUbyQ+950MFz/evPgP96wV+z4TtA
wW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzys02kaYWTut3SryCqHEfBzFkB4u
rMk4xrIJC3CzWruS2Q0FHBBlfkgKN5wXVgkWFfi0ucfCn+IQsaqpo1d3f9jSkbtA
V5w3vzfog8919mXKI9H614KuElnAtJ7BtZcs17dUy9u9C0gEyKriVokFQgqQ7XND
U+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDA0MAwG
CmCGSAF1AwIBMAEwHgYDVR0RBBCwFYETyWxpY2VAc21pbWUuZXhhbXBsZTATBgNV
HSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYDVR0OBBYEFLv2zLiT
HQYSHJeuKWQqENMgZmZzMB8GA1UdIwQYMBaAFJEWjnwHFwyn8QkoZTYaZxxodvRZ
MA0GCSqSgSIb3DQEBDQUAA4IBAQBziaI2p86poGkjD/4Kkk0HG25nY/0eNARD6/oF
0/sYonX2doizcGmk53riugAocCn5zbzhW/JVdYn30UxfyrZlRAZef7GHqgB/Nyj0
ad3pdpVYEDh4ciNKjbs+aEoTWgAkoqEnt1sRxlcvb7HVX524bKZa1oPTUNlm6Qpi
vtqDIIdGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JCKzP0Qhp7poIccGE6I9Tsg+R
r0A9icQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz0KypyQ3eoZ6EPazX
qMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCafwCAQEW
bDBVMQ0wCwYDVQKKEwRJRVRGMREwDwYDVQQLZyY1wGUgTEFNUFMGU1NBIEIENlcn
U2FtcGx1IEExBTBVTIFJTSBDZXJ0aWZpY2F0aW9uIEF1dGhvcm10eQITN0EFee11
f0Kpo1w69Phqzppp1zALBg1ghkgBZQMEAgGgATAYBgkqhkiG9w0BCQMxCwYJKoZI
hvcNAQCMBwGCSqSgSIb3DQEBDBTEPFw0yMTAyMjAxNTEzMDA2MDA2MDA2MDA2MDA2
AQEFAASCAQCMZj3YztD01jbNLEaAm/3QumEiuQzGfQctH0akbQxvEdazDFQuz4XY
tnXnadpjedB8CrzjKdgp8A3ls1mzTSrobnZ4hEd9uhuMDgVRUXaEy+0rx+XCfBek
2fvCIwvVDT5dZ5k2X95CTtcAhBu4VcXo/WJEiPKAu1/p+iZtRiZeV4jZQBfquGT9
sVqKEXkhfyAj18pyn13y0MoX3AEnPOuFhEDm5Sx383zfzF9jvoaK5wOne/PzZ559
tzHJBnv+nQN7UpC406LCCIyji+hoEV+GP0m0LpClvUcRap1G5vgwshhHJRyje0t
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>
```

```
MIIX7AYJKoZIhvcNAQcDoIIX3TCCF9kCAQAxggMQMIIBhAIBADBbMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBtIFdHMTExLWYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIElcnRpb2ljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAAQUABIIBACsFMztj9S2Us6fsAlVzAPVWpbjptMKEGnAZ
b+17E/dNLBf1K4WiN2WVycsvg58WSEIUfRBxZ6BHePpS3+4Tg4PlmzBV41gGZu0
4eXWbrkGAwB0sckyRgpDLTmRpnN41czjVx4gSfkE0XeDTU5FCoed4i1jnIHdP1Uw
v7WWq/SnDrwVfBZZKya0Rpn58V299JxTjDKL1VKsCK5NV+weQo16deS9d3deg48n
dv/C9Gme0jUo0UilZCngEytRsGhJSoummFm2sieZ+ypP1z18uZUHfnJXPqPiK2Sn
Ji3nypkx1BJX08M3wsaifNGmk/Rj9mz8mXWkAL2RrhP7ViISsswggGEAgEAMGww
VTENMASGA1UECHMESUVURjERMA8GA1UECzMITEFNUFMcV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1UyBSU0EgQ2VydG1maWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAf7w9j/+bUK8AFDQHC69/A/xG
/IygoRihTfsSINKsaezVLHmVvJXq0iPDavHRvHLMQNE0lqLy5edKD9tndyLCk0Ty
xa8kQWwzxfRJHBq++paJMNTgdSLWpSMVxxP07FghXbJoHPRq5T1m4q6V0Hjixfeq
lvtnWcGTFhwDiW09beFZHZInMGJomRcgqHjToye2RkN8Vna0ySczcoW15yFqW61J
bW1bHVun8Rn80yEtw6XDDbnUgiVB3MYa5daDcVUe09npf+04M3gPQRDe27SBbmFm
LD3KfULs8Be4TBRVaNkuruULjidQ0akI4gEaSpAX3y+ALHPDFH4UbwQrr7wdizCC
FL4GCSqGSIb3DQEHATAdBglgHkgBZQMEAQIEEGKhWdGWZa/xZkxt86e1AK2AghSQ
hTHm2t4nNf1Tgo2kzG18BqDLWQN1UJVQdHShktmLMYXbJ3/qgZIm7wnh+1ZecrR2
aJ8yXfgWs8Po3atCKApsxA6eqUJN72NsrLIKiLSASXbsQHbRCtr+uJcs3M4z607H
UHplSej8FRWJ7iRY1d4wJM5K0TKS+VzbMgo6MzSnhlZKZtq0okDCVgfg7t0fZKEd
mD7fn4qCeMCw3nkorWSBHnTkxaPC2vjPAMaFbxuRgbdEtEOK1DEvn4k1q0ig961i
2b31Ne0VDTFyJLNa+3a466wj4I9nnwaQsH/F3p5GAJ11tVBLQXi4VVYrDsn4Xiza
gJMNmNBD4wXm2jKq7oT8KFTWY9vt9noH2qBgXYBvEkT0GDVx3gC5wCZ1YzUzUVS8
X0fA4xsZ3nb+YpP2ir6fXP0t7JvyRHV1LA9Gf18cQ09izQR4IebBu05xnn+XAp8/
p7aFpcIJgJtrgUeE96cv0591GCNb4pIgyTYYZaHyb7xNwbTWqGVhC+DQgNB8xiUT
/jS6QmOvXUMjSWULEaAeMGLB2NdxBPW2tyZxBpAh10wn1k0yPgxyBa0r0EVok7o9
p1ah7SOY+GA2UEXATAtmionaJdBdBTADN7Cc54tipN6+ILHaSBm1j3F3H/G4C1l6
qHatDbSeT1RucMmPW68GIERAKeVgMgrttQAoTNWycy+QYMKsZzRhmFirBsew37E
8s0crEx6GuQ0yXLCQCW+eNIfNqGelzZmg9oNKSItFfOMbeWKRksu23vKzRzix7s
fBk7HwCWwjSm1bHxr9djP2wKLK34k73LJCE6TPktH69tzbQpI+2fPFEGJASyTi
V3h2tjw/pWP8I4B0ScHYoJ0pDB2z2sio2MPXUKghI3gaS2UEdJiyNEBclh8a40ffa
scxnVAIdKffJcDvufTlEACd8lIOJSke9+fRNxvhKVk16rtxlovvnAlCL6HddrFD
NMFCbAVERIHYwXUuzj75cL99/X51exRFFMZP43s1thRvwVL0BDAhrm7VebtyXQHn
iKjdKeBLhQ+FovYjve1vMcDPn1iaWKctQqDIK1xzma/Ybm0AalrdODv06lwkYWeF
y4G/yLLiPDsn0TisdFwslm8756750TEIXw+y91L060Jkm7Q351dHPAa4I+mIc8w9
1MtqcU0Ly60nRHgdEJDJC5E05YI2wGUPqrtnNxydU2+JEZ30o58ATJRWhJRW29JX
0QViBhwmbaDkGGHnEQzjngNDqBLSgSN0KeDIYKPoGAza1b/cjhDmckaUM1cdA3Ie
3AsaCNIizoTN4LS5H4TpkD3/ck98B8RiDbWODUigG5dLAMU+096Xw1CPp1BwYc6F
hAF2n94fh0cY/PiSycXJm0VBHVv5K4iP+d+eHpcQrm0utMfccej21Uy8VG6cKCGw
1Gv8YuAK7Sf7yLF8p1NhEC4YWr8up8KFkaP26Vf3KvVWWQYI0uVqaTXECiq0A3Xo
BXN37nWnXe+tywk0UWZ218xpgirMTtBZjFSx1QV51bZY1D6P106qKHU34WijCCOZ
5d9bZ5j3dZmfhEHUjGHUWxON+JD5sAExSi0/bYGC0DMLSz54PHp0q0S1yPx4XKj
9p45RWpfDTrpdB9iXDJm6qvDOHUZQP6uMjyEAu4nR3XXJlb2rv+qXhrx2S0fu8zV
7T+uu+ZKPvU3AuVw1/ciCRXuXYPUB3jDEYHLJ8y7fzeic3hN0zq+Dm56B0p/0Bz
```

zX/fTa1hwaW0EICeeTTzoCMSKbak494WxpaE/ekoC3T1/RJ6xWhvjrcqB1KeY9km
EQ500ZghhZG9J1wLVuEDD//6cyaMoakTGqv8Q1Bbfxx++GRdUE+4zqFkB6GygywQ
wbJGy1rpYd1RpPNJ2/3zS2K+DTzKiuDkVo9Rn++AfLs7b1Zuke41KTnI07TTdL3E
MHRyV21J1CWmTsEPLjAbgAlNQNWK+EaIMenuD62foRyajGvtXahPAqU61Yr1+DmC
fQMLGcph0kTGoI2IJLf1U3dtRvI0eujpkjM0yi4tWVW0NdKF7rV9rP78VnXvCmUw
urP9o4oCICaCkvYPhYpCan+P0JxaGcSNSrY99HHIDoDLk5/sCVyMEs+pXy/9DvDX
luuWZG1dUU4f+2YZ7I76LcNXhUfZScKH6dPxxxQw1ypQWvdLGSQIXResiyI8XmTy
1maF7MZJjUUFm2GhEEExFLgjskww7Tn+dV+KxDek1ucCGxfXQb4tod++oJyFzcpNn
mLRFBJ1t6BQV8P2rkq0tbXzJ+uqETp5VgZHY0pMnQqNHu8+U8f+4BWWLZNE9j5du
MDij8uBAdZ8Cjzqlxnv8T2kn0KD+qoohmHzUQibGiVPM1heI5SuScE2wV9Kw5D9m
WApogFxpPFBhMLtPVVUvFp0dGpLSME+5D0b6JPnauwo5Kng+FndVtpiDPh/C2Xh
3GSBPpEbvp1Mb0V7DVUxuAQY0eFH43YVACKgQskBH7bqZdrhI70d4R/4xB7kYA0H
D65yTXjKyviGkRuPyEZjjkb1R/OpzBCEYh+sJ+OXZjKkOW1gxVsOnYUIjYjUe9qZ
YAavaev/JRFIo2ungs1bwgOfgpnHdghLUW4UAtZdk9b0ZkoUY4aIp6Q6ycPX9jbX
zCurW4hjRwjdwPcgr0R0YTYiKrnZ18m1t+SFA7GfVsJD06ivittMQptTm0aNI1
I3eTlvfTs7012C0/XEYBJ0TswJXNcukDG24bZayJ21WyYbqjEfwca3n7j0TZWLgZ
1oIJ3qrHRAw2urFXfsyGHKaEq12QcIdS2Lu0PVDdUdYQ4JL0/BUPqoT/dq2W8mi
ZLmygU/xCPAYngkyT02FLibbtBMuptz3SfEU3XVzxirHRGnoQXDxKQmpcvbPf/o
bM580RH+E+U6a3ETKi/yHUI0F/5iuFH5AdaWqGbWLAWE/TNGExGVSrYLaZpvhX
hw5hCnvqP/cti9fkYwK27EbrHsTsF3jdToTvddHZ0oxWIut+1Er+DKq48uDnF2Ar
vDJJmWQVBtuzxjAYtNn2HyByjSg8zuEZK6Iep0hA5v11tIRnrwpTaa2aFmeZec0H
OyKr087p4Qo6F0ztEXd650rzYtYfbaU8HvHfMkW9CeMCBUwj8obBYFu0eLPki/lk
1EU8JQ4/ZgarISB67pRs/sRciMgen9UW3WJXfh1Mx2Rk0GPGzsG69t9amb4Vx/WE
3KPSe5YS/hACUL+Hy9ods3ZGQt4yAR1Cx8NH1TE5fhDQL6zzDJ0sT0amsXZJGstv
VH+nPsW3AQfAfD/FWyFKJFCG6VsVhh60+p82ZGqBQk1YLZs236QVRmiUXPeui9+
0YRV1cvcvbybx0AWwRCNajEA3fwAGoin5Lw4INIE+oJPN2rQaCD8wwKRzybKRIPsb
r9mHB74aUQjmMd4c/Hn7liLnPbWSOMavxj00lbykQxjIFVYbC/yq7chADdPpM0Ay
j1EKbMGpKuiGqtuU3Gf3r6I8M4yMRAHEKduNEZNRqprs+aHu9DcT5GN8GJ8QRHYx
CCYwAsW1GX+oLkfJliY+hNW2EYC80u/E5ZI7ZssdIcSZbTEWMrPHTpVw6UJJPZ1hF
xVUWYwENB1QNuZnAkR7P9U15ZWnEdheoXaj0011x4ffgTvap167AOpf1KBk3m40W
N7h9hMX+96FWSg1ee0xu0F4ENYLaWJ7RwJwLvWfc2tos8/Xf9/mEWqsJ2whjf81o
rpi1ze0fQgOmiTFnNe56ghXZcTo0ioV+GGZAQ0EdfFWv2HyvBpfx9hZyKW+x81XZ
TJN8LvInqRL/Gr4R1eXmEhNEbvH1PAGAZ2wa3t/ZNEPsGvq7vvGW+rE9dudc1o7P
YooLVpV8g2IeEkFF09+DjrTg97j2FnJbIn0SQGR4Iv0HQOpJ1fMkWOJHQjTjbiNr
VcmrNYlo5yD7F5nQDZJgtJXctXoMNDdjFuf0Ta0yZrLC0Zjr01SRssFVMPgpm0Xg
Ae/I96d2PxAJA1wZBJWV5xQCekqIHnB2Jud7TxH2Vc4AsEEfbxkBFWGR/kHycX8X
ZMtDpPH/qPaJsh975a12WHQY1cQpHDC12jadQi5u//6VIg0zxMS1wHB3TU7Mt/FQ
YooIMIjW6n5Lekoi8u8IKQ+sqy78m+DVoL4XRZr9leQpvSukCWPeQEbI0TitYNrb
wTmakYir1Dt+vuzLDQBzF7pBNSxdZh3jKUZ/YYsW8/g/D4niekNP1sHSSY0cI6oi
wh+sSWm746AYtg+dBERBcTjQKhK45zcjUDPKC7tu6HuanP4HvI2fZMXDySUYvISH
GdyPtR29w+XX3n1Hy+TX1NsmyP3WNv61qdCLSWwxXTwy0Jwv1k90EkmGmd6APJP
0xeTXUozActjge40xvGa06uuLdXIfdwcuX4yxpj+HEWShkb0kHcxaY+byF0r3SU
Jbo56UbDHQS+OGpELp7HeJL5MVvcU9N00SGfKTFfK0jyC0j2rdeYsf5Hidb/9078
z5C9L5x23ChCvd2ipk0EwcwWYkNwRJW0T193cur5qBGisZQfDbw6xNS2PCI3zp9Y
21Epegrtxi4pDWA030EWzHCw7kcbt1WdzIW2/iaM0W7S0hHjcRboPgSzuFpDwEFS
M9k33iqH3vqfdrs1SfMXgumEzKA0ns1MEzNHPJzC07UaV1J0BgqTdNBaHqXSAfdZ
UN7z5+xnmdp11lBAbqNG4kS34JDEraArdfn0B5nQSYAP0yvu+Ub2S16/u91RYznb
PcjbtAt1Tc7pw6/0V5xNEpjRYBHbG5kPZ3DjaSKIakKJpS+zfMXbtr0HoM1TryUo
0KSPI/L199NbXXpLxW2tV0wNr+FexXYB4IsISC0Z331lqPTtr94rv+G1Z0f5KbFj
Rp30h0Wo7EKnENVLPaijraHSYI7f51nuDsIi1/ZFqt4lA9Me3Vu/Etv30Zi5EHEq
e+gVbiUb6Hivik/nnfWpDhj05LFLga7C6r0KSnlRIidj46NnzH6yeRkQuAcU/Fby
zqawmYz+1QfcyKAXNaqrIEbKDOn4ws3XHboxSJWzAQ+72/vqhzSV4ih3MLkDeWHy
rWmuzsTJk2cdmSwt1+dL8UfjRDV02UdHjaBf4Mr1KaX3ngfqibiskly/HFSfZrkK
DB+1SMASPLzZ7Gd6pPK3Ie8mzVYnE2SSIpBzgAqIs0ooYb1oA4qLLq75HfvEuJKm
mBqcjsGu0FemASbZzsxrPbS4ASQ6L2M1H5HSoY4twvQ3b0SXhzYYKi++hZqB7prh
MujPkThFQ1qyDvFHSdthJb+0+DtD0NRV3yPTkJNQTBEAVEPMEo3q87dkwAruhUpQ
0uTtA2f8ROHW3YM3AKVhR4ZcwbF3Z3CEzg6gR2zdcXSzyD090vyycryfmhA7Cnhf
Uyy9uShwr4J57q+XE/nYU4vgGhoCyyf4LT3VcX0M+Bun2a0rqx+7cxCyzVlHaaIA

```

3sZv5YQ2ZgQBd0YfbcWYGqxDH3SJoon7G7T7QWp3Mi1TWjtaGXf7GQ0fZPJWnlrp
H9ZCvxKJ/vKnM/q8BTsCKpbMqLc0bDL4W0SKioTp1UGqi5Rf0bW55d4b0oNn5tkP
1nRLHdR+vP2KUc6B4pdZa8ZiI9ujg7R9xF/KwQb0B7WYC3a3Gu9IADtj5Z1oCvbk
2JFQ0iUER+OyE5VmoPy7QoGmiX1jrLWsuwflnEbUEkd+qkx0uv84jRHCXFsgxS1
HZ9hdNNvyTyFrmZrv2a2QcSPfnlvGpYv+7pXL0gonnct5lc8PSVvuucbdV0R3Im
j9Hdiz+TZpE+XCU88jqHx/1CYbdgu6pLgkcmvUx2Ug464aRATy381PTC1eie3Xm/
z3tjOMCrOwkxfUa8VMTmI6gljeqPWodNgNtPLJDUPhJc02EWC2REcVAzCJGTnu8
LRfHAPMyY1DmbLg5QmmPh5zmkkjGSLaRbuSr2+k5Cd3XjNbE08dbJ0AEQtwBkD0
QSFx8IkC0iR03eV2+WY43wnaCV5pvCYBHE557V6vkGYeRGwTlRy/oGRQBKu7xvU
wfKLTS63XAluObZeOREWANEZd79TqTdsoSz6IYjbF2EKgXJly8tgfkSvAbiFL0MX
3mUdxBUCSbQRw5eITl/MBRZA/VUYxIgJMv0H6H01uCaWxR48S2Zfim/NsE7+BUmq
4+Ihx9ZuV1c1IDUxMCuDL0x3EjycQfVuM6loi0/B2qxHVILoMbldTZSavL+iWbCF
z2sLzt4b2ULzXZ/UUIJRY3efPlUzsKX60HAcim2IjCN2fWapGv13oXT3XiGvtSym
Ez2T7TpTetaK5n40+nEfIDBC5WH0Z744zx04fj42hTbFWzy/I3+aR5vhdK4yJMUt
pq8vrEdhzv4FJulxW7xUdJxgiBE5/YLHEW6EE2I9zhQWjLem8U+HdLaX1blnZu5m
vZgEV0akIGuuMV7dyG7mf8R0bqt17V4B0A0+cEugziyruHnHSxtLAvWiRP2Qrq
b10PERmJdrMQNCz3ZBNL43PHwc5z8S+JjNlgJut8YU14ZnQND+7Msb4bKRPB8IhQ
iZWWR3VmZfqcBeBNpwe8+1sVQcntUNViPPBOK4XWGbHuYaI38fMfsvghL1qvnW
ul9n5vE+fayvImn5m6THMcIuJGsQd5vYEFazUZHo4lL4RuN1MmbUT0sBvewyZ3AG
BrcDix/ZdpSafATgAfVFDib26E7k9baX6+3XWfj8be6ND5gF597Yo9Ad12MyVhs0
YXX5DeTswv00/00CbZQMluC3hgnPf0fI8FRLx+0ioxx0h8dxvTuhQ0vQMdaq9TCw
MNFfkyKt7RsFd18ZivEUvwy/sAIX9W75zjzNdZuZnyeyeNsB/XHR7TXgUKUUYw8Q
fjb0RZ0Iaa9KX+LnWhppOGIAOcB9NSkHv9mwmZ59+ZWoyYjH2gCpbBz8lBZyusqF
MBG2+EWVcXDMj6H/NHGEkKGqqj74X1j/Zg+h0drIZWXu8cu6Wcb2UqCYvkLvQB6l
A7Ihrk0TXY6pECERvfrAhWhVQsxBQqND3Fbc2Nk6vc=

```

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"

MII0kwYJKoZIhvcNAQcCoII0hDCCDoACAQExDTALBglghkgBZQMEAgEwggS8Bgkq
hkiG9w0BBwGgggStBIIIEqU1JTUUtVmVyc2lrbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwh
LWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1o
cC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KRnJvbTogQWxpY2UgPGFsaWNlQHNT
aW1lLmV4YW1wbGU+DQpUbzogQm9iIDxiIDxiIDxiIDxiIDxiIDxiIDxiIDxiIDxi
IFNhdCwgMjAgRmViIDIwMjEgMTA6MTU6MDIgLTA1MDANC1VzZXItQWdlbnQ6IFNh
bXBsZSBNUVEgVmVyc2lrbjogMjAgRmViIDIwMjEgMTA6MTU6MDIgLTA1MDANC1Vz
LWVuc2lrbjogMjAgRmViIDIwMjEgMTA6MTU6MDIgLTA1MDANC1VzZXItQWdlbnQ6IFNh
bXBsZSBNUVEgVmVyc2lrbjogMjAgRmViIDIwMjEgMTA6MTU6MDIgLTA1MDANC1Vz
Z25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29k
aW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5l
LXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbG
luZS1yZXBseUBleGFtcGx1Pg0KUmVmZXJlbmNlczogPHNTaW1lLXNpZ25lZC1lbm
MtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Y
ml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5D
QpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXB
seUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25
lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5
nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJ
lcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS
1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLX
NpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY2
9kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW
5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlb
GluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTa
W1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyL
UVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2
VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1i
YXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDog
PHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwh
LWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1
ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1
JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVR
yYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5
jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklW
VuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2
FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW
50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZW
QtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnb
mVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogT
WVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb
250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1za
WduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWU
tc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6
IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQ
pDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWlt
ZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21
pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0
ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVh
ZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBz
bWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia
8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAt
T3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWx
pbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo
0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1
E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0K
SFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFz
ZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJq
ZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdl
LULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx
1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaH
AtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQ
pTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZX
NzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBle
GFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lb
mMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Y
ml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQ
pNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBse
UBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZ
C1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nO
ia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcG
x5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZ
XBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ
25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29ka
W5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lL
XJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGlu
ZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1l
LXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVu
Y29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2Vsa
W5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNl
bGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNT
aW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyL
UVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2
VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iY
XNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogP
HNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZ
mVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhL
WJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1o
cC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1J
RDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRy
YW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jL
WwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVu
Yy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2Fn
ZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50L
VRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZ
W5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVkl
WVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc
2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250Z
W50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZ
WQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2ln
bmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQog
TWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpD
b250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1za
WduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWU
tc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6
IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQp
DQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZ
S1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21
pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0
ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVh
ZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBz
bWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia
8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAt
T3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWx
pbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo
0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1
E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0K
SFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFz
ZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJq
ZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdl
LULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx
1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaH
AtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQ
pTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZX
NzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBle
GFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lb
mMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Y
ml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQ
pNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBse
UBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZ
C1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nO
ia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcG
x5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZ
XBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ
25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29ka
W5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lL
XJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGlu
ZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1l
LXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVu
Y29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2Vsa
W5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNl
bGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNT
aW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyL
UVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2
VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iY
XNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogP
HNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZ
mVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhL
WJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1o
cC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1J
RDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRy
YW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jL
WwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVu
Yy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2Fn
ZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50L
VRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZ
W5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVkl
WVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc
2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250Z
W50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZ
WQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2ln
bmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQog
TWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpD
b250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1za
WduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWU
tc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6
IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQp
DQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZ
S1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21
pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0
ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVh
ZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBz
bWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia
8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAt
T3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWx
pbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo
0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1
E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0K
SFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFz
ZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJq
ZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdl
LULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBleGFtcGx
1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lbmMtaH
AtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Yml0DQ
pTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQpNZX
NzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBseUBle
GFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZC1lb
mMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOia3Y
ml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcGx5DQ
pNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZXBse
UBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ25lZ
C1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nO
ia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lLXJlcG
x5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGluZS1yZ
XBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1lLXNpZ
25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVuY29ka
W5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2VsaW5lL
XJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNlbGlu
ZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNTaW1l
LXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyLUVu
Y29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2Vsa
W5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iYXNl
bGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogPHNT
aW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZmVyL
UVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhLWJhc2
VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1ocC1iY
XNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1JRDogP
HNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRyYW5zZ
mVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jLWwhL
WJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1E0ia8c21pbWUtc2lnbmVklWVuYy1o
cC1iYXNlbGluZS1yZXBseUBleGFtcGx1Pg0KSFAtT3V0ZXI6IDQogTWVzc2FnZS1J
RDogPHNTaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmVhZDQpDQpDb250ZW50LVRy
YW5zZmVyLUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtZW5jL
WwhLWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLULU1
```

cHRlZCBTL01JTU0gbWVzc2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3BlZERhdGEg
YXJvdW5kIHNPZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhIHRleHQvcGxhaW4N
Cm1lc3NhZ2UuIEl0IHVzZXMGdGh1IEhlYWRLciBQcm90ZWNoaW9uIHNjaGVtZSBm
cm9tIFJGQyA5Nzg4IHdpdGgNCnRoZSBgaGNwX2Jhc2VsaW51YCBIZWFkZXIgcQ29u
ZmlkZW50aWFSaXR5IFBvbG1jeS4NCg0KLS0gDQpBbG1jZQ0KYWxpY2VAc21pbWUu
ZXhhbXBsZQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0R0ZdKzkJU6HuPTQGirQw
DQYJKoZIhvcNAQENBQAwVTENMA5GA1UEChMESUVURjERMA8GA1UECzMITEFNUFMg
V0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydG1maWNhdGlvbiBBdXR0
b3JpdHkwIBcNMTEwMDY1NDE4WHgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBVTIFdHMRcwFQYDVQDEw5BbG1jZSBMbzZl
bGFjZTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfLwLj+j+gB
UCfkacKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXP
mrszyidmbuZm0pB5voVQfiliYY3i0x7Y0qzXr16udP07k0sV+UdSNRFxrfKeoQEF
Xg0aGdmnx40G/e3p1fIKM0dPzZLoAJF5m500xzXPL74zFCWp2f1ZkuE4A6141ko
aZXCNSXL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX
+TWzB2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iP
sIVKarUCAwEAAa0BrzCBrdAMBGNVHRMBAf8EAjAAMBcGA1UdIAQMA4wDAYKYIZI
AWUDAgEwATAeBgNVHREEFzAVgRNhbG1jZUBzbWltZS5leGFtcGx1MBMGA1UdJQQM
MAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAWIFIDADBgNVHQ4EFgQUo1NB1U08gCkV
fAEj80eOr83zdw8wHwYDVR0jBBgwFoAUKTC0fAcXDKfXcShlNhpnHGh29FkwDQYJ
KoZIhvcNAQENBQADggEBAIFJeKCCsTKcFqQMPTryujRGzJdYA+R9eBaUdLsatbtK
tl4FzkRyOg31/+Cw7H8e30iLrPIFLWN1qjHrjg0yIs5AQ/hgxLvLir3hEUVZ23M
R5Mtjh2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzPEYPLror2X4P5uXxaP0
LIZRzWmkw1RF7F0D7Pfb5v94M5274XYxW2W4uKGd7QGnUZROsvSYkGiWDp1JhqXw
fDz8A0enITGXnoEkAFvviCqh64P1hIeMorj36pgL19oWZD6YrzSWHuZ1F00juyu
OfQsqm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgwgGPPMIICt6ADAgECAhM3
QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBAQUAMFUDALBgNVBAoTBElF
VEYxETAPBgNVBAsTCExBTBVTIFdHMTewLWYDVQDEYhTYW1wbGUgTEFNUFMgU1NB
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOfoYDzIwNTIw
OTI3MDY1NDE4WjA7MQ0wCwYDVQQKEWJRVRGMREwDwYDVQLEwhMQU1QUyBXRzEX
MBUGA1UEAxMQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC09InoWDgWPK2af0+StijSNOR8K/hN8D+1078oullsk4ASvSwjsCNo
7shUa4xQU15J06VqY18LANw0Rjrc9BaX4MguzsbFXBe6uFh1mVpXmFxFSpUByQ+95
0MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzyms02kaYW
Tut3SryCqeHEFbZfKB4urMk4xrIJC3CzWruS2Q0FHbB1fkgKN5wXVgkWFfi0ucfC
n+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9
C0gEyKriVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAAQH/BAIw
ADAXBgNVHSAEEDA0MAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21p
bWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAw
HQYDVRO0BBYEFLv2zLIthQYSHJeukWqQENMGZmZzMB8GA1UdIwQYMBaAFJewjnwH
Fwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQBziaI2p86poGkjD/4K
kkOHG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30Uxf
yrZlRAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENT1sRx1cvb7HV
X524bKZa1oPTUNl6QpivtqDIdqGJdGf8L1zLfxBuo2zL3HR+M9CDr40pq2JCKzP
0Qhp7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+
JJtz0KypYQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AjQJ5QfH+0e7NSz
NnEmMYICADCCafwCAQEwBDBVMQ0wCwYDVQQKEWJRVRGMREwDwYDVQLEwhMQU1Q
UyBXRzEXMC8GA1UEAxMoU2FtcGx1IEhBTBVTIFJTSBDZlXJ0aWZpY2F0aW9uIEF1
dGhvcml0eQITN0EFee11f0Kpolw69Phqzppq1zALBglghkgBZQMEAgGgaTAYBgkq
hkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCsGSIb3DQEJBTEPFw0yMTAyMjA5NTE1
MDJAMC8GCSqGSIb3DQEJBDEiBCAn/5Euey54zEPMTWTi6D1FzMPXZyPmKLehwiHU
u97UIzANBgkqhkiG9w0BAQEFAASCAQClDWAb1Y3QmHJaNLnrFOVtdBYsVLQoKmlE
oajirYCQ8fv1D9dKnCP12tRdshOMtV+c7sR4wW6XNQNBDLh/+zw9aV32quYp1m5
LmvWZJnmbVCuFqZwG/frYlk46SXkggJZCFNuTKRnIBMERuYtyR01QUX3VlchX3NX
n07FBEgy6SwD6avoVEG7pG11J6xlclUh0L14aPcb94LkcUHPNj5kSet8+k1HQw1KR
VCjMvXymn4aygpSkiZT35CjFhZmAoEaFUilf1354s121RjXMZZ/2fLho2SzWXCRA
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>

MIIY3AYJKoZIhvcNAQcDoIIYzTCCGMkCAQAxxgMQMIIBhAIBADBbMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBtIFdHMTUwLWYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIElcnRpb2ljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBABcSvh6m3bqMqug7JtspPDcpNnbUKLh0maZf
xtgFkNpttPxzo0rbgzttatlFu0HinFXrm9p3onp4B/J+UqntN6mGVog0hpbBeRFD
xDEEI+2rs0NPk0qKSTmIrPSu38mHMTUCfYpXegNs6Ez5pxf813Ack4X504qFKjKc
P77YqBvR0Zq/LL20s6+kTABWgPsRP13LUNUbp4HUcaQ+SH3uZp005IzFrboYrDb0
vDjLvYKvfjraLgLLzFW1Ie2eGLQ1L3ri8hLMIWq9MX3hUlegegVyKo7515i3CTo
cdp+8YROM5zWx7ID4y1lL0gy77wZrP1JWLUA5jloPOB9omzv19IwggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFNMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydG1maWNhdG1vbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAVPILzTVhXASgTJZHlgb/wSMv
aGSEh6a4nM5Y1lTEfVh00IXIyrzGMC14HCAMLkrmjDEnXtCvMHMd5vLKJB49UX1s
n7x8EKYLqHC3RJkq18DN0mnIJ2mr9qiohxSQN9ie//93a8ar+kKgr12qRCTtgTcP
b6CXHVWlm9FazwJlC/Z0jS3YY82Up/P8cgXEbAji09ZIRyaUUr1jr1I8R5ivjIPF
cAFtnkcZ32eyahNU97pmnF8nZD5JUxBpQ70t0qemBBkJAY2YcqVzzCJG1se08id5
050gc9YTehBq1EbU7HAUshMw+3T8cZgH22vec7HJPvrS+BMvPGLNYWBGyvvC2zCC
Fa4GCSqGSIb3DQEHAQAdBgglghkgBZQMEAQIEENgnBbo7rgFT+sfWGsbyP0eAghWA
eDNEsIoFnkJJHi0W+TI6ecod4Gdyku4qQKjULEzI35mhJhbof1/IrffWdG8CAdgf
VYjItKwG0zu0W0RRJtVqaYcjcDXX2HXcgz0QjsLwJETWR6n0Z92PfYwJki0sW6PK
sfNZPRnK7K9Sb24rE0nMLgb3pmlXXx9JsH8LM1TVuN/Jmk9wkqSwDgubLMix6eFS
QHtPLys0YLoIyli/sw+fI58IzplPsCzpuA8z06jptlroi3j6iCWuSj2NlFhea+c
t5PVR6I+UuGhgCj8VaQisat1yFyUL+joeD1EvDQK2wMio0iEpP/m7bJuxi1malH
RfdkeAWxLf3A3P1aK8gBxVGE03hFyWjmdw+h0JoK/AEK+0q2ctSfyc0bmkz8TiHR
x6j68TnDkVUpAud5NlW2ikitk6nsA4c9Bj99Br/1LqKonmA357r2sYG1vEtxviJ4
pqxZhHiKsIs0D/eWbheXuXkbT/jrEDlR9ibSuRXmgq8JV40tQtDvUvdVTq/h9Xg
JCR1zj0PWUSAHyziCg1yDI06YLvHPGFlxQtT97EiX1WRAlkEGL//W6v33vkhXTJ
oTYyLr0U3d+oQCILxQBCIrsB194p1t1NjeEK79NrMs+yhRAQ6Um7ckddPBWKHM/h
AcOPv8oAyu8eDTi0oJv1ZKNcGIc+itQn0HyMHBBC0sRPV0J5MIZcgdw8y0e9pYbj
4mY70rq2Ii0nrjn+y2zr0rswfKB73fQNdff04rCTbzLo4x0oH0B0DSdQJ67CmtJ9
hBKLRjb4PPd0sdDaAjTFnVY0XjZUOKj2DUhDcDBkiiIrPf+PgOXtE5qc85FgzDZ3
gKyAnaKqEnVqYbmEhSKMRJ/dfAWrFQQBX+5Da5tp4BSRxNJ8glP+fvr4W6jftPF
9R1SfplT6XgPRgrHaDKc/l0rAlis1JaGpR3ggYB+C+Bd9DVD1MAmuVoWTw0LNM
pJnHCHSLsvR9HdcUuobIOEVDspIitfi3Phn5KGfGZ3a7SN5a5gX0+l++DuX3PgZo
x+34fGY00wN9EdtN0qxu3PqfRNYQr6723oHh4aTxwx2P2hr2xCp5t6aDWFie+U+n
yZ89q8f63WUL8Goo0KjnuXp4I96w6/eG7ixLv0Re2QuAFSEvF88NzN9m8CiZ8yQd
PJGPOqbgeM89CbM1oFoI5p+PsGgtZp1vxPti0pv0eVyjlwBrGEX6P08iimAoe1HB
p+Sk+UdmAUGmxGFLlg+Ju2PqyIMRrYc4NV7cTi0S9NXV11F3Pxo4aIQuVv1HGJ9H
7x3KAcM8679WLTjXTNcDifLTxJlH7RO+Ut1UMc4gHZ5Mq0I2WLXWjGW/UJ0cB0uP
Q0AsWvpDso0Fw69qPooFBf8bt4Cjj0x3Z1IWIGLiva61ct2QQjnv2Mo5ccxJ1qoD
/Uw7FjCGj5NHCHd0P0o6fv7Kc2QyJSJB0rjgRI3dbeZ+N6h7kyx430JaLvU4hXiY
B3CHeoea5y6YrAv8nAmhXgXy/kaKISJXyHmWTAP5t/z7eoCPYbUNPyKmNEI1iYqR
swDc5ENFOQFhs6r+xbak4KEVD8RLJP614KxzVrPZyPE5mkmcZ3xWK/YZcUhDKZ0h
```

XqKx5Jh83yWMQ8VgGxqUd/rhU0ltSnjiRpmW0wGft3fLh/x3AD71j3MEKrkJHSBK
eu6HcC9ratgaCXunlbvcx6Q0x/q2fb+eyEhFtSoZQwo47NbJHUSYvF0jqoqA3LhH
1j8GfPzN+sLlkZ5HwBtdIAWXTQ0C4epY5n1BYWsRCeDjKl/s04wR+VbGJsrPQ1jq
f7143t1T8yMS5g4iIpjEOL1RL/WoPYL3ooIz8tCCMQQh3qL/zaKC2iZJaj1gy4y7
dusQQRv0azSNNWjK+1WYbzabodXHsQ3R87TNq2CNWRIEcRkYibeBEA1xWvECf5TGh
jtOnkEZcIFKMHnYpIK+9D8yYtuCarzo18BeOyuQN6LWZyMiNOZXm0rvzCIzq0RQF
MI+xl4WJetdEt6wwFiskTVGpJPr3HyjU9ageiNSpXq17+A+DMCSgaQoyMKRt18Sf
tizJCqGdWD+/S6izTnr4voJdsJ3nParNlu5Tf+tz63S3APwbj5uS9qoBR2Vas3cb
IVNgTwURgznpRa5TX0+sDlSz/nNMr5uZAXiS0RearVtOyK1aTM6LZ6t1Yf6jVh01
XZlGcmW3hW5bdN0UMBmgZznuSuqA+0rjCJsHoPUw+3ubSdegmBGbIa7lyeuGGyJZ
sNeB9KdddRm0Cbk+0RybzDCZJhPTHpw8yqVi2ht0s1ZE1Aa3obCrbVEU10xMs70L
NxdPXZPiv/VDw72JECmfKUm8fTbQfatWeM10U9m0s7Eub32VH0V3RbB48bnDrs1h
XL/ZUs70Y+csMemEVy8XrbBvNuhSZLo3mdD0/XmDYrCxa5pK0hZmIt3PGeamYRdf
IQDN8WsaNGIDSPN3w0M96sJWhn2pYyErwpsSiBMRnLmz71yo+embXKJWTsxTXubN
bmCIG5vxJ1Ew9vxqj88y+sbWrpI+2jUT23GVqy3+/iSruFtqZL7f4QNMmemCWq2SC
1m3Bis0q48T0bm88Q6B0k8+owhjeG7Ky1FKQJEZvJE1NSisIsEDQQRfzwGBgpDyU
D1diWrCmpiynhq0mBDe1jtjIHQT83knRiY3XbSABr57w4TM9SLCUZ+/b826TpMiX
hl2aKH73/zVPH6PAamxKCub9YP15Z00BHKKi0zZHQQtesEH54iUGY+0+1/LCSuQ/
Q45Qvu5CnWBFx4sYvFRtJfMyna1AjUbWfQK/BGnS9H1rJKYiX1Zr01t+/cqU+r+h
P0c40Aey0Rsg+szBns4y55gWhGVicyNU2RRqNg3dsy/sUZhysFiNbyWF+NCXsYa
ND79DR0UL4nm7XVXjz6y34dRV7u00nWRPRWLbhum/ekv08Fv03oEQ6sfJE1hx5M
6fNV8R+8849k5oZKFxvsMb6sJU6N8hXgpMq1CODGH6KnizJZ0xfjJhMgiyEX9h8J
CSV2noFCpbDsIu+JK0Si2LFCfj8wT35q1hsdrn16sUq4/crG2NMOZrYPHh5Uxwim
nCGWJm309+TUH0CRV3JmU4t/Ls1mdduErr0/W/7SF/pD6zCg11hmpHBKFu2mzXTT
Gjw1JuHSy23yzQ3x8kaZLkw0tNWV0tWz1HdjBq5TX0GU/IBj0fRbnsSxC8btiIFS
ZlcyVfRphNT2WXgXZ6pX3soWiE7rkj8geEsYkQLIT1yTSYRz1X98NuFUEgrgTWaN
j0VgflqIXf04UrMhkHp/cTcAE311b1LaackHTdRiJ3Xciubs0dZrIuc2AlJYJi0e
ITdAzgFKx437Hh9MhVdW9DC60sa8b5FEesiexc4ZRYBALp+XCQLiS01f1UoQxXLh
8dvr2dAYkITswQNQtS07FJlvp3ugNNW33BJS2LGmaLhvosBh0YngJx10fr7Fbkyb
YHenw90TSy6gtF37j/xmtUjz4vI0cToRunPh18fUJjxQbaepXFw6M+YC2Up4S0GF
sZEAvoQqjBdXezU5z4V8wz4hgPcuvb5w371+fp50lmqHjC0FHkwi04JdinaetrpS
Nwg/hI6d5A2s0gMed472SLP2bR0INNGW+DZKtewTC6WqrniR+WT/TcA208NNsZVT
GZ00Sf5/Kd+HR2apkm0Kq5hIYsDX84Ji/eY32jHZ09K0DfCQ+zBatQ00JU0pYMEq
lDLxoXKV/qUuXEp34foZvZT0699btpmPhaD8aTKL1FV59WD+TwdC15n7V6at9Jnq
kqe5AVV28faXxCi4LV0JunjNlKCA7SuraGVayRPEL5SG7dUsqCP5jFPowHAZgC2K
Crr+zJZgwYJqTaUI7gKUAsxph0bFqn3RL4Qhnc6b00Zx4zVcwMIWTDt0W39JZrnz
3ia0x9U1KvrNlnLMD15xPro6Xwhq0D1QEGZ0GaZmByTZ07Wkvoe0kL3s8s0xCWHW
bjoWyd6grxeyfPW3ZY3Htr3nzqfVovFupFbdj7icm/iPM+B9gw+0sb7IZ11v9Hmy
NFx6DqPDQXv0Tijea66hKfIyxPMTfZFZszX/K0009MNBX70zAibgprJ/fK4VYUsc
NPSJlHZ59DWPAAZZEaCaolcWJBxvby9ycir5ydpudQUpTN8z7agosdkNPT9hxGKz
WrsV5hxe1nhDklG2VJ6ohkCbiJawB08pZE48nE1r4cwYT8u/CvzfIHx50SmXN20L
ugVbTDygrRG8nCKKkym6hqi+/0kzHKRk2V48HAa18CNv7h/iVz8R3a/PyGD7cc65
w9fDjyjpeX40hsTy6tmz/7dZtu3lFznNDUYuU/lDqDAJUG40SGSwCUzlp6TRmTZd
z4U+26pPW74eKJ1isz8QVfrDEsn3Jk/IBE3Srzm1VyfuVxLKYEMXARAJosSVk5pz
n/rM+gIKQ0hXTUYIyoKgfe75SXV4fSCSy1GHgdbuub461HDEXKvC43qTbQkh01Yp
5u40jdfdXcq790GfGL9Ns1VxTVCCpTrQc9n7jjkplvBXQXwDXCfp0qzTar6+Nkcw
EL9r2+5PsV0zw5mpHDY933W9AkVaLsnqxyVsFJz317Up0Q7y0yqM8ecA+6SW4gAh
Er7UHCemljNidhLGdoZKjMijDGRAiCiavFi+nbihkRumrDhStQHKqQhfTU7JyiLq
UmWN1hkPax7Swc/zBW9J272LgYV40mQfjYNacY7KaHu44xGda/SOrMeUnFPZB0mU
edkdsuG/jhVT5UgifiL8SXnCL6DzyA9Lo/IDb7PQHUhHEhWfNsWd1F6qAZohJrdqq
lDShd+g3t+MBshapvaXtwjI7DbZ3WKRfeyhdy+Leml+Z0eD58cR1N3GqCPMRyWa
+fEvrVdaJBizTXgeph3g2Uc3vjGnmNH4x861zuG3+5pKpONV+10z33noByApeZg
GrV0wwXVZQfr76ZSR8wwLpAy6EvJ9E9gCMC9Q2R1JzdZ93hCqQVn1srocqu9RYD/
YL+P0Mafk7TpvEJmYvAMMydiBUfGkrCI0Za5J3D1oYZSd392gt9SYeju+EZ4HRJn
usZhz6T/eZpSNJcVEgrHSORi9t83o2Dms197VyVE10Y52KgpF2H7sGTauWuMwJJO
MmaW7xzG1mP7+4miBs33urlijeToL05EKXD0eEL4l0lddLHmHQ96189+orgzi8qt
kB6yeEFfwK1h+7ilooPmfSaQj5Re6G8HK82CIJaVH59Yo3QoCIEAZhcnxMKrNJSh
GRC5+XEntchPH4iDyGC7k5Du0CfNKNyrFpJ8vwdGmNZiqnEatCtXEtzqEo4Z3ib9


```
NHLz/bJzPPDqG1sLIe+fv3Cpb9a7G9uMyn7ZzAcDarsRCJdjdfst3NG9Jeh2LeeK
vEDFK6XyQiz9QxCqNqdpEGgUff/zuWMHaXN9RmR88uyNPN2mClnF1A2pY8oRhdVC
kvF6urIbOPS2Tiih66duBPd3nF1y8xFwwCCjgeWSffhzVRfvpdqZ7m1N4GimsI71
o6V6ztsVM7A247X1jOZ1/WBIhF1fyMF/jf37Rq6N7FAFnMOZWSf0b+UTXexZs6z
6v3PbA4grpEC9U6wDD06zq1JVdAD69Ecw/IsLa4uhoJNJa4ZmXxhPg9gl301nMla
z5LMu1GDShTgb0UYA6Z7E7WGDm1oTYPeI+01ZzPDzpc0rKd/QqX5zhSAAaYqcuQP
Zi8S1C0N6AYL2r0bAvrBCc3oKUGIAXCgc1tiRrt8jW3Tm1HylgtX9hHxmQqx5Fwv
EK/F2qxnZLpwX6y3ooQncBIn14TC2fGTItbAdwReyTZjLv6l13zSgGWNjcdXQFPz
koLT4iykPcFXJARB0n+TQqbEQC/MkZ6VeJ9DHYhmN/dXIAx6aVWBgJ8yKRs/8YK3
QhAzQiza0gtluVA7cNcrVk1lk87Ee6aeYKB94fa4Nk142vukEerCGXNUW+wZfw07
wK/+yCh8yFIKSeZPRk9hejMCCuhl9rLoVvXvr7k0p55Eugi8ioBBjnJ1Hj73p2dj
Howx+JIEFrT526Zmf1oMxnjT23+mW0UQNxQGvEv4/+XdfR+mG6ah9xF0b1MD+9oP
vVqHxsdUuLtpqPqFwmcg7JmbWgAB+tvCa4ET9Sg6yID0UH0FenejcotqaltZiDRGG
g1YiI3l1BU9CASFmzN3bXVfIs4u6RyYHS02VTNA4A4Uen06chZkWNxYtb1BjImn1
6IG49GlfT0+yhtk38Z/JZzB2WcVAFNExQdgx1fPQEU47NSTa8EgyJFD+0uwr6A1o
gm1e2S85ViHL26YTzmDP1CH5CjD5/ZlBl6m0BZXt3euA7hr46zFe/XCa5Yq1Uu0s
PER2c0UlvY58rEiJghTvy3p9sTbAj9m5wUef54wivUXXo04LoZh1leHpiFdi1kYJ
13B1KWKs9HwLijv3AML+rS0gWZjT1QLDM04RohzDJP1GKRmMp0uNY2RtcQeWt7hv
IgNqyOb0BUtWFiQye9lpF8rmtsFTfQmFfYmcALTvGqEAL/hQbYYSZLDHJBGT/D0
FM1X8K83o3do1IoAYw2kBcm7bHLAXT6e6WY5URJ6bhpYk29GpLIe/RPtbnLefqW
0lzmofzU6I21VRqb1A7NrWge3UPIx++mImi/qK7n60S4p0Rq8qvpZqoVSGWNE0wd
QQD6Zh0RzjyB+H52xyGZTSb5GqJBMCIYw/2ZiH0HGMbH6iqChMT5abMzkCFejWlX
LHtD5sz1j5Bkc1ptpM3jYoIwFLB1er1QnNktOFFzJejj4f+0i0DBIFYxkac1zKx
JdgkL6orA2jZ6AE5Bv5QbinpUySz6o7hlGvi2bdjnJuti3I3dtaMnzF9BJxl3aqN
sSsm0obh5ds5xURSxhkK1Q7T3buV/hMZlsBakX+xmHA1eA8uWYRQqf7KCQqGem
6Hk01xjz797mSnpmi4w3LrI52MSjjXdr9sf5aCcLJ0Niok5I6SL0NyeH7TwaKMZf
ReMp83rBGP+KLEyfGMp0/PuMajQAsqXgJG89T22tMq1+G1uGuWqYW4GI3Zuk4mDq
ygZqKcWHiR8wvDjppzTiuvQegN/K6MIWjgKRcfPmBxI4KryoKK83Xs7rA+z6spK
zJpUtlGSV24ooyVcWy03RQ85Gc/HMMwP+z0g37J/YZASBpqjv1SWxDaK8ZzR+dEJ
1EAhJ3uCRenTRURzMyrysBdLayLFW+gHuDfC5F+INKPGMertJqtYdf0s0tqG2uPU
JX8U3mubey4B4G3j58ok7ZBD4r01l+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
hkiG9w0BBwGgggVZBIIFVU1JTUUtVmVyc2l1bWVjogMS4wDQpDb250ZW50LVRyYW5z
ZmVylUUVuY29kaW5nOia3Yml0DQpTdWJqZWNo0iBzbWltZS1zaWduZWQtdW5jLWwh
LWJhc2VsaW51LWx1Z2FjeS1yZXBseQ0KTWVzc2FnZS1JRDRogPHNtaW1lLXNpZ251
ZC1lbmMtaHAtYmFzZWxpbmUtbnVnYWN5LXJlcGx5QGV4YW1wbGU+DQpGcm9tOiBB
bGlzSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NC1RvOiBCb2I2IGJvYkZzbWltZS51
eGFtcGx1Pg0KRGF0ZTogU2F0LCAyMCGZWIgMjAyMSAxMDoxNjowMiAtMDUwMA0K
VXNlc1BZ2VudDogU2FtcGx1IE1VQSBWZXJzaW9uIDEuMA0KSW4tUmVwbHktVG86
IDxzbWltZS1zaWduZWQtdW5jLWwhLWJhc2VsaW51LWx1Z2FjeUBleGFtcGx1Pg0K
UmVmZXJlbmNlczogPHNtaW1lLXNpZ251ZC1lbmMtaHAtYmFzZWxpbmUtbnVnYWN5
QGV4YW1wbGU+DQpIUC1PdXRlcjogU3ViamVjdDogWy4uL10NCKhQLU91dGVyOg0K
IE1lc3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtdW5jLWwhLWJhc2VsaW51LWx1Z2Fj
eS1yZXBseUBleGFtcGx1Pg0KSFAAtT3V0ZXI6IEZyb206IEFsaWN1IDxbG1jZUBz
bWltZS5leGFtcGx1Pg0KSFAAtT3V0ZXI6IFRvOiBCb2I2IGJvYkZzbWltZS5leGFt
```

Page 130

```
ZSBMQU1QUyBSU0EgQ2VydGlmawNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJc
OvT4as6aqdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCsQGSIB3DQEH
ATAcBgkqhkiG9w0BCQUxDxcNMjEwMTUxNjAyWjAvBgkqhkiG9w0BCQQUxIgQg
48aQJVg4Ai/QpEFw8rsxq2fGKjdKAo7F9AiyJ9AcDQswDQYJKoZIhvcNAQEBBQAE
ggEAVvcWqGsebWjsEhsQ1ER/C5Pib2KPH+9KhVGFbCjDFZvBmNk1EI2YomGPyrXq
OoPdQE0pVKLXB3M2VfV9BotUyXNQRR48gRU/P2kRGcl0naK0kzJVnBQjuNkcTTDF
+CHduHMFtcBHNmvWn9TsxhzIksqIWWqTS2ugc4JGJ+0h9IGX5HBpFcuXU3ouznUt
RQDZNZuiqo7MFcw4z8uJXHXiZM4lWici8jlSs7Lnt1UX01Wd/K8rTJZZZ01zpEtD
vjVftz2p54sEevwkS++c3eM9MUyNYT+GC/Hm2m3japmH8E7grmssDeo3d4a1aKy9
wd7sRi7PdwAgwUXi0uso3yA0qQ==
```

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>
```

```
MIIXnAYJKoZIhvcNAQcDoIIXjTCCF4kCAQAxggMQMIIBhAIBADBzMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUjNBIElcnRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBQUABIIIAEY/MQAP8JUKxGJR2+gL9fUy/gTYqzyKkkZF
GQqKBR98jCom6wtry9FqxMqirrkIXmy6QgPsFh9nf6QmP62K3QjP/aGDI2VLeKJk
beQfZRRQCLqqsP0MRQLT2d8lAJAHC057N8tdm3jXavSWxaZkEqWF1rtcVCz2QQRg
iKJ99BPNEjwLLK81VCjxTkQ0cxRgUNUK21pMQVFoltXE7SGVjV8jeEiEHj9q65nb
ITmfNgmTP9oNk8gojEj/cmTy+hHGPVFjDJZxAHtd4tjU4k/LP46NRAW3tmax0KMP
v/WkGMcYQGY+qdaXn3n2Fp5VCTfJjFW1bZHDShW63kTGr+u0QMwggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFNgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQUU1QUYBSU0EGQ2VydG1maWNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEak75ys1csbLhA8HayfcCB6yPP
70o0/9hlsazxTzL8NcP/f3vz1VEdaCXKGzQSWRSMgf5RoxQvUrFCTaq/F+rbGM7g
S03e1DfxGb8wUgE2ZeZB1o0GvSd6eNB6gjajEJ9AEHwpT4bEJeh7TQ/Mi3PDwelF
kbmA056B7R7529w55YeQF7ZgsJxicJFp00ADPw8iYGd1b0j3wGt3Kz5uycUqsc+4
Q8VWlU5N+8jeJRDVPtEQJwa+S2HyuaPLUZcyZWkuGtVA0PRyCqSjtGSwenLmRTGU
YtwaFvQ6K5E+vCRPyIAg/HYwaYNeUJn5Cr++YkpNBofnrofxaV8zKRIx96IoxTCC
FG4GCSqGSIb3DQEHATAAdBglgHkgBZQMEAAQIEEHawOvd97z0NJQe7ccQnSR2AghRA
lqu1gwka8gwMldV4laK3pICE0Ta0bvJGW07wrvSEAgZU0bXjd3ekfVtDGWgXhWbB
8uaam5ssV4WViD4h3iZ8HTRPiczbSsJ2lF8CK0wq0Yp8VKQ/wy87yVB6Mna3ZHCT
PqyE0TYTsc6nrf9vQIXrE6I0Roa6FJ33+PpS312CglFyMyhs5bS3TTt2xwnBvLJX
HoPF8JwGxe5xkd9xqOC8jjkMdBcUM8y+DRf9vcDYLA0NiuJzpaixkEVG8lFdsXtz
95b3Uedf7Xdx9ep/gnqfeVvDLvTjUoxWa98KUM+ZC0bm4gHhTwdP2itiUGMiGYZf
yl7WICIW2jVPVZ6GGrcE9fYwqsG60+5vygpte2juAQUkwQ74PIcVY6sSWMVbFmfu
```

iWCQ070XmND0tcSHd8Uh1uqUGQxNElzfQJoKc9Rz040+jSgSrenVvfwR0AtZy24
WnvbnYUHEsgmcn94eHBYow7fqmC7N63kTwtr4NXuMAEH1MvW1iVkJNyB9ZI/D0Cr
0fv+/yPflr3Jobx94CYnP/FRqir1h6d01M9RonpK5wj+YE12zNUmegCDizVCcuvP
md2nj91RGccyWgmQ4LPrNdMk2+nQvKNm9Jrv2iHNseyuwGJrc9cczv1/E3Xf0cnu
mS8Y4iMPY/wRnIBN5+D8IzgWXvhMEGumwtT58XFL9KwrLjOKRvai4iNIW6K1fh8J
hh0D7HrdneBas9x0QV7yP2TMu009LB1n0M90A1IJAA2LNBoML1aaeJvv4/AzTIEm
GEYbVIXD3ovj0jm9GCEn1XNgktaTJzt1g+u1v3bsU0IZZcNGdsiUpMY5a4xn09N
7KGyn0K/ALBt4dsfY4V0hfQ7HrgAl0s/p0/6bgfGfAu1207nzGUV05C2gvn0HApq
tU0RpW7F59q5rr/EM1MU4RIE4RtsKFv/jjLVMqwyQ8c6SAVsdCUNCqWPPN5KPKne
B7NQ397Wfrpd5+f0IiQ/g6GQpSpiQjjfZW/tKq+EGxVpHqrM/wtM9W8phh+rRas9
meavN19EuB8aJ2gjansk/IezbZkUuN8GUzhFxEQHzSQNADeWjt4rnPaBzPrKzDlH
MqRk1j2LrH80h4xBzimpEz4Z+MzEY13pbdu7g1ZWYTCiewHeyZbIoRZNLfTYG6rY
uGjEX1MHkY8HarcAqii4Uk5Kti/cEoH6b0Yj8zIlcGxqiA9Xha6jsaG/BkRQS0Mm
/YqBx11LNoyiTV/VC53MoHfA4Ro2/4YrdaykBZEPoAn0mM99EUDgm0vqQeiKLD3j
IePb2udTgpPLHIR6Nw9XN1qiUxFyD5PcBIz/JNY4FbZQ8xWB50piQNm8zL4Q7Sim
6RH13Wp11MIU6FhS1K9966Pjkh/nMnS7hPtsH/rBXxrgFVBv75Kn1gmccadIXvQh
fgZTXjXDgw+7i1NxnJn7c0tCgZpuGM37TmjIXANDwBCSJHfeVG4WdJTKsM2NXJrzH
9uFOUnhwY8LLmy0MJ4BgYMqe7cCHBZ+ElS7bbUCA3la4tYXQKQY5Z9XtE3bst8r0
2fxWkwF0qncK/giXEHsURYiMr9yc1T0LGfF3jSxMahSohnBA3cKHBww0Y5Kj9n4L
kemATIjN88n7IazxyAztz9n7/I2FXmPatu0W8FG5QBoIhfBw4cunuHkzAU7yTSN1
MNCjYW7FL/ouvnw/MY5I1LySF0XqfJ5JEdgfk1gXsQKG5g4350i1T3I4XWsk6h5j
dJxTS9v6U2efWIDWYtAKqi0tNnvcBjJQBNx4zt/sPqqU6dCTS3tn9QdYm40EuiF
aEBcna52jUCncF1EETp2S+yy2ZudNOUysRGAfy7maNGcqrUuLtXRfa1xdJ/TBYhs
w1AwdMKtakFv6dqu/h3kMBDEqcu3y6pWnB7mFlcso2CUkv7/CEl0cg6KN0tPz5k2
WAin1RylzYjBkr+0oMexQXQNSXk1Zf8PKZ9QBTfF0iuiFafAizyAGao3CebY6WNT
1ewkZBAMoyM3iFjvCXjR20312bkKSIZopA0FFIsDsGwn3ILZmPWq/9TcrNvqPTKI
WzyIK1m12VUSe60tvGShW18wW7BNB1sZeAi8naGvMe/9Jm0ShIJj/neKxgoivxrV
oM9B8a5k/qB7W9tecEHAYohQP0y11+1HfDTeClJmdhui/uhqFJW6zQv5+qCdx/s1
KRXR2uxdmpFex7u6EfaDUmKy01Pzg7a81808fTaBX+LL8N2LpNrpeo08feH6nnKE
vvU14wH1fabHsqUcOr+WADC1Uxsi54HmUszrdK95byESEjaVLJwL8LXj2APu7cx6
tZ/8qsDqz5x3CgsCTS1QXv74GwvnJdzs/07vE0mG7c1v7ukn9qxd99wPg9vHwkEf
+d/45beotS4F5kbnxL+wXm1PBj3+k1BgnFYuYodvXaDMUNZDnpPPQuKoC6RRVqYR
pja0pmi9tuIjURYQMuSuiBUt280fzhBK+kte8rZIZ+ZwykY/BIVEWbob0ZMXEzyG
+3kPPrPxcV5omNiPdE7qjo0Skj8QPAEx4IcT1KBIS9vL60XgH1tDbz5IYrX5eF3A
jFE38yKxMAJ4Z4NRFzHddZmqiPBWSPcR6+aYSGjiw4T4yWP1ZwKaPtB/2AXDz88b
lViai4VNsa1feH2UIMKY3BPpWRf6ADfWI1n+jIBYAc0UkNynB/gL/U0fUOCLaRm0
QUchsCq06vou+/Yil/czE9VxrW/ARBTw+mm0h7Hn+7aW3jsPxZLdTMaia9exM2VF
rBcyA/1iv+7zEPHlWJv6rVQHR6/goDQsaVfuyeuMZrouazmKXpwVRu5i0pV8Ie/n
QQ2UXU7JytaLkeSqqsnLXo2K+NdIp0MX0BCu1TiZ7f0Zs/iUZphAxxZ+9qZCzHR+
j1X74Pu2lZGDWi9ElFIH5xrb0H9jYnqYWwM20d5nLg9KB2oGluR8pgVSZ/c6FWaf
7o+2X0QpBdX53Ggpp4LqE/Mi6HbePQyt3c2ldkp0y/IFlg0WvyTWH/G3CBYPLldb
iPv//0yVozh8Z0KRpbNLUAjguDd6+m7cSNl0IECRjeZ9VwDU6YFnRwraFD0eTbkZ
/5jjwrKVj+bCX+h6puLsBh+KZDFnw/T5J1t5Z4CbMv5sPdwMBLjB9AmMcMEHwLvr
E+pWoT71Tl6kfQbd3Kyb8e5WeqqtvOQbYaVuxArxEFsKfzg6T+iN7F3jElfcBG3v
XRIgBKA7MhyMs4ymwjSH3GMKCE72nQ5w//F5L/Pv9kpMzB/t6SJ08TfnYvzqWbp8
HuSnYYytoys6+DdmW1PNWESYX4sGYkov2vHbnRoj04qGSqfsf7hmZ41WKKcbyRp
NcZX8s76oWYpBfGdFRQS0Mx0wnuh6B3TL6dD1Xy+HPhNePF+yp6eIDIo/pfji8pz
F0WZMKN+DGqNgF/EZw2m2hZGY2EyWxuDVSR6C7d7jbbBLE2ydfxCpWjNWwQ61D/
SKqCgpiyLmLG36M17MIDy7xpfra9pqadnoAMzfkzMnjky9pS+Torv+Yn4pP5H3m1
7dE0M43sLRx1ypkBSjd5S7sHYv1mqf1aWYQ5KveElT1Um1UtPz9j3qFyeJMYhBd0
/yBU7AZEHzam0/Bwjz1fZQTW+5IdfM3CNPhxNC60+zEgFwXDK1FBGQ8Ys1ygryH6
vXU2Vkg6Int5TWUJw2JPvBznkqv4eQxK8WoGCEIHCaFryS49nTpa2YL+BA0C3Ct
Du7wF+FEEGr17xsJq6ok4IzqoA5LtTa21lde5PssaeEeJT6kqXyw8XjZ6a0Pn76v
0P60mu2Bbp3xC/yU/SbVrAvkekX7Ah9ZTeGLLEG7ZxW+oZg/wnOc7eMkdz8xj+0X
X3an+SsHkf8xuIs/ryPyR1UU877yD9J/eV+1xgP3x7xwnWURgigan/qK/TGe2WM3
FdzaF1oPaq+jAjzItN259+RY0BCGiGMzUu7XDN0t15yXL3CeAP42YIi2exVQdj/u
jC27PzoF6+diNsenHt95jedzYB9FjY53++B7jzhqPTmv0QL+pt4045Rbqtk+whgd
MuSFTsFXvL9L5BkBFm3fg2yYwJTAmyra8516c8TQj9PNtua0weCTf9WYfcmH+j6u

```

W2Dfhc6Zuu+0cXFXWhew50PqlfdeYJvxGG0qLP8hSBMN5zhyj8Q5z4Mxiy0a0QVH
+4N+pAqiKw9rbrg5J0fMZjI9FgmcVJAbxZpxXk1oDpCgYMp1RcgkMJhaZ011x959
bpfcbg6L6HqyP1T8iQxDJt3wpRAinPvccScBE0JcJcaPXk1pVRfGTfwUtH+PI546h
uKdJF63tGZPIExodinaerZBiqbP4jxPB4rGbrSJB1928QX5InN+pz3MQ8uJmyND
uGus9+FNgJ7a4j6mvd0z8lfcRn+U3YE1jLIEE0R/VtIg6jgezyt7/Z4J7rbf1pJC
ZHJQ6x6UR1VA53pQKofVF9bsP13ZvsvHWT8yblfKL3U3EJm0Y1+GHbVqaZ2R2XF8a
knL2/j4tpd/73j0v1b7eAR+eFgjH0HQdR/aEQ46eF0gYZTPDoXHB+91xjtika06L
HgAQ6y10nxuQWRaburXeyXYEoPVLURyfdueBBRn81TZY4esZNCAaCeqsICN2eKE1
wbF0oNH9Hn7vuIkdPCbSLMQxs9JBe1Ijgv1X/V0VVG8xiA3F18Jwf6XZ17AwpWBA
MBD7iBxovI0XAClxcWrB6Z1RYxwMujdIw2Dm98kaAeGpr9vXvkjxPLdcsSZF25cg
iSBoXR8KAbAv08X0Eci0/0r1qptyUgu6tUL+jFox7pC9Byaa4BW9/Dr4biwe1UFD
IT3M70hrYJDEwoF6UIjlcMpymnJYmqGasG59Ah4uaEieQxYk01RRFiytF+N6oc2U
39qNFtxzMs14dQr/+zuLdbugVge7v6DgC65iQ19ontT/lH/EX3hChmY6daUmz4kS
2Vmwd0Ehu06H7yeoIhBTZ2v4+vkGihgQTo8xm+6rw/t55+nQfgQYTC/ZZ+9MuAN3
uKsVsTsrorp1I6kK5zI8s6r0Y+YaqS10ckNrYXmyq9TSIwyBzk/btb/mDvZMF/TpK
QIaHsSVlkIdmfq5YmTr+inlwK1fc0ZjseesYAhehpPJUzuP4KdGWr8Jc/pC0QNYd
iGL23ieFbTHKgPyGCMrdYgEMqpe/THE65H7pGuINigDEgkG4m0Eq7xDVbvvy1SVJC
jc7o/08cONG3kbHyYbGUlaIKBBap285GWNSotQSchkaDo3hT6S6cjPVsrPoqMN8j
PQNPARqKYRriyI3ej8msK311VRTjAGKWwEVgxn4nF02bvg9HBqv/TiFrTrFLSsd8
6g4HpglcnwmxWVjAeCsruK3Ijv79JWRNPxOX9+tnd3k28E1QqwuEA02uNuHZLbB
TvlHswfi9xmPwZG1bytwrSB+kv/oE0cVLI9fPCKpe3I9N+oL8xLr1qG7vNqwaZAK
MTd1VoPxWmlvj/z2NahU05eC12yx29sJN90qz4DB2juUaLFA45+rJMqc9Vj8fFr
/Qrq91UVuXQJIXXCWfC598YJ/p4VwL/g1K4ofs9ss15MZbj3IesHFEwN5BQm2BjB
kh0/s2kG3dJ5jSHSfCB/EDexFZtdLCyEwjIMNQni0UwQjaZCKf4U3QYV2vxTL9r
jA7KfB0gAdwgXX+tKRwv0VgIOz6gITE21u9envfZ1eq0fex1fGT1xv/E+iGauIST
qgVKh0ciZMPqhRgaBHtrjtTyifweXbSKo4AFVNNH3K+swDmXW/XHQ6Y7UAjseZS
ZFtjurmHB+uYz+04kxAct4fJW7d2e5iU6tEGKseCnBZ//PGgzKlbwigdNhopou/Z
s53h4I2Z0rxJFz33NHwTx2wquT7MLwCZwD/Thttujx6uI2JXMa0zudluK7S+lj2y
d3DBHNGszistpi7cUo0gYVMvFwuTSPgvLfyb3CiyUH1K3TIEqox2BJun3tXL2P9s
7tFBjgqVRqm8AYDRzSpkw5jKL2xWBCI0j9hd2PD0Qbhw/EgLNqlHmLK7Yqy5TK/v
CMk2aLkVAORtQlryJ2M8W10bq3RPjwfc/zB9NWKTPX/EuY03nYXQLG9510ajvodu
sNZB4JyeNkbIn9LPNZ+8mfaxHE8Zmqd3A8XSN/KfSG0j5k1wkh2qrWW1hbZQGBnU
ocpweDkQvxKxun/nGsfrMdvMzSMqRfXYxATneXH5IhmCLsBx3qeGLiYoRkLd0434
3Z4937SMWwtg+oZYcd+ndW10nEVyGqTmWB2UKhJhfIhL1YzpkS6444tdlIV2LKeK
GwhG/6RzVZ+qnNzeEF1JjwUsMTd+4Xa3k2bkMBJQZgg0tFxCeIANKVsBzrT6DTLa
L9xJqDPD7SR0KHubosXhFwx/cDcFveWL+mbkfQc9/edeHffeCvdgX01CixPmxXHY
y5vETDTiJqDd6+wjQHRrjoTv17Zz2Zb1hhvdxLnoE9IMABvmd8H6fF3L4jIn2k3K
Kc0CAy20FA9K2eMgCOW1+JeYcgA1Sh5Y8x1Fg6Ah0FFH62SMn33B9rMYOB++Sjg0
vh/1cfHXaZPwpMb1gNU9hipbThL+2MH0irtzQ7sn7X9FQqvKqWA570aXXpUID2Nu
U0rjXrw8AXmaUtFpN43rCk9t58eP+vوسفCsG/ua80ptkEqb0Gz3FM9B6Be4crw20
30ivl7+0dpJ/rAD1LG3Vq6VAvpAQNT0g0/TmrHJ2rnHx5UuXZB7YYPF/eufDDtLF+
BZXMT9+snguEJHRifIxfXISe/MFti9ROSsbT90u4k9WxY0PI5hp95dkvX/PfU0
lNsNQvN/OjVFx860ZCY2UR+18VhYwUKTL6qlBAeVca2QvdZ8BIhr/GNHfXyge0yo
cIbqf3WQnU/05jV6v1Y0q2TJZa8tLaf+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"

MII0VgYJKoZIhvcNAQcCoIIORzCCDkMCAQExDTALBg1ghkgBZQMEAgEwggR/Bgkq
hkiG9w0BBwGgggRwBIIIEbE1JTUUtVmVyc2l1b2JogMS4wDQpDb250ZW50LVRYYW5z

```

ZmVyLUvUy29kaW5n0iA3Yml0DQpTdWJqZWN00iBzbWltZS1zaWduZWQtZW5jLWwh
LXNoeS1yZXBseQ0KTWVzc2FnZS1JRDogPHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5
LXJlcGx5QGv4YW1wbGU+DQpGcm9t0iBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBs
ZT4NC1Rv0iBCb2IgpGJvYkZzbWltZS5leGFtcGx1Pg0KRGF0ZTogU2F0LCAyMCMCG
ZWIgMjAyMSAxMDoxODowMiAtMDUwMA0KvXNlci1BZ2VudDogU2FtcGx1IE1VQSBW
ZXJzaW9uIDEuMA0KSW4tUmVwbHktVG86IDxzbWltZS1zaWduZWQtZW5jLWwhLXNo
eUBleGFtcGx1Pg0KUmVmZXJlbmNlczogPHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5
QGv4YW1wbGU+DQpIUC1PdXRlcjogU3ViamVjdDogWy4uLl0NCkhQU91dGVyOiBN
ZXNzYWdlLlU1E0iA8c21pbWUtc2lnbmVklWVuYy1ocC1zaHktcmVwbHlAZXhhbXBs
ZT4NCkhQU91dGVyOiBGcm9t0iBhbGljZUBzbWltZS5leGFtcGx1DQpIUC1PdXRl
cjogVG86IGJvYkZzbWltZS5leGFtcGx1DQpIUC1PdXRlcjogRGF0ZTogU2F0LCAy
MCMCGZWIgMjAyMSAxNT0xODowMiArMDAwMA0KSFAAtT3V0ZXI6IFVzZXItQWdlbnQ6
IFNhbXBsZSBNUeEgVmVyc2lvbiAxLjANCkhQU91dGVyOiBjbi1SZXBseS1Ubzog
PHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5QGv4YW1wbGU+DQpIUC1PdXRlcjogUmVm
ZXJlbmNlczogPHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5QGv4YW1wbGU+DQpDb250
ZW50LVR5cGU6IHRleHQvcGxhaW47IGN0YXJzZXQ9InV0Zi04IjsGaHA9ImNpcGhl
ciINCg0KVGHpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5LXJlcGx5
DQptZXNzYWdlLlg0KDQpUaG1zIGlzIGEgc2lnbmVklWFuZC1lbmNyeXB0ZWQgUy9N
SU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQplbnZlbG9wZWREYXRhIGFyb3VuZCBz
aWduZWREYXRhLiAgVGhlIHBeWxvYWQgaXMGYSB0ZXh0L3BsYWluDQptZXNzYWdl
LiBJdCB1c2VzIHRoZSBIZWFkZXIgdG91dGVyOjE1bWUuZnJvbSBzSBRkMg
OTc0OCB3aXR0DQp0aGUGYghjcf9zaHlgIEhlyWRlciBDb25maWRlbnRpbWxpdkHkg
UG9saWN5Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGx1DQpGcm9t
MIIDzzCCAREgAwIBAgITDy0lvRE5l0r0QlShoe49NAaKtDANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLZwMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGx1IEExBTBTIFJTSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAwFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOZENMA8GA1UEChMESUVURjERMA8G
A1UECxMITEFNUFmGv0cxFzAVBgNVBAMTDKFsawNlIEExvdmVsYWNlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmPUp+ovBouOP6AFQJ+RwpODxxzY60n1
lJ53pTeNSiJlWkwT/cxQq0t4uD2vWYB8g0UH/Cvt2Zp1c+auzPKJ2Zu5mY6kHm+
hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV
8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41
/0HJvmswqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWf
NEbkN6hQury/zxnlsukgn+fHbqvWdhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4Gv
MIGSMAwGA1UdEwEB/wQCAAwFwYDVR0gBBawDjAMBgpghkgBZQMCATABMB4GA1Ud
EQQXMBWBE2FsaWNlQHNTaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQw
DgYDVR0PAAQH/BAQDAgUGMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASpW546vzfN3DzAf
BgNVHSMEGDAWGBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOC
AQEAgU14oJyxMpwWpAy10vK6NEbM1lgD5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LD
sfx7fSiUs8gWVY3WqMeu0A7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzT
jqB8+dz2AwYeMx0DWq9opwtA/1T0kRg8uuiVzfg/m5fFo/QshlHNaaTDVEXsU4Ps
98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJY0nUmGpFb8PPwDR6chMZeegSQA
W++OIKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTS07K459CyqbqG+sN0o2kc1
nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJc0vT4
as6aqdcwDQYJKoZIhvcNAQENBQAwVENMA8GA1UEChMESUVURjERMA8GA1UECxMI
TEFNUFmGv0cxMTAvBgNVBAMTKFNhbXBsZSBMBQU1QUyBSU0EgQ2Vydg1maWNhdGlv
biBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WWhgPMjA1MjA5MjcWnJyU0MThaMDsx
DTALBgNVBAOTBE1FEYyXETAPBgNVBAStCEExBTBTIFdHMRcwFQYDVR0DEw5BbGlj
ZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0iehY
0BY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LC0wI2juwdRrjFBSXk7pWpj
XwsA3A5G0tz0FpfgyC70xsVcF7q4WHWZwleYXFKlQHJD73nQwXP968+A/3rBX7Ph
00DBbZnfit0LPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZ063dKvIKp4cQVtkWQ
Hi6syTjGsgkLcLNaU5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKR
u0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGJWlQVCCpDt
c0NT6vdJ45bCSzsCAwEAAa0BrzCBrdAMBGNVHRMBAf8EAJAAMBcGA1UdIAQMA4w
DAYKIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGx1MBMG
A1UdJQQMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDADBGNVHQ4EFgQUu/bM
si0dBhIc164papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTCOfAcXDKfxCSHlNhnHGH2

```

9FkwDQYJKoZIhvcNAQENBQADggEBAH0JojanzqmgasN3/gqSQ4cbbmdj/R40BEP
+gXT+xiidfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1iffRFT/KtmVEDMR/sYeqAH83
KM5p3e12lVh40HhyI0qNuz5oShNaACSioQ23WxHGvy9vsdVfnbhsplrWg9NQ2Wbp
CmK+2oMh2oYl0Z/wvXmt9cG6jbMvcdH4z0IOvg6mrYkKTM/RCGnumghxwYToj10y
D5Gs4D2IJCw+fX50Dxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDd6hnoQ9
rNeozIcBVyybQYjfrgg4DRvw9Ksk220H4ConlB8f7R7s1LM2cSYxggIAMIIB/AIB
ATBsMFUxDtALBgNVBAoTBELFVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQD
EyhTYW1wbGUgTEFNUFMgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhM3QQV5
7XV/QqmiXDr0+Gr0mqnXMAsgCWCsAF1AwQCAaBpMBgGCSqGSIb3DQEJAzELBgkq
hkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDITxMDIyMDE1MTgwMlowLwYJKoZIhvcN
AQkEMSIEIAsnTrJmG9vhEDGPGAIiq3jNFKAZg/b5qnb8K8AAVkcFMA0GCSqGSIb3
DQEBQUABIIIAH/7j5oqF/rfVNLmPNfU3UFn3oHiaWt3+y8+fLX1e4uMgF0she5Y
Iz5rkMeHmP0HHtnqfbPjyktjTR/wlmHazGcasD5/KT2/1/HXOJJdaM/YQ4g5RiBi
h7TDwAFdsNMMeEfYII+gDXrVeTc0BvtrWetxrGYhbMUNLtM5tskMhuUMVYrQBcUh
vkYBamQMvmiZMB0FHhA9hEay6QFIAC1v3WtJvyiJCSHld1Qetd+NudbaCr6vZt
+C8LsBh8hQ0+TIT8AnV8yBhQnqFGj61JQjwGBRRwQHbvAEG4uxaWr20wCa0VW0h5
237SEh0m/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/TCGPGKCAQAxggMQMIIBhAIBADBbMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBVTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIElnRnRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBQUABIIBAAs1ng0ySnXdmv6DCfeI7GaiqqHxw0Gv1EI
l0jgi8u7Y72KiMZWvjFeRLtLpbe3/D5s/MEJ8AJ9LN63jhEUv+AyF7L29pqX7h1R
SQVY2I51zrm5ilPMkB+v1Dng6GguD8XDqmsxgi1oloDgExg4dsqPbGvYcXqQ0Uli
B4XdqnREveBuiXp5KetN7RR0t3KfD7o3Flakl90pyUIh1gpArSbndjbnjinlwbby
fChri1V9NT99P6BVcdt0oduxEFIUxW8Rb1mmj1bpZQHUN9sxFftA2+qZE4YPG0nn
j5GyLFamVbJSOXYeWN2S0TMrFl+RF0H5HVfoTq0MtEaKbro+CgYwggGEAgEAMGww
VTENMA8GA1UEChMESUVURjERMA8GA1UECzMITEFNUFNgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQUU1QUYBSU0EGQ2VydG1maWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEATEB5GYpWDLjGLqDyORR4LW+h
3+Sz2jt7VF8p4jo9c2WubRx1jmmzULRw+Nc12RKtprjftmWXCzEwiqMy6KKijCI
e9Rd5812SDL6iNp1WUXYbqp1x969IQNvBTfNGutgQogB21jNm/qbaL6fAjwIZXxW
1LvTBi5LDe+K6/dw1RjPJLZ/BBhyj2miqz/x+rYsSaG3REExLSN/uIv3f5DGrqg2
2kHrHjXjIQE8/qYPa0t2fKXFJsmH/4FUT/384aepm8oiN5y8xSxlgeQoW1drFvGC
sqFVHomUGvReor5zM6Q1bwrj2FAKQS+Qd1r5Z8bWatQmMfWGu5Ix8m1/kocX9DCC
Fd4GCSqGSIb3DQEHATAcBgglghkgBZQMEAAIEEPuytcsL/JFRST8refH5jrqaGhWw
myavNN8eGoalhPR5erxp3r1BVoRpk1biqcaFsojj2XyGUSqKM3bcnoVAW70KVLCK
HhxzxEFYVeK1BGHW/W9d9JSiwn00017Z0KX0Zf87C9xgnigppjB8c7/Nm/7bmD7R
Xp4stpyVCjn15E0Yz2R5wLMvh23b70d/c7UxS4yivIxM8eW6zDsHUVmb8/TT+0tG
kVXIc2I81l4WQfVYy2KsQi7Jn8nYt5W063CVin+FH0SRSDx8hChedXptVj6YXekp
24Ugp6cc1AEHgcjo0NHNZC6wn0QjEhsra0VyUt2e8FFWAVE58M1HpFNRIgSXNFdY
eq105nBt5g2XnYgiJM+AuEuXD/QpZwpdJrQif4UwLW4nJCUCnyTxquT2wE+CuU/
```

8JWm/8xeVmG1XfSHRU9ElHdBTF30iIAZBfu+9S7LHnnB2TZraKBqKQuk+K/DQMj
CZMzXLt7HMVvS10lw8erpkPTz87ugBzXvLq9iCVZ8CirmQouXXTWXyoEf7uht0BF
t+Y3aNHnmjoqs7S/Tw2HCyvk6azw9hFibYm7TCqviLhwpEk640l5g30PhpKGZdw
sYY0eTndS/j1uBNT0uUCluwj7Nh60xCmRtzpuFZXG+HN5iTR0wgGpxJH0Mj9QdTV
uctaEakmHfeJZZzo9N7DfqrQV6Cs5MKnWQ9YZQX/mloY2WDtQ62umI+T6avdkfsY
AJPUMnxBZgvS6TYWwpW7xwxWms+skLRydzjFBds3A+08A0k9E1pQ0Cr5VPV9pYNs
n/tZyY+LMgF3VV6+eN+menuNet9BDEqntk2R+waAlLDZ3mQXrsNTgJ8U8MKXEu3E
NdcRRl6ek0mbEW1X0Wn9N+oVndbZbIiERHHLRhmz07nNSniBKn/0AHNGBM425kT
HfUYPVsm8038NAQ0lNsjfa35Q039UucojLLazsEQnPr0T1gSy+CMhz+K/HYF20HY
S+mV+1NuXrvfZ7sUUDsSKWoqbxwVvrohhXSUrmmwZrd6DVE2Gu0jog0Ahp4xA1p3
6/NN2/3szADTOXD078jmchqY9Beg09K75VByVFzpc+1A9ZCJv6qS29GilWoaPbz
RIR8lxox9Vtj4JD1toPL2Nm5LHdL1napAMNuo1ktDL2lKuMVCyGTwaMM/T9DSDf
shr+FTB7rD6YKd/GcBCCJehy0cRd3Y/hLFI+vJBaVetpCSeH+FuYU17ap9+EPGmj
kJwkVqPyBXW1TYr3fthwtWsrwE650RH78vBbkoE8zny6RRtdV0ENPZEsKgCp7wpt
1/JrGN2M5S9P6A0ZTsAkBvkPMD52m6dYJsopIDyaDvtP/QMlIPuS5o7npfvDCsr9
qpE3D0bT5L3dRKbDdnW365+13oaZ6Jnx0FqL/XZp9h1n6vxAxx7MGm0lrd3s1/nL
QI8w22c+jeJbfiNsIzkbGfasPxdYgGcU5xGCR00TlAqn8cU1W1NRKYGsXTZSp6l
vNGc5MN9ShtJdlc0xoG8nW/GMhx0MGNh13htAfcQB6d61v1tFAT3sJFruaUF1pF3
0DGQtY1Lh8UQRqAYkfVfSeW5oTd52hBZZfeHMDHEwX0HJLjKR4pLTqPskMFSpla3
5F1uw5abtKgDpqT5ilf4919FBPKT/Ev1BREnt2nlq4jSDjSkTm+ZyZtRdWkoUMM6
LDRnA6T1GXv/+WNDS3KcGSSKZvMwQHbOdgs3lBEzvcNka2jGiNiwsWpj/6axZiJl
AyH2ySc1zR47bfb/Gks3NVZiyAmedt4WU8Ph04uZuoSYuV40V8c6ntk5P9g4y+rG
RdXpmUHKM5cTTezrs3EH+p80/cD0Af5odbWQE0EZtam6Vdn13afFeJoKdn1BET3K
Q0kTL8aFxErAbpF0TbCgNqzcP6iozqlxz20mBGdNBhDLwLWDzQBj0001aeXe9rs
3Nv03t7oZ+ZToy5swk8JdLakS9JOWAc5ofZwfhWZDlnPldkwticucEjyn8SoqeLA
tFAG67GGFStNrpPXtIbdndhS1NLP45UxCeZU8e03fcs8doRjsaTTbpA1MmQMh3+8
pCJci6DlKlvwtb0DwwQ+LWSW9bEHwKGFxHo0y2hiwhUCnTw/DvQRoLa7feb6cSFW
o1wW08F0kzyD7I4Qc6gTdhnsSepJdlG0Fia9R7HnmWhpJL8QY+Okp6WFxF9M1Bu
TJkzhwK4XwdNPoX7eKPK+0Mhft4MFedAbPNTgHyJ02JGtUik/h8dduxrhDtgXVw/
jBUg1m0BBs1rhuXk77HedXoj2ws690Fb7UdwyVA12+8GzGri19z0jYMHpE/V70q
u70zUByDhQEQHCEomGS27jv6mBrL8jKqnB+EP7p7prxSwrGsXIIfIzg2+cKp53SRy
4eOR2gNzdHFfMH5rRNM0ad8aCBtL6/My/7zTE0uh7Btm1C8XDtkksQuJaTz7BrR5
SyBUrf8g7S5gk3oezrC+U3GQ+B8v0AlQ1yVJbIYPHNuHy4VbiiYC56zDUc5r3680
R0oF3tcbQn39X+sTQbtjJk7dftxgCTwr4irxxCxxAEA0wcgK0XBhI1MIL3Vo/Fsf
wFxjai0LgkNTwY9EwgYNDgArLZzyuSo0ZBhQZ6oxf5jXEBh05tYTIunCFIwffLqh
o8sg3ZoaUS9NHaGESruz+sBG8zsbwSgGjzPayJyw95CN3gM6HI/Uaoi9x5Dx/IR8
883bTyK7wcjy4l7P7XZF+Puw9fGoG0ADVpJux9brsBluoYQ/Pm3F9RvC0Ji/89LT
oMznU4lZEKfNG0SnTuGr1lBKSdSe9DTt2J2oQwJFnskVYPhGrLIa2UetQBs80qve
iMKrNP6CRhKwLbjgwe1fc7WTiYgrhrLUUsjYxlqRsaPlKeefXZzFBWH10o01lkU6
vkr5R19xtv0zJVPGD0jbWVMY9QLWu8Mne8evi20LSJhyiNcVv4my9Taf1fHCSS7
3xK6rdJPWy27eCNvOQwE6USLwsSyb05hsZCbECWXYM+mvD7EudFSPPRSJzHyB1RP
8h0OwZVM/V0S1G9HTBFJHx05iCxsqszlePsKmZPzGQFc15xIxQdt3xtlI0Qy2FQVq
Mfz2Eecw+mgr0Yf5q38i/IxvcJRN9x5u9efAuQNuf5mW2CJTml12JEtNuYQ3r9W5
QNmSvQZn0+whGIGyfbhvBLhDQJYGN0TXmImoJ93qceLyWoy0TLrTRrM1y6h1sfyp
HrTnW80Mcaeqwx7/K9oDkU5yG3i5L0uy4I80kM1HMuY8zUcuf0tWbqwqb9kJn4ow
/FWhpJWmaUVoHy/Z8J0ca9bVUNEzgs1DV4TJSzYyAJiS8vfCuhpFiwZn9IdEN2B8
xQzKj1gHH8BKzViYnsFyjxPERPlwe3HYH3mYSzketCyMAWqGCLjnx0A7h73FGAe4
q0qkI9Ea1204BH7+zzUuaX3l62SXwwXXNIWPGZquXrvwD1IT7y1JA9quKM3GShUX
ADv4J0tR4GB4VzVijEBJ09Z7Yo47PQwLYU/DpbimfSgKOSKhUyHF0McHzyrLV5Mv
PwB4qCvvvTH1xL6vCKzQBssZPIFFPFSu7G/xUTiSytioTeTn0ecnyVX0GrBuUaQF
IXe1Tn/M3rz9DYBoutCvE8iW3nTPF3v50P0LfYn0sooxy0mi/5e0fjtoesz7L5sm
nLVwWPjEg7PAHQs5jHSDhRW2x4kd+Rx7DCEsIJXEqrc8ge6CQTWe5IoA8IwqN40e
+MwXmCSdSe40HTqbx7+0tN/HxqbzGWCjITTVeh9QKnCjhjNlLB05KTV4nF1K2YS
eomLT7FdE0LxsNbZIBTZMAxfSGJUCaEylikNHeseRc4AbKML4YdtL/5Mtg/y0zMB
qwIldlXDjjwh87iYDwJoxBGL4GewGbcYICMzu76qnnfZd0j6R6jDg3rna6v9cXr
8RAI15+3t/bnmGjWV4E/18/9CE/N+8Lk1+LknVbehykbnM9vBb3smEJgESqmn1sT
4quIsc3z1Pjv3q47iR+1RWG9F5icqRSu7ZgmCXnWqw6iuep3mSea/HyX23x0U6oQ
dvLI19vT4ji8wG4F+WXlFVe5ac109Um/30cG3pJTjKcogmBvlyJPJt+1HESmJT9U

```

rGfrA9k/94+e2Ye9ksf9irp4rPmBVYTAwnwzr2hLAqlaas8yxGMy15fOuPQ20IWX
sFP/eRuAeVfbYDGGsqmYhSKXbvd5AJtupiM9SBKqBHCjQYT9G1Q3hUE2qspHrweE
hvhdCcK/T0sfVuZrcykUtBo5G8wTtdxSLMUU9prqtYR/brtQGBveM9BchW0iPgTS
/jY1R8V+j37GQG5oWV5EGXS8IObsMYzRM2SugwsE1zb74LJrsM209+n4Z+CQT0I1
e8z0EKbikQMtx6Im2SCYyYXRi3e1IhFo1CsZCQel0bsr8neZ0jVS9aQkH60Ed14C
4JVit2D41Vu7nq2CvWqsjgwz71vD2nVEEBVqPnk3SC6dXXUP47GAiyu0XoL+zFdL
kzQoFuiBSmWav053kU0LhSWdt/hkIqzRT7uyd3APBIHSG8ZvTqEEYX18c4dZr8Bz
W6Q6o2DNnI82Ht1I7g/ioXI/U/gmc6sWdYh+W+1VxIntu7sjTZz9i+PRQPEvjWdM
bG3hqkOaPj62+2Mp58FHC8CzILViy4uND4AsFrzBY0sybRi48SR8LA0a2QuUPzHa
2/ofW8pehUmhYtqP6kFqtibHdEGBmxz0ntkYzp3bZAPrlyLFSF+aWS8rKVbrgxjv
wGHUxaRvLUKaQJmQ+h50HzglaUPPdElq2cshqYVjyIKqrESk4m3si/CKS6GqWW5v
3oaxs+WIn4cil+PUgIKhRtJEwpZnJzX0teK9gyKabPjvNsJWmkkI80dXafDVdJ7F
iJ3PQGZmrturTlGRavwk+EW6cn9jG7KTrQ1jBgYpA3r31l7EKe4f2YlScmZLswX0
GeV6FIcdU3xC2a2N0HSSCleglNffJiYJPTcWkiQK2bY07pgL4jXzsa3Yqnjo0J32
pDC5DMaTQPLjNW6hCC7JxVDiDhxCj67b074YDyhWjQMnIDXLVFanRsZVG0Rj5+Yl
QPk27a8EUF65vGFAUAvX0IXNPDK/JwvT8BylHX5HjASqK62i9fuHqOrg/OBsDTKI
XKJnS1T802HuQze1ZZEDs1lDays6Bi4JdIVZZKXt+RqevZ6YoZ20/1Jj+t4P3cb8
e7GK6vLEel0g3F7N42P0F4N16NiyCftuF3c1RNvGbPw46HAZvUkU+Bdd+ZFy90yF
CCaVsHo6/9YgK1oSASdr8wY9yMBZSQFJ5zdA5yt0USWARmu7YwkGN0vRpUYh0oAN
0WGS+1VSmfak2QplyGHJzkkUVTlGcaBCbd05RPyLRe/brwvGQo39tTCHlgsspNLO
RyDWZ64ZqFVSBCjch9ys4BCSxdFzS56fAFQwX/Yq2bIXmbf0RIjDgMju7e5hqXvU
r0Q4uesP3V7P1t0uYz8pJV8L4hBiJHoPb0vgx45wzYrp7n6d4aqBm6h644Q1/0hS
Irf6cCU+ue41dyC0w2pPjNxAaFHPwBRg3J6ogg74LwUWZUQEKycQ1KjI8AHY2jLq
9F9nVb560KPNob7G4BHS+5T1mKZmi6qx8o7VTWLF1gYudHKldF9eNY0dvp9/9kKX
829kbKQqX0xPi0kdZy0q5037zcGTRuv6EIfqJTERYkIxHCfsPFHXUloyhgzu3X9
ffJU0/ue/P4ZXT8K2EbeG/9Eegzytw1LDkFn1KjG/G4AVx1+Hd3/UY7ia7ZPMCAR
Sw/19ZyElbzoE/x1/7elPv3r4rjkJeUh6oRBknd/nENW6gakpFxYvHDnru3AEoxK
kNZCTqyH7iL1Xs8RN1QUHILLXNG9wc+bIgrEpwmqqEAbxVHcmZgX/07bxGmYTHGX
tNht3QcKaA7EuVTF2Fx5kKXgdeM6P1NaKgn0IARXHdfD40rLDPa9Sh5TF0APOW6Z
vRvuG1qv9biI7+FMJBuQ2TSPCVX6i4VM1i+Tckx18VoBK3fQdOmnc+BaLks4FQNA
ayKrnZBFRvr0n+aUPfb4pfBWn/1YFcJDKXN4Isqp+BD0rqJqXUi0zEAHsJdjiZP
dXzpKSygdjR8w+d26KKlky6HS5dBuoUA1cKo4kyMTBU7SRv5kHm8WWKg02YMM0K
/Gj1ApNrNib5wCoBC1LRGS1IpeHNjCI15/mQGJPk4wF67GT/37JkDQH+hiWh0vdN
EvCEGqc5YkTFh80TwDD+5uSLmNvSWdf9BFaQVR2RwbMSVAaUc6dggZe5qlmBqN4R
T3xrKPUADPxyZiP11jUJCFis6wsLP4b0Epvg0KZ/9r4+27UvUbmZk596ptB4I5LE
Ck7Dwf+Hiui/RL2RHfjPFfRNJX80OdMHjRz4meAWvS/0HlyENc2ruc7lt9dVECW
K11KiuFec8zbEZGDBJcv4V3Svkplf8H7zZSTER7oB0Nvi8uNsIaU3l6JdpusAfiV
UHCYJ8kTaVoT6b6h/9cJ2TufSfv14ktvdMiW0wJ1vKEyb3jE3fQgaHQXbihPAX+g
uIIgYYo0/myUIITzSKj0INU9/TPgrs5M6fYDHbrZVDA964EDYIToiGFQZTu5TbyD
ojrdR9FTiuYuoki8fkTPJc6HicaY/rDyKvNlpINpa2jA5qSv+MwtLDLX7c1RcBFF
/z9p0Ho7SeZiREWqDJZ6pN7bpAumE5XgLW1WGNuWBbtLATjqy0eAUrnRbyXv2RhFW
gHjwk6RDv0ScssPTcribodZWHpKo8jf1GzE/AxkjdXxH7ZkoXfuK2mTNRnynFhqp
328FwkRvik2udbFka0AXI/phsaVgffz335si9EYxEGa9VXR6K2ikZ1YpTNYkvN8N
inJk2YRXjVWp8z1sswNwmyEaRdsV6E5EYmpCT0xFD6YnHanV8t97X1EmWYV8Vg1v
9jaL+nhm8zrEK/R+sG6nM3Mvn+7/igG8Q0bvZfsmcRTKxjtpHX0aXgz/vuDACgR4
wVMY3xSogDsg+azivtAmhCpkfpbRkjr8PdySvoY/t9FymrZjBFFlHYLsIsr32KKC
y/cEwUm/a8yUcGWzDfDUWeTxpr9kVy6NpKhQopnVlVoYwruYEJFauHcXKI4htemb
VZuUNio46th+9sSzj8AMCpn0PDbVq4Q+XMnXK3seF2tvclwCei4r/pwudKum8ggx
x+Z0pRpLkCn5tYbjKedS3nDpTEHLOIRa2zACLvsqCbsNn05af11MT0VyRfUwKAI
FkEq7a3esIoeIkbhjv1P4ZVnmWwK0HlMvdI/PxH39qJDI170y90iXQG90GA4NRwL
HI+BvWMJ234mBSUFIZ3N/nfmH16/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"
```

```
MIIPYgYJKoZIhvcNAQcCoIIPUzCCD08CAQExDTALBg1ghkgBZQMEAgEwggWLBgkq
hkiG9w0BBwGgggV8BIIIEFe1JTUUtVmVyc2lrbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOIA3Ym10DQpTdWJqZWN0OIBzbWltZS1zaWduZWQtZW5jLW
hwhLXNoeS1sZWdhY3ktcmVwbHkNCK1lc3NhZ2UzSUQ6IDxzbWltZS1zaWduZWQt
ZW5jLWWhwLXNoeS1sZWdhY3ktcmVwbHlAZXhhbXBsZT4NCKZyb206IEFsaWN1
IDxhbG1jZUBzbWltZS5leGFtcGx1Pg0KVG86IEJvYiA8Ym9iQHNtaW1lLmV4
YW1wbGU+DQpEYXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEwOjE5OjAyIC0wNTAw
DQpVc2VyLUFnZW50OIBTYW1wbGUgTVVBIFZlcnNpb24gMS4wDQpJbi1SZXBse
S1UbzogPHNtaW1lLXNpZ25lZC1lbmMtaHAte2h5LWxlZ2FjeUBleGFtcGx1Pg0K
UmVmZXJlbmNlczogPHNtaW1lLXNpZ25lZC1lbmMtaHAte2h5LWxlZ2FjeUBle
GFtcGx1Pg0KSFAte3V0ZXI6IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcjoNCiB
NZXNzYWdlLW1LE0iA8c21pbWUte2lbnmVklWVuYy1ocC1zaHktbGVnYWN5LXJl
cGx5QGV4YW1wbGU+DQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhb
XBsZQ0KSFAte3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDlwMjEgMTU6MTk6MDI
gKzAwMDANCKhQLU91dGVyOiBvc2VyLUFnZW50OIBTYW1wbGUgTVVBIFZlcnNpb
24gMS4wDQpIUC1PdXRlcjogSW4tUmVwbHktVG86IDxzbWltZS1zaWduZWQtZW
5jLWWhwLXNoeS1sZWdhY3ktcmVwbHlAZXhhbXBsZT4NCKhQLU91dGVyOiBSZ
WZlcmV4Y2VzOiA8c21pbWUte2lbnmVklWVuYy1ocC1zaHktbGVnYWN5LXJlcm
V4YW1wbGU+DQpDb250ZW50LVR5cGU6IHRleHQvcGxhaW47IGNvYXJzZXQ9InV0
Zi04IjsNCiBocC1sZWdhY3ktZGlzcGxheT0iMSI7IGhwPSJjaXB0ZXIiIDQo
NClN1YmplY3Q6IHNtaW1lLXNpZ25lZC1lbmMtaHAte2h5LWxlZ2FjeS1yZXB
seQ0KRnJvbTogQWxpY2UgPGFsZW50OIBTYW1wbGU+DQpUbzogQm9iIDxib2J
Ac21pbWUuZXhhbXBsZT4NCKRhdGU6IFNhdCwgMjAgRmViIDlwMjEgMTU6MTk6
MDIgLTA1MDANCKg0KVGHpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtaHA
te2h5LWxlZ2FjeS1yZXBseQ0KbWVzc2FnZS4NCg0KVGHpcyBpcyBhIHNpZ2
5lZC1hbmQtZW5jcnldGVkIFMvTU1NRSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw
0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lbnmVklRGF0YS4gIFR0ZSBwYXlsb2
FkIGlzlGEgdGV4dC9wbGFpbG0KbWVzc2FnZS4gSXQgdXNlcyB0aGUgSGVhZGVy
IFByb3RlY3Rpb24gc2NoZW1lIGZyb20gUkZDIDk3ODggd2l0aA0KdGhlIGBo
Y3Bfc2h5YCBIZWFkZXIgc29uZmlkZW50aWFsaXR5IFBvbG1jeSB3aXRoIGeg
IkxlZ2FjeQ0KRGlzcGxheSIgZWxlbWVudC4NCg0KLS0gDQpBbG1jZQ0KYWxp
Y2VAc21pbWUuZXhhbXBsZQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdK
zkzJUH6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMA8GA1UEChMESUVURjER
MA8GA1UECmMITEFNUFmGv0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0Eg
Q2Vydg1maWNhdG1vbiBBdXRob3JpdHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1
MjA5MjcWU0MThaMDsxDTALBgNVBAoTBELFVEYxETAPBgNVBAStCExBTVBTIFd
HMRcwFQYDVQQDEw5BbG1jZSBMb3Z1bGFjZTCCASIwDQYJKoZIhvcNAQEBBQ
ADggEPADCCAQoCggEBAlJqVKfLwLjJ+gBUCfkacKTg8cc20tJ9ZSed6U3jUoi
ZVpMLcP3MUKtLeLg9r1mAfID1B/wlbdmadXPMrszyidmbuZmOpB5voVQfiliY
Yy3i0x7Y0qzXr16udP07k0sV+UdSNRFXrfKeoQEFXg0aGdmnx40G/e3p1fIKM0
dPzZLo0AJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXC5XL7wWTLMLenF9
Byb5ksKqUuqEHAMd1nmoNMggjY9VfVfcrv9w43GG8FtpSX+TWzB2zNS20F+XIV
nzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAA
0BrzCBrdAMBGNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKIZIAWUDAgEwA
TAeBgNVHREEFzAVGRNhbG1jZUBzbWltZS5leGFtcGx1BMGA1UdJQMMMAoG
CCSGAQUFBwMEMA4GA1UdDwEB/wQEAWIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkV
fAEj80e0r83zdw8wHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSHlNhpNHGH29Fk
wDQYJKoZIhvcNAQENBQADggEBAIFJeKCsTKcFqQMPTryujRGzJdYA+R9eBA
UDLsatbtKt14FzkgrY0g31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5AQ/hg
xLvLir3hEUVZ23MRsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5
UzpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7F0D7PfB5v94M5274XYxW2W4u
KGd7QGnUZROsvSYkGiWdp1JhqXwfDz8A0enITGXnoEkAFvvjiCqh64P1hIe
Morj36pgL19oWZD6YrzSWHuZ1F00juyu0fQsqm6hvrDTqNpHNZ015fOURza
1SkCvi9GFmNUPoVgwgPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnX
MA0GCSqSIsb3DQEBDQUAMFUXDTALBgNVBAoTBELFVEYxETAPBgNVBAStCE
xBTVBTIFdHMTewLwYDVQQDEyhT
```

```
YW1wbGUgTEFNUFMgUlNBIENlcnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEy
MDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQKKEwRJRVRGMREwDwYD
VQKLEwhMQU1QUyBXRzEXMBUGA1UEAxMQ0WxpY2UgTG92ZWxhY2UwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgWPK2af0+StijSNOR8K/hN8D+1
078ou1lsk4ASvSwjsCNo7sHUa4xQU15J06VqY18LANw0Rjrc9BaX4MguzsbFXBe6
uFh1mVpXmFxpUBByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUE0
ls/gkUP2Gxzyms02kaYWTut3SryCqeHEFbZFk4urMk4xrIJC3CzWruS2Q0FHbB1
fkgKN5wXVgkWfFi0ucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614Ku
ElNAtJ7BtZcs17dUy9u9C0gEyKriVokFQgqQ7XNDU+r3Se0Wwks7AgMBAAGjga8w
gawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDA0MAwGCmCGSAFlAwIBMAEwHgYDVR0R
BBcwFYETWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0
BgNVHQ8BAf8EBAMCBsAwHQYDVR0OBBYEFV2zLIthQYSHJeuKWqQENMgZmZzMB8G
A1UdIwQYMBAAFEwJnWHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IB
AQBziaI2p86poGkjD/4Kkk0HG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAo
cCn5zbzhW/JVdYn30UxfyrZlRAzEf7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoT
WgAkoqENT1sRxlcvb7HVX524bKZa1oPTUNl6QpivtqDIdqGJdGf8L1zLfxBuo2z
L3HR+M9CDr40pq2JCKzP0Qhp7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF
07rNmT0TzPCVzUAuBlr+JJtz0KypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSr
JNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCAfwCAQEwbDBVMQ0wCwYDVQKKEwRJRVRG
MREwDwYDVQKLEwhMQU1QUyBXRzEXMC8GA1UEAxMoU2FtcGx1IEExBTVBTIFJTQSB
ZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69Phqzppq1zALBglg
hkgBZQMEAgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCsGSIb3DQEJ
BTEPFw0yMTAyMjAxNTE5MDJhMC8GCsGSIb3DQEJBDDEiBCD7w9aychKiKqa6/sht
F4TUlddh7IbF6DnI0Vaa95yhfDANBgkqhkiG9w0BAQEFAASCAQCEsnuIovDVN0BB
UStxOARiNhm/IrfGyx0uYeIMCR2K+UZIEQ2+aeYGEYKh/2yocr6VfauX0Pk2prW
s8bxDewJd0Vgw13Qbcmgyh0Mg/5dQLh0pTcFx/5b0rYQp2dLwpFIOzUrFnycGJI/
6qo82knE2ch/7NMWtKB7Y7n9xKBXTC6kD8LwIrG/li0tSyrqcx/LUODNznTB6xoV
KwNJBH0JiBiqYQFHoH3wyXF7nw3l5dr70TSpAt2A/Sp1GSYA6cKzvI3XcEZD3/5g
9IUQmkPXIZPWNBMigxBZX31d+R+RRwSiT5gD0zwFo82KnuHeoDtH0l0caxXd3ocR
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

MIIC7AYJKoZIhvcNAQcDoIIc3TCCHNkCAQAxggMQMIIBhAIBADBsmFUxDALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBtIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFGU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAAQIBAGPIKUb07uaza7TKuUY2av9QvG0rh+II70JF
jmfXt0q2FRJynyfRCzQt0Th9HmQuiuv/0D8oNXyiyMvPZEXbXc2IECoErnn8dCN0j
fpq060KYN/tpAsUDCLXiLPa581D574tMwb74AZ2AULbEv7TdNT2HtdFA3ZQnts1
8+WB6KiHvr3Q9Bwkf0tyj+fUvVm7MeIn+i6PmdlQjoYyBGzKsYj/dJXFfNM1YHC4
GNuHvUM8f1g4r9yUb7QkjMmXksY5CUBVb+FGry5tMa0qY8AHem7eSYdu04rdgBaW
PUC8CP+QWU7lau/XoH6Gq9WTgE88fEZpdiaMPEsLXoc4eDuWRxEwggGEAgEAMGww
VTENMAsgA1UEChMESUVURjERMA8GA1UECXMITEFNUFGV0cxMTAvBgNVBAMTKFNh
bXBzZSBMQU1QUyBSU0EgQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAOLJluJTXnL4l2INjDQAw0Hzd
h2yJNC1q02iZ0VHyGxsA8Q0YTHjggBCB7Div5Mx1AyAKZ0URNwDkPpkEmLM1l0P8
hH1N46zT740PBerrdR4+tCHoxExhwdwS7D/5gh/5FGZTx+TqLswH4UG9hyVT3fWF
f/bEXPTaTpm1SwUajnJVsbNwhNxxXUR4ANzCIJvStWsxRxCwv/U2v77oCZkmbpY5
yGz+BeLSx5hX15PbL0AjYiVnMHPx1DeerBU/4fyxLRBi0+2LpouR+K7NjhmDh7JU
6DQabdXzyh97AF5uR1neBztOLx6VLbFh83XbeLBoRh46WsLrFP0HuggyCZV8+TCC
Gb4GCSqGSIb3DQEHATAAdBglgkgBZQMEAAIEEiYh3k6aQwiv/CB/9ZJiM1eAghmQ
WIC9ITS+o9nkZZyCWgZEmdcyG17lZgLRCP66EibaFTqKmbfPUbcSkzKz/yQgTYut
Y7KBMXLh1066qhEK9HzU1ShfQLtt5G/+FI+YcYwgWY3W50HHkGXtAVfF16quVP5G
fuJEHx7yV17KCgVSqvgG9S6inZPXDHONHEo0GhpKRvs00LyVpR9NT7ToDIpLMihT
GwxKw8QtvmIPkp3cxt2zT8+6VZR+M0DsPkqKTZcP+yFd1ekvifdB+TEdx27Y096h
0oCJWxzKkYVqHYHBmI9Mn16p/I42BaHLqL4q9Px1AZlAxG030dHURVHf3+z0nARC
rTJwo1gsxtrAYJ288okEeZUGI4Ia3j7/vSXu51k1ZPg0iui0tw/r0xpHB/XStsJz
qC7Qnhi+FU1nw8icx9d9WzzhVFuY0Qcmnvk1xoLuSdDYCVShUvh13punCT+k6/Zo
T2HGqq039+NYfZBi8DhpefyXyRFT47YB1Xyi4JUa8/e8+9+JrJdzpcRf1YPED7Bn
+tDz/OqQOGY9G7hNS+2BIXmIBK7QlKQo6L5wT29MjpQ5fCNh5m+lpCPPP48zi9z5
7duvKwRM+nB0bXSFdFhpxr5A91n10Cnd3ptb5XNaIoNQ00C0FM5CUYDTn6aHr30A
QK4xKaDX2ktEKwIVifziPtvlSIHEOBqawn1C/ABM71W/7BRDRddzs21B1IOfS9aH
26bcy4vQw/+NSemAuREIO1hY9HA1DTgY29ogWot3zPE26TRD854eyi/ETKnh1x3t
GlxsDbEitSoykXpuBHncmZeFUyG010zjCuzDw1Myf9D8zHARm+65Mx7ViKa3XPsv
8x7BK/OhYbqSSQDthDtL/El5icm9Sl/yCZijnVIlDpQa3jPM0QfEy3/Liea8UTS
ODaJ/tjY3pV9SocZf7DBBXUkhHBb4fRrJKsK/sDFh1CGWFRL0AS+YhaH/qs0NNbA

```

9Lns6XbbSC/4iV2IJxoTuJoZ45+05f/q5ZGFg062m8nvgMAQV/eK2g1Va5/jWkwG
lMn6X4JT4wv+uqaAQJWm1Mlb+9gdbV7nM7VY6th10Qm8Cm1bQdv1x9d5MSkm2oK1
/LwScnf4riZW4371CBucGpmmWcguoQvokf9jew2nzpBf+ED84hEtHX/IiAvzZ1HI
T0IvB0jMXd3j2Rt6h7HuhxuBgTb6ZcTv0foGZsxRMFZEz6niVCq5ob0Gjff00RNB
v2jCLAQ0h4H9KkpUZxSTKNSypXIBXyWylQm407Wk1CLZJb9qkXKwHswoFGIYmX
VqpmNTsthLgou62KeVssCypIASBL02fVbJwhkVWHiaq0c2KxYiFecesfyDe4S4Ux
/01uQCdbQKdSnoj/nDX7oFF+iTCCVFSnEr/6ihskWCjnWmYqu0UqSY0zZv161F0Z
ajOU6WcUUVkycB6KuHPgzMQqMLbHFGJ8J4lk09IMg3GYSZubZRq+XnwriAsnuZQX
lpNGh2EzZdJUU2f7U/FFNZOCVAXinaxJVvUrszi/1lhjNs5D5ZbMZdfb1tWuZ9F
gSRdVfSnAs2Z79cMD0fowSGefBHp/JmNctqZvGaknv0kwuees36nvxIe2R8Ggpi
HsrgyXWfsJMX47Ac12IHwMxDSLWT+RG4yuiXvKQ2nXiwFWr1LgyAv7V4RX6oNkZ
YvnQbDx5QfjZuBnBRW1tg3RA6DfJaeacZJLXG/fTAB8Mfi9xMHLX0m0Wrbjsz9M1
Rn7EjvH0sHlXvos0ayazwQppzynCn601MNxVqZpU2MSWanSsh11LB76zqZHPNMd1
mM3Qy3w3q7aN/6pI2EPraFTtbNaMufQ7fTnxELGs6pBgZjBqG18AZ+w6Legs5AE9
k+tJpmZbaGGyH0W2d8GgYW347y6ZRFrdGv7uSwkVE0iaJt7//zLChnBBx60VAzqd
fFztNGDShtQJ4Q+nx6uKt9D32kWFsvS6aDwviqWE1oBcStBSNzrDQApVvKUNKsh6
P00RT/hq9QQHM6WnRH55L35CQzyj2UT1Q7mIoZ6C4Iibavx9Ln81SnErr0IUVIyD
QGdAUytvyvVcc1dgLSP1Sw8AIr93BHs9tJ2r33gmpgQS1CZT1nMqjNj+H73A50Z8
lfri5Dz3fP8LT3RnSIfSaxaw6yYT0ysL0P/3M5P0D5qFw58srJjq8Wp/NueZKWqH
+5vBpgaxn/pIy2xYSiSsP4o9jk9Yx8ptRBh2Sw3xeoyuL0sgzQzL9CqyncgAaGP4
W1aWsLziQk02klzDSPaNo41S6w4320EiM7Txi2XJbsnmKq3ad6sv5yuC6s0SW620
ywMHL5PJXg+yiFGU0Lbeb9zgoxhDU2nvzj0ApgZKrotf2Nq8d1K/x1taS1gQrUVnf
hS2M19ifp9ymMZqm0D/wKuvfnSkHkN8pizK9CrpaFzUxNk6X0d3+pqQUHQ4iPBJE
jizY5DUq5AECn1qNJ7/UONjnneZcQMNArfIXzYDyDPNWjs3uptM56AOS3fRP6U7g
lXFgyybC4oK1To9k6Vx1VAL0skWSrT+WtATUMcGXfD73EuqJvpj00Wp4ATiaqIsf
QiXUCB8fsbFxidjcm2tJ3A5k8NKMYTdB0YhEzHKDRk+r1k06xagghXird0fJ5rx0
cPzNvZTcSleLXKHQ8e1HAo8NYF+dLaXIrXQoghAjZFqCp9A18ksvoFUbXVvpaND5
5bRMaaCVMOPXscS0RTD/UP95kDstpywBQVC4GjILK1bZ7n9lfKMRuT/3lqqJiW5j
FTId9wmeelCWSUtExyihpJBsBKro900+bTZH0p5Kai8YPjPxf5PNw91Fry9bPFXA
PbziUOVwYXj6EZMtzzFNu0dw9ddsyzw3Z00RWHVERBMR6j50JkCyBCwbU4F4hcGs
KkyM34GQBrrtCdVWsq0t09rTzFXj/D/oeTegveQelRhAeNWKI10z3HOV0c7HdM5Z
w5dYd0w1D4pB0JvLiR8B4/9H1SStyuVEeu9Df2qsXdbhnNrghY5KP+nPU0pJxyGe
G9NYxlylCc+b0jMW4gzMU0f+n7vux4ixKqsCfkG/5ju4dgennJqAZX38dsrL/MaU4
Kfh8skm6ovp6RTBggxQ+js9tG5g+5Qee9y/uq+uKzGic2o0Iz0LkX0wH9k70Sm44
d7j1z0sIRG3qeT5mNy/Teq/buX86kcjbK4h3G6u8haDt2QohCF0kQ5e1ffeZCUKk
/da/WyQNUv2ERmgtfZCnXzaf0CnvkZayhBFfe06rY1bt3S2kJgIjgfwgPuS1+wZu
XV/5URoKKK4RcVeY5pcqkUNjXhLTlMQXnC3Ahw3N+855qbqxsyeFTTs++Y1htM4x
H6Gu/fewKXFTiSyzyhOnVbpo5Hf8gEnITBiMa7Ji0jgscZ4YZyyt5X50misnSRYz
Mf5icnM0BKNddRTRzN5UQk821KYyoqam2fMSWMTdW9SNvdSPY7B4uX42XVqChZ3u
5rS//1kasqSNm0e0hVxn+2Q3/5AaScU9c2MCu2rqc3Zy1eiVtUYPDkR28jDpGHue
M9UtHf0oysd0l65ihmG1sv8IEpPpVUq2qjIL5FI9Mk3IX3C4geYHf07+85oXV8f7
5QK1J86eCdJ1DEzcN6MP0z0J2DycRyPL1wSGBmiZ9x2PS/k1S3N3Qh8tWJ7KTzFR
od18MSEm4n20F01yWHX9fZfz1XH3NIJJTdw41PUW731xfRMeE4/j80rtjQv28aIR
iHQ33hNVXoHaG03Ws2iEZweYRiroUk7wJXBx+K9U8n9ZuvmaFErfX5uXGcsM9jxf
MbY2/DtDxqTBoxItK7s5cThwFm0tcFfM68JmyqunprH6A5iUikm0cY4Hkz2xSmbo
vW1DYK9/TQhhr/axl+jp1jr8pu1GXG0fbfAT+jc+WM2SJqwnrKgAvcLCMs3QeXe0
2piT0pIWG47aIrAjr5iFkJtBsc7HQEH99zhUTPE5rfISvr5xpPi1nhGTW64PhGUW
ZSvBkw0cn5BjPqcBM4selB3B1fm4vVcy2Gq+wd1LPhiYSPw0nQrHWysxljk0BbmZ
ln/X/XoBb1/66MosPE5CVkoi5B2kpJCPMfAIuyQEgbH+RGPWLpcg8sP18oQU6HK1
MB13KYNEK0T3o0Yeq10LEsc+wTmu+zkCJSajRtWX93TtLtjSo7oA5cSgyjvcFepL
tE0CvyS2XVwL71uU7cEb0sMtJRdtm3ZmbqTp+zbGJch10D1c8BN+Eqkx0wL8iHuv
JRTv3gp6yeg3M/3jsz7HBMEVPqrrTWWaAMRd2vX+RfoxqPRD13N3A6quD61iXvi0
IYeStHLMsLKRfZLoxc5dpDgxXEeq4UoEsJbLilRqr68Db95zS+3sqAomgDela1fD
GL3BzdH950kw2fQuvuMTm5XBeymrsmFxbyslVb5nX3jKoM8IGHn0qiIDN1DoAu+i
CmJxQbDyJ1HcyI6HjTC8jfyP6DT/eEwnKzahiopMemQXBYDQ8tgVhm4IkM+t2gG2
enlGVK01rubR2EZJ4HQa8adhNjGxf2MkzUfh1Effmy90xpCvShnQ4xp/Y8JT5B20
5SduazYH21lyjyP3CtRPa34fPPE/lym6aniPs0R+bRwG/ExVqhdzcNnp2QCJRvaf
hZB70RvIx6qux5Hf3wdb3HaFqmpH7PH4Q/r+QPk8yE3xtLyjBShmYrx5NfRfBlr3

2HpjdBCtNlVmaR7yNy5TBOR05ihkMZ4nMXzcP/GJ3Ag4e6kmWZuHkUBo/pTmBBRa
u15Ybtz0emLNYjMiWgFg0XMXxZVpuMwiSmxVj3aJUjMSAp+F7uVlPOi4pCm2/4lY
dBDOu5xZ9nOrIjdXm/YW0QFqW0KoMNFuwlx6KtGBMHUgxPeJU1N+oaUgnjomroGS
ZhoarruT7G1NyKSotBiaQkDSEKSWn0WnjcObCdedLGJqkYGeeadITiRWL+zxbDgG
XaRTHuiX13avTwapZPYfD81dXMq69RHfhnGr5rhU9eXMowKALeoT0uD1bzEQvg3M
r/YDtQE53Ysfe0ktAs5Vn5w5kgFMeHxb3B9DnZCE6DK1j9qU6G8/NGe8Ev0tihT6
XVbhFovfwN66igL6MNqm6pBqtIWIImVAPeMp8C6VL9EkvcFLRUDSBo1HTP185UPci
DgJTERFXiS9GmR7R9b01JFjVmwM8DbNwimi+6LZiLA9GtcdRMFG8V4usHDV40Wz
Yv0cjLv9403QmXZtvcUjB1716UIngAx0bLlZ/kvUh60xo4hkp+FSdnH+R6+XfDG2
44YVX0s5Bnd6xMaxc6Wm8FNlvDYTmkkqVmn2i7z8EaSuif/08VhNNP7sMFodG34y
yhmhtVW3fkod1G3CzeDKDVUuRLKO079BTh4208GtNL0Qmy6iUCxnjAbmgc7LIzfP
J2euFeMD3ysne9tVK3h9J12iBUHEvlpeYVew/BwcnbZgBenQ03PlqfNRxW9pBMQF
rtrv3zeov+H418QT8wn0thzTmDQUEu3BYsbyZ+mwKs9Dd31qNvZ/4oV0HBoYjfn7
ETMLy0cFi+L5wfjxHbf00wgxlf1/ch4tc/0moxqFtsPDzt2kUzfrTPJjaxui1wz9
AFnAR2Vpww4xITn6nZo6UJe6BMAD2TNLMnvA5EFWNXJEOUzbv0Q8uJkfJhLEtCpE
Bw118N0R7KDUWI39xzKGA9+j/A+s/00zGG5Vet3DdKWW/domeWo+d4rYmpKQDtrr
V0/Dp0rJJkJVItyuDl+0yEJe0mDDhHgffQIhx/Y61D0KvE0yEG404z10eGvHoVGX
aSv86D10a8IHVoJbXRtNMF525c4UP7VPh11wKD0sjzYkofaJvwPqZp/GS18wSYo
pyVmrzIWFwDXyrqEiXFDLzXxcGW+L7g15ntEqP/XLsda9DQFJSg2hTafhhWgM0og
fmIHUy0cEUtycb4RvQSM1Pkg5h+kHUMMpUKuhF50Pgw3+UgxwG2J3CW1DKUQZd
j+cu03J46b0o4/0eY8NoNqpWK6XksqSH0g1wVsyenFuugRsuESiSiZMTNmCqURS1
PPFUYeMtUgSQ2EDLV9T2RkaabSNmVG35jE0CQM0BaF7XU67reXpLsUqPg2yhQwn
EzX6KM4qioqC2wrqk2a1SdqRB8L8BEKykK2kv1bqvc0DNl9FoUxFt5uEH6iKHARk
SkjLaQZsRmzu+ueHRhTqcSHEKeVstq9jWc/heW4RhP3LQgD43Cvc8m7yRqSa0kor
08Pc707++t7SDvYMsXFVmj9MbB34HNgmXk5gTTb0AqI6fKyXEZCfJl0UMBWWBsKU
mEGUu0Y0mgK3hRCsXBugFIS6K4galFCx22U3hoByZoiVjLduQhRQNPC0mFk5aB+i
NwPL02Y1B8rylvz3fV88GH9A1PrIEPJzCVsabx0RVQeiJYCISJnvRn+PME02aqBh
7q0tTD0lTChfj7jBgMsDtgyptWEnObAsiL9+Rm4UsnHBbbp0Mbn7rhZLyjEKkc8d
Ej/6LTuQGjI0dPEcfIU4LMFh3mZiWoJhLTDXi8mEF/+m2BcX77fKgdum3KM1FXzw
Te4TnpIET18zeigaj5ie+BKmac2Jmxas0lrmUP4KLD1kwF7bgT0sahZzkPHmBP
ykrogqTdmYUjkTyQvDzVUyKi4PhnthaljLEY0j+LhZ0DSr0hhbsfM70FUXqpLeE
+tr2hGdj3YZOIJkfsYWH2DqtEeD1WDbhBfoaT7EbCFi0doFHsAz+BX2PLZJsIqJ2
BuA9mci9XB43ssokteKCqGT4QQn6KAekoEDZ96wHDTudcXIbYPdZIrD1xFHGjS1a
ZON109Fa2IBuLnMhKuYQXoZwUUnXSI18Ga3Yt2ljCEcKeXmo/juIkt0b9UPTLBq8
r4kb/ExUJ0kUgqUGmL5rSZszWWYmxt1nz0JkEd3v4i7LUk+0mGIIdlK0E0hqLSMn7
YVJwhiEqIPHu2PnnDUTqlDPVMGG8wCZFznzP/sDBm98/nIJRVXSEc15BYFtiUqf
cqG0gVAV81z40FFfg6TlP0AGoZqXjk5It0p1TwjWRR5RaoggYzL20DmL7Q054ogDI
51EgMtbY3jvN6XAA2X3qPUsCwinlxaUMCJJsvEN8c9YkouvsbNG19eBRCpsC70+l
HMP5Ybh3ypJxSQHCn8zEa4KmJYsw+7Q8VQ4nCmekbhH7Z8l+5Mmw4/Y6+Wn3j+Zi
n195bYnS0S/FF/QVI2CbZAn2IKlwmGVtIsV+XgGS1rPk6YvCgHurK9NhrRS1j/5/
ZbFWKUzMCpBbXwuFWP6yS0UBzTRCTaEGIZQTpNJawmoyHsRJm45Sxxq+q/0Gkieu
u4GD2XQsYZhBKL24NhEW2fMTrqHeuyiouQi0dKJlV21pCDo9cgqbd0Ikz5wx8Zxq
DKVP8yc+RXQHKj6PYnmAQDzsqt0+21rRCrT4zt9I9uhSIAoEhv8ue6TSnhhc0QbM
8aB588Ass35/PGIDRVpBdIEoDrjHx51oss9J0WGN5E0iVkdCwVRpuB2ttM7UmNv7
3lGG+Hji/FconVZjwkSEQ8KUZ1jss7Sx1Ji1Kyv02+aQ0VsTePkh5JJpJoRFPrcK
dgjZyCnLl/VysqlGFcwKbop2QfgUqlB4ZWZMsnBT9ZmgkD9pUoS12DnX0PiFqT3+
x7YWr+z13W7br9amR57w7TYwdTB5dYCKfuLFC2th0nR7cHKPxAB509pbdTqTIVvB
QtNUy3DpqVpiAp8pAM67ElHjfp/WZrnP8SafvE5tLZt0vcvVF2fHnW4visb/VCSt
xKIKnhsqKJZ8gZLz1l/zV6dQmvAVvWeAwsS2D20UyHlvHKLWnA9fWVq6GsTC1wJ6
2El67X0VbGYPIHgbQ1PgMecWwaapHsmRu8Lh4z6nnv+H3vUG9R+rykvR+D7x8V0y
xXt9h0Fbhfp6PaXLhFkEwAcaXE+w3bLyPrWS8rUv26zYL0KN96FeJTysT+/juML2
FQP706NRcsHaxoBp3jddqxdigMxUJDough7zINNzWCryMq95j1jFP+JZFumD43Aj
tPfvfqv0vZ9RjiirxF08skjG14NNovMys+jyaDv41/1MRt4TJq3Alu9Fwc5DibVy
KWKzf2XlVnYsXwiB7hLc9hv/QG/YTjJbNHoNSlHEP7fgNI5WYZhefmzzkrk1ueW5
IPfgwrQJSG68IpZ0Gb1r71n74YgtyxtkM8sVpk1Hz0l/mUFS0UczFLFc78nTjiR4
Zl54J+pfv6dXQp8KBIhDnyjg1pH2Uvg4Ie5YU5twJ0QufhBst7ookPbj4czYBTcZ
dha1mFjbVPTTqaMuZsiRSfMjMvE653QEWAG+bt9b0DNFTk6/8ZFnmULH6M3h56xs
LnAE0Us6ikIKwJON7AxVZ+YfG6WJpHbqe1mC2V8MdB1tN7ku70tm2KmE0SleadBW

```
3p8lZad1pvL/A+F+3ZzcVYqGV62ojnSOHb7iSEttZA1EmLVArCVCcAqM5IWtjyT
Q+aaZgaKMEVov9FY28UB3Y0l+6SMPWq/r2jxJcTd2z1y3L9yXDLTLg/eIYZtP0VM
iqIkeQ04Lq7CNwQa1GXbI1YmUSqKra+588IQWG5dbCIctteTtY6iLsquK0Yu6ReP
Cs0IQnGrZ4W+Pp43CEZ2+UtnL775n0WgBF9T14U/toMd6+EwTth53KmKVQWdYJq0
F7NhRu0i3RGHQFHUv20RyOwHMRP3xsCWLpx301zLxKzzy5y81puzEaGcsZ9nbq/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
hkiG9w0BBWgGggghNBIIISU1JTUUtVmVyc2lvcjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtYmFzZWxpbmUNCk1lc3NhZ2UtSUQ6IDxz
bWltZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtYmFzZWxpbmVAZXhhbXBsZT4NCkZy
b206IEFsaWNlIDxhbGljZUBzbWltZS5leGFtcGxlPg0KVG86IEJvYiA8Ym9iQHNT
aW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDwIEZlYiAyMDIxIDEyOjA5OjAyIC0w
NTAwDQpVc2VyLUFnZW50OiBTYW1wbGUgTVVBIkZlcnNpb24gMS4wDQpIUC1PdXRl
cjoU3ViamVjdDogWy4uL10NCkhQLU91dGVyOg0KIE1lc3NhZ2UtSUQ6IDxzZWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtYmFzZWxpbmVAZXhhbXBsZT4NCkhQLU91
dGVyOjBGM9t0iBBBg1jZSA8YXpY2VAc21pbWUuZXhhbXBsZT4NCkhQLU91dGVy
OiBUb3ZogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4NCkhQLU91dGVyOjBEMXRlOiBT
YXQsIDwIEZlYiAyMDIxIDEyOjA5OjAyIC0wNTAwDQpIUC1PdXRlcjoU3ViamVjd
Z2VudDogU2FtcGx1IE1VQSBWZXJzaW9uIDEuMA0KQ29udGVudC1UeXB10iBtdWx0
aXBhcnQvbw14ZWQ7IGJvdW5kYXJ5PSIzYTMiOyBocD0iY2lwaGVyIG0KDQotLTNh
Mw0KTU1NRS1WZXJzaW9uOiAxLjANCknvbnRlbnQtVHlwZTogbXVsdG1wYXJ0L2Fs
dGVybWf0aXZl0yBib3VuZGFyeT0iZjMxIG0KDQotLWYzMQ0KQ29udGVudC1UeXB1
OiB0ZXh0L3BsYW1u0yBjaGFyc2V0PSJ1cy1hc2NpaSINck1JTUUtVmVyc2lvcjog
MS4wDQpDb250ZW50LVRyYW5zMmVYLUVuY29kaW5n0iA3Ym10DQoNC1RoaxMgaXMg
dGhldQpzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtYmFzZWxpbmUNCm1lc3Nh
Z2UuDQoNC1RoaxMgaXMgYSBzaWduZWQtYW5kLWVvY3J5cHRlZCBTL01JTUUbWVz
c2FnZSB1c2luZyBQS0NTIzcnCmVudmVsb3B1ZERhdGEgYXJvdW5kIHNPZ251ZERh
dGEuICBUaGUgcGF5bG9hZCBpcyBhdDQpTdWx0aXBhcnQvYXJ0ZXJuYXRpdWUgBWVz
c2FnZSB3aXRoIGFuIGlubGluZSBpbWFnZS9wbmcNCmF0dGFjaG1lbnQuIE10IHVz
ZXMGdGh1IEh1YWRlc1BQcm90ZWNoaW9uIHJjaGVtZSBmcm9tIFJGQyA5Nzg4DQp3
aXRoIHRoZSBgaGNwX2Jhc2VsaW51YCBIZWFkZXIgaGQ29uZm1kZW50aW50aW50aW50
bG1jeS4NCg0KLS0gDQpBbG1jZQ0KYWxpY2VAc21pbWUuZXhhbXBsZQ0KLS1mMzEN
CknvbnRlbnQtVHlwZTogdGV4dC9odG1s0yBjaGFyc2V0PSJ1cy1hc2NpaSINck1J
TUUtVmVyc2lvcjogMS4wDQpDb250ZW50LVRyYW5zMmVYLUVuY29kaW5n0iA3Ym10
DQoNCjxodG1sPjx0ZWfkPjx0aXRsZT48L3RpdGx1PjwvaGVhZD48Ym9keT4NCjxw
PlRoaxMgaXMgdGhldQo8Yj5zbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtYmFz
ZWxpbmU8L2I+DQpTZXNzYWdlLjwvcD4NCjxwPlRoaxMgaXMgYSBzaWduZWQtYW5k
LWVvY3J5cHRlZCBTL01JTUUbWVzZ2FnZSB1c2luZyBQS0NTIzcnCmVudmVsb3B1
ZERhdGEgYXJvdW5kIHNPZ251ZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhdDQpTdWx0
aXBhcnQvYXJ0ZXJuYXRpdWUgBWVzZ2FnZSB3aXRoIGFuIGlubGluZSBpbWFnZS9w
bmcNCmF0dGFjaG1lbnQuIE10IHVzZXMGdGh1IEh1YWRlc1BQcm90ZWNoaW9uIHJja
GVtZSBmcm9tIFJGQyA5Nzg4DQp3aXRoIHRoZSBgaGNwX2Jhc2VsaW51YCBIZWFk
ZXIgaGQ29uZm1kZW50aW50aW50aW50bG1jeS48L3A+DQo8cD48dHQ+LS0gPGJyLz5B
bG1jZTxic18+YWxpY2VAc21pbWUuZXhhbXBsZTtwvdHQ+PC9wPjwvYm9keT48L2h0
bWw+DQotLWYzMS0tDQoNCi0tM2EzDQpDb250ZW50LVR5cGU6IGltYWdlL3BuZw0K
Q29udGVudC1UcmFuc2Zlci1FbmNvZGluZ3ZogYmFzZTY0DQpDb250ZW50LURpc3Bv
```

```
c2l0aW9u0iBpbmxbpmUNCg0KaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FBQUJRQUFB
QVVDQVlBQUFDtMlSME5BQUFBY0VsRVFWUjQydVZUT3hiQQ0KTUfNuzcz0W5PM1Rw
UncyMGRxcGJmQVJRRWpPeXdPd1luQ3RrREtYmNMazY2c3FsVCt6dDljaWRrRSs2
S3drWg0Kc2dyemZjcVZncEwyam8wNDQ3Z1lEcGVBCmsrT25KSGtJaEFmVFBSaWNp
aEFmNVlKcnc3dmp2MFpXULdNL3VsaQ0KdmRQZjFRWjJrREQ5eHBwZDh3QUFBQUJK
U1U1RXJrSmdnZz09DQoNCi0tM2EzLS0NCqCCB6YwggPPMIICt6ADAgECAhMPLSW9
ETmXSs5CVIEh7j00Boq0MA0GCSqGSIb3DQEBAQUAMFUXDTALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTBTIFdHMTewLwYDVQDEYhTYW1wbGUgTEFNUFMgU1NBIENl
cnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQKKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMQQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCalsn6i8Gi44/oAVAn5Gnck4PHHNjrSfWUnnelN41KImVaTC3D9zFCrS3i
4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2Gmt4jse2Dqs165ernT9
05NLFf1HUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCREZuTtMc1zy+
+MxQlqdn9WZLh0A0peNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCq1LqhBwDhdZ5qDTII
2PVX1X3K7/c0NxbvBbaU1/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGewy6SCf58du
q/AOEksCAW1b+MD8QH9Yj7CFsmq1AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDA0MAwGCMCGSAFlAwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHsUEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBSAwHQYD
VR00BBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEwjnWHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQCBSXignLEynBakDKU68ro0
RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsoX/Ht9Ii6zyBZVjdaox644DsIL
OQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhdvTxDN00oHz53PYDBh4zE4Nar2inC0D+
VM6RGDy66K9l+D+b18Wj9CyGUc1ppMNURexTg+z3web/eD0du+F2MvtluLihne0B
p1GUTkr0mJBo1g6dSYa18Hw8/ANHpyEx156BJABb744gqoeuD9YSHjKK49+qYC9f
aFmQ+mK801h1M9RdNI7srjn0LKpuob6w06jaRzWdNeXz1Ec2tUpAr4vRhZjVD6FY
MIIDzzCCAREgAwIBAgITN0EFee11f0Kpolw69Phqzpp1zANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQKKEwRJRVRGMREwDwYDVQLEwhMQU1QUyBXRzEXMC8GA1UEAxMo
U2FtcGx1IEExBTBTIFJTSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOZENMA5GA1UEChMESUVURjERMA8G
A1UECXMITEFNUFMgV0cxZjZAVBgNVBAMTDKFsawN1IExvdmVsYWNlMIIBIjANBgkq
hkiG9w0BAQEFAAOCQA8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfcv4TfA/
pd0/KLpZbJ0AER0sI7Aja07B1GuMUFJeStulamNfCwDcDkY63PQW1+DILs7GxVwX
urhYdZlaV5hcUqVackPvedDBc/3rz4D/esFfs+E7QMftmd+K04s+A8TCN012DRVB
DpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtwS1q7ktkNBR2w
ZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR+peC
rhJZwLsewbWXLJe3VMvbvQjoBMpEYlaJBUIKk01zQ1Pq90njlsJL0wIDAQABo4Gv
MIGSMAwGA1UdEwEB/wQCAAwFwYDVR0gBBADwJAMBgpghkgBZQMCAATABMB4GA1Ud
EQQXMBWBE2FsaWN1QHNTaW11LmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQw
Q2VydGR0PAQH/BAQDAGBAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAf
BgNVHSMEDAWGBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOC
AQEAc4miNqf0qaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJ0d64roA
KHAp+c284VvyVXWJ99FMX8q2ZUQMxH+Xh6oAfzcozmnd6XaVWHg4eHIjSo27PmhK
E1oAJKKHdbdbEcZXL2+X1V+duGymWtaD01DZZukKYr7agyHahIXRn/C9cy31wbqN
sy9x0fjPQg6+DqatiQpMz9EIAe6aCHHBh0iPU7IPkazgPYgkLD59fk4PGHnYxs1F
hd06zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+uCDgNG/D0
qyTbY4fgKieUHx/tHuzUssZxJjGCAgAwggH8AgEBMGwwVTENMA5GA1UEChMESUVU
RjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0Eg
Q2VydGR0PAQH/BAQDAGBAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAf
YIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCsGSIb3DQEHAQAcBgkqhkiG9w0B
CQUxDxcNMjEwMTcwOTAYWjAvBgkqhkiG9w0BCQQXIgQg2xAXJLd5cNPK2o3i
Jrcgqk/WAtQzwmzkVadbd10R1gkwDQYJKoZIhvcNAQEBBQAEggEAWsHGjwENGvC0
GRVd3mp7i5QJPMYvHhAuma75gcRKwPleEQdka1P95xnNFTJiDmaMzf+5wDEuj27L
zgf7UffeIJns/d/xIGGXTuUR/IPvT1R0sY9dS74mzFH15fY309iHtBLgaBjJ76WD
JQ+9To+vEIk/gFhx931G9fYBZ3i5wqMcCoG0UHYG2AXTNLFEDhW3+7Yz11eqS6NH
yCcFwEB8iLvLs9hIGoCbcsckgYPSbbQx82NzQjaEH0tXqLHXAn/c7a4zn8y6qV2k
o9ewCiLmqimEsac09ZJYmi7XdwDo1B50ylpCM45Mvn0n0WIjaLCU30oqw8LPQWS2
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

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739n03TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+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
BAoTBElFVEYxETAPBgNVBAsTCExBTBVTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCsQGSIB3DQEBAQUABIIBAFzRRJ4ae2Mk811B7yZRDGmCK9wJNrPFJTno
34WR+wNG0/sDCZCYzBvpNXScUVbk/+Y90xyCKLXZYvP89rkPvPPEDjm0faAKPw7r

```

9CodT58+Zxc+mW50t1G/ERj0yL1MFa+yAvWjuAXuQ25+mZ1fB2TkMQ6pZPg38smk
Gt13Dzqx31lCmB3JSYfBJQ3SCNOeRQzZENp9dpo0o4+wfXBCukVTGPexmnX9GIkL
9bfoTfqc0t9gPQBxKnOG/hg6vmEQN0avXjI71fCMUwj6nUr7Jmd5e5P9Js01/4Qa
jScrAk/JdFNixNiVarqYWEWiIeTRu8NidcW3L941Fb/3CSfcgR4wggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUYBSU0EgQ2VydG1maWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEGgEABb5CqsgXnqK0Qb8V12/4362F
J3hgPcMNbw0/59c8Fmn1ETL5R85beGapoHKD9hlejMVgyVPJucrSzVX458JBx7F8
Q2gcINWqe4i1Vul4vGwFPQVsyK5ufH7VnNYJ3rwaig1mc+3zb2NaF8rS41xnCHVD
0Fc19lpsN3iQ4hqzUNKTupjVKmZJfIVvjdwWrTnqdSbovmCAFYe4b5h+1IPfGJ9p
RZNDWB4mZk+adxhK6qYxoAqzJE1HmF4NwJz0BKaknBPr9jWPa6Y6A+ap3Fn40fYV
NXqRS0LSSqkT8D31CoSdbWsBH2SLVWHm0tSzvQfNh1jXDRfQFssgg4d0XiL+LDCC
G34GCSqGSib3DQEHATAdBgIghkgBZQMEAAIEEMGuYxUySDVL/ohXx2NMvHaAghtQ
poigIUJ21hyg0R0MwSilm0nxXu6R1AVjlj9LiS9iEfWStaxj1wv7I03AnTJDMpEn
4JUC6w+ZKkG1N7KF0vi0Ci1l/dIBcmBrUIBH6GTb1AVVlUI8NwnIR0Edv/Rq1NSj
dViDiZerCe6EJeD0oirYPPjzofrd56glnYCetuDXFnMas2ECP7pu6YaB3MiuL01G
McK9B5G5ior0BiAigYPpMW1dmufoOJFYX6F7v5+1ZrIlt0YvGGYU0We0vM3mY1Js
49qkzg8l/6qc89+vLAMDa3f6P5Iv0g10/s37Yz3N8roT78C9ZegPC/85RgA2KY6t
U6wgGD1lqgPUfg0Fd9yVd/konoBN4NxiK2YmM6mJTj73Ii3H2LFSWD9HRJjXwpda
JZqkCjWH0jbugF+z1wpLSFLznRxdgje5Q4BkQDSw7BJsm9a04EgRg/4IDZTXsY6e
zncUis1IjVf2dKCMzLzNA/KNBoSZPxvZo3MDIBr4z9Mp07I2jbtDM50AQCbWwNGz
oUuu4p1NvUJDJoLae/w2j8v2RDpI7rss5hWLqmwEnJJNPMmr7PtqU5tL7kbonPjs
ew6t4aAN2AakJOjHBHV+ABtScANhCDacMa15/0MyS0CkxAIU9ydf4WHtvQLsu81i
4XXLgm8JYgu1znbsil+FSJtVirsasEtHny5xJAHA1CwFCr10Wt9ggCv/t8tj5Xl
gKoxdtM2mp4zsXurP7BsKDXSA27QGVyuL2l60q7VHrwg2ex/7AB31qCP0hZni86K
Fk303ZxjjN3aZo7iXeN/IjaQDhmKEg4qaZ/Kfs+gGA31a1BopZKL4UyFehX5Le/J
BbXPCFaXCxU1eztGqLA4BPSNSuDoUXzHMnm/nRsuUF/d0YHsNp7iVORUVMj9JQP
891eNWch1R70I2q5THAFJVLWwCCSc089vFeeFhZDJHMZ1EdZRP5hdE4pG0j110m9
DGYIWjd59fN26eSbB8Eh0R72L/K8ziXI0bxLd1pLy7F0ae/WyDKL15fykSTd581MB
UqRf1yAiTn8lojH9b1svp2XXNVBNRDuCTJCjQd2VT5Nq00UNN5Hy9ojVyCyqTFza
pwbyx3V5MCZfnZMtEr9A4y8e37ogWC6zm2Hg/3/mgaps1PJsWBZHRqPaIhnytKDq
J3WlegHY6f4WF1XyTVOKZ98mjTytcwRZ+D5QwrNdULt3EY0eFGdBj6Ao11+2EDZh
0vMVjdxFLAXxIyZ3srdqf1jFoLnAqsmJMo1WBT4eX1379SQK4UULoGVIU0rjsCd1
YK7vKED3e502hQc1IKHFD790Tg2VssER5QTLXkxHvoLXzL35fif9gZN0K5WEin6K
aBHSMcFzT2sFtESHpzs3K12FLEUBnxAX4QfvmiFcvH212yUAvnwczoH69w3+xaaqW
mm0QmpNRMxMap1j11LI9lZGG4bp4sHNPd/t4uN/RPjq71+f6HNjbJsu+My0bNTIc
zfmwTlsg8zN8L1biu0U1Nfn79XY01xsLpJqFYGoYUitUy0SBPz77LT3BE6j20sLp
H8Nh1JVlrfBeYwDJJnwkgbElwbQwI9eDkxf38oUv79Az7NFCg3VLtuUgr4VWdBv
6e4vEwamNB36hEtHZuTL7tPuv9mSZD4wzK+sPHxrVyw7Qvnln0PDmzS8Bs211dQI
RIi7/oN7bLJ8YUZWALukzJ919wuicYjFJg4315Gvhw1PBZ4mHNUSU6/EUmm+rC
ULCIyQqAY0CAZj070EEI96J0ZHh9Yh06Z0dh2iNGaZmQ6QRCIzLEiikKPKK6euhf
RtzTM2pFQNu+BUj+vB7rQ8aGD2snw72kd175+Mup85Ac7VJiJU25mR8ojNgku3x
tPRvU0z+/bWw/12RhRfVNUy7Eh4CTB1jixlabRWHQFgs69cLrPly4kXjIR0yw1/Y
7l01or7cL2mFwRzoBJVcu+/pVr9DKya2E65ZrmitUUBF/QWUBEzc78adBHQCt2Ih
2bkfB/E7I7KVQd1p7n7eo95RnVtS0WbwFHCXkr3cK5PzJA0QwGi9sj3Csk6cHrzU
GSi5iGA51V5MAo38pYJdhBPPzAHsD1PLRYcFP8McjBTuBT30xKE6B08voV/9NsAk
a00uHPABP1GwQ11l84a8mECVChkfPge/HJ8T1d9my+Ra8jYakMIWiudd9a2q4/hQ
VzL5Lp2TjAQ9IwbpPZvT0GFej+4KCb5nfW4vgqGwRc3XSX1PNsrDpfrFPUyQjdQ
mAcfjK+kYYBaYgsTYZBaZx00oCqs5BbstQ+Ibs2M3IPqDaPhY5pZ/cWiDtMGRliY
y6yyM2B4oLUdXJH7wbjI1UeG2Zip56QmFbiob4s3v8w2i0fPaP69+tIeGZSCdpky
nqKWZeJZetqwhdbiXIapD3+CsKNmmJHDTnwWqr/kRzatdDIYICZtf+WGLGoIo2tx
g+y4N57sn+CZLEnI7wKwZYcPTSXsWrsdA7+h9EZT8FIagdesKx7B59SNXPQ0/7EG
qzH1ko+s4NbuzJbyiXvEVmD5bNQ7w2Yrv0tZMekQa4CtDusF0zjStqHSZTJ16J7
785dMVo8x0/72VLP805jokuTJNGTYddY+Jh5FbotALz6qtrQiQQ0xRqv1oKlcC71
X/dsH+xzBFvPCq19dn2zEcgrJulYu40jmy5jLGfg33xVMYEMNVaiNd45SU/cEbDX
rBxtsKJs/e3zmKqi7siJ/GvAIVGrVQzMOT1izVjyQ/OUZMFh1vUvBTfAY8e7LjA
wbVB9PD4VdtwjpZdeXkGylCjSkNumlTG14h04mKn0FbuLxOFMTDrU73RE58tsdqk
MI1Z7AnhytTRWUj6s+jBoXtRXwWZgVgb1Ro4CZ6EC1c5Z6DFfcy5ICgI52r+Pz6x

cdINTvTgPedoDqDXv+5kPy1+EyT5/pFzRfp+eIzZmfzXvrUzXSK2UEyxVxvJe+t
eS+jmBFNhhvkzZQ10UcCsdKjhgDc42dR+N1gNUem5UXvsMV8JGv6rcK+AOxGIA61B
Aby/E5dXc1YT5CJLS9NRGidWXW6ltJgoYORM/97GVNJeQRa758t+7A0rV/CaHJlg
HR8pjTne10CQT99BmYknS2NhG0XrZsT4/rtCsUvJRrR3bPyd6M868jWmW443w0Fx
AYkvOQW2J7GDHjJRwJqhK2tDhTp19Mtuv1Uv75UuPSP+sxncjz4mGYR/A4vkjFD
W1ZLDXH4RcS40511TQPI6Tf9ii0C5qFTVqj1yZUVnYAE49nqqXVFaRH7b+z68VMq
D61ThDEMvAlEMNrM0uPK6czLqu7jpwBAFaJGsJrFAgfQ8C0VE1+ZcjWM9uP43msH
2CNaqPKu6rhZgbhNt1TMSzIS0hJeTCK5LT7rGc00CLDnM9yqosAZ/3Txq0xw5pKX
0tUsaCvyXOH1WGk0IJGA0W5k7Q/tV5zBuddtt8rVj8WbmV659SLU3TTZkG0p6SeA
FsoN3/w71djAYPJtNhHPqB+TICv7rs2JhhHbHvrHU16L6118UgSM2TUtxZEQ5CXD
CFGvy0zap2VHbUyiSdE9mGzv0LrnhR1IarQDYy6Raxha+5Efd87bhpCdluiT4oSw
8zsq2q00Yv9XyGDBgpZPRtZC2GJDYarXvnHWtqVvFo0HHyNk8GrOWfthhR7uINuP
xopCfRl7ijnBhVSjC/cdXP4KiTJkp5CkkRLxuy7polGvxzB1Y8EP62iyhP90z4o
AW6jwfvYaAa9bjX+B+QZYKjYZiKXbdu55h1WMGXng9yDhQ0NyQMPbCMprfu4tLr7
Tv/bFEak1T0ahNORfVzioWE/Flig3JotDqB6wJE2EmXtjH426cn4orFNyai0ff47
PsoiGdUJvjKfWVe1X+71AD9+xe46JyJyrnvLY2y1gjYlJVKFe4rhLfrCwU91xFoD
svrvz7LMSSJhuCdvCPq90S6fw97upSYVLUWt4KIRtD0i1vxJper49VppMY4EXNpS
6+6mv2g4SWIfPCSw8C42q+s06KUmqmCMcdXx37mrBy9DT1EjAbrq17WyVPmMQz9v
ehaCSiAAOZCXC2sX3pC6N6o2d56Z6tdFbPSgMB0FW1vuHULMUtOkCXuxIjtucF/v
/vZVmtSAT0v+tpDqcB2tWg5a6vq1/EHXV29XsSZ/Hty/1j/Gt4oirtmmajAVMevu
Upk9+WaDwWtJ44cWEOLnw5d1aiSupG1Xt2Qpo+QtSLFtYSoalZRenOvZcdEqMEMg
1ufw2oTq9SufGdoVbQP+Cjd0hnbaIjqArj0BXMZ2dcxcluy0txz4kyRn72DvcpTiY
UaPFchqerEJ41wTAD5xeM6vFLpnUjnhHTuY8Z2muY1IAspCHaSuQbGbCvtkLSFVE
gM4U7W7xM37XoM5UNnuY5CR0kBs4+RpKC9WxjL9b1u2mHSmHWg4h+bUNSG/OQvM4
jq58X2QVYE0MsHeCgUS+dWAaSSvi01YpeuWkf9LSH30jqrc1gCM9cbrkpodCSrYr
xp7YJpa20hUAB7zobQXNBavpxgOJSniV/NmTYSe+7B7qNPX6Hm3rq2ETH03JvWo1
GOCcW1mhJfxwIKK2ddAasxiZ5h9+r0jE4YDxX0SFCUoTtHZv0AES+5MT5g0ZwMjK
tkmSx7uqngBbnYeo31snUIQXuwjbJymED4sXNcGEFAB23EpJ6ewzdpX8NsNj4agp
Ubtj3qoXs+gvQjmaJ9dI2AKhRuhpBAJ4kb0CQyFLO8LJjnipsFI5Bjsxh4Ntc80W
w51Zb8QCaSEZ1ARJ0T7L6g/kjUd0q/cviMb5zCUdA2hq7m8zL8MhTIpehZgq2Mie
Fqc7nY5YyvKZDkIQF9Jza6bN/8HRSJLS2rYehVD0ja6Q0R5xVsV7EYoEvorBxg+e
4MutPpSDEgQFqGkFQuaKKT2c0Ifv1j9FMyv55o+/puAebsnEBL0qeXGVY/1PWc2D
1YNQ0E001fQeSvvqdC0c54vbU1zsnOGdgcna0w6VgN93aNFmifAcUVoCG/QVGmfg
3yPGQH0/t2RjX2Df3b/oie0Vr37m7Wc9fTmlwPuaib4WhBgzbkAnNkan5eFu20rE
9NnaXTBGJPMRQ8/aNaf178a8L55rFRDJJ3d0MGdq8/Km+1u1P+ckJ0yZtX3ini58
D8q0019JS8D6r80FPyYpGbM4xA+EovnWiA8udN/C3VXfTPf10sIzQ7BxoiFKZJJ8
etGLINGRftBrCuP+sp5TfhfF/9wzLvryCT0wBxBWsqe9+r0uU40yzSF50X9tX/BZ
DrVrIn9lo2t5a5KVYz8gLJvTCDvjDLdE2wWAX5wnmqXZSvoN8vjC1rx0LpJaHH73
fNh2P0PbonAfvj0eWXsdI3AH1nC+AsS2rDQguURUH6i/pFJM3iT23vBkFDVK1s46
SxRyIeUx0LNqoD1J4k4hD7DV6JROMJ2CnXbMe1K8VUXNla80yoh2juCU33PG9DU3
3DN2pUmWUI01p4hYatx6k2m+bB2cJhncW9ApK/seF4XvvS3HmWZ7yBZVv20mgz0H
Swz4pIoLhJ7sHXUTRFdkF59D8Jho65gmGaoK+EJqtNZU9hPxRcHMw2yKW027oVw1
XCBAtnASxDifG5wIqtP4aK9fRPPI4zJu4voqK/qe40DVpjDF/4xnacbmB70q5X9
wgIiBWeZW9Yiu2Ssk2u6s0nfb+JpfqK6IniAtLtct2LUlc0h6uiWQq+B26UgG+Ik
EDKvriy7HEuzaaM2m4lmUy0bay10n3et+sdmbSg0oQ0y0GQBP+TOUZ172y4FNGnq
edg8Dhd2r1IfKn8RHs52FudiEhbtXHfMkiapvj+SDPqN4FzpnUtrk8u15t7ASdr+
Xd0Lqp0uAXlK3kDqEZc4eVmBKeQjet7aNB3goEEnbu6AxUbeB/8GQbv5aNeQUPOZ
/NPxh0rhtPRGKm7x/LgFw/nCqW7QU2fPQf/6jJE5/CpXUgo0ZuT3HZriSLFoIqfS
3i0ls8MS3WhsaodETFNyLbalwyFvMqS64K1P+yWbCVm/G93ermWj4uoLZ3Jhbx/t
jPs1mKxGBXu8JhUrQ0sBwMv58qTVYyNPKgxssPGohTdGiC9Du3nhEqj5vUVRfGdp
nD2IaQ80/ugsIr3XIsaXU8p8QbORKaWAbmz3B5pt2vGRa361yM/pirNUse6h8Xb8
KC2pHottzkt66qWz3Q+sbRjexeJdL/0qjx82QyPaDAfwT+A+8utjBrSy8rvHwFco
NYCfKhZq6SYnUSmo36p1wZae+CSP+ls+1zN3uPtXEzar81ULsvVYn5Sj6+sgZaoP
w5R0qExM8MFua/aab+kMjIVU6DYcAm4r+E4tv0P1Pf6FKstFSdVDCGVhHkmlpFu7
/lcjcx0lcpMoGLkC0CdDoiScJ0D29jMa08Fc0ifq6PCiJuAHKowqJS2H+VnUwo0
wdwPLiKDim6dSCzAVatzM2/SRB6mso4LjwCzGEuk0ChkbbDinc9+UoG6tV8xdovK
rx0i4ZZfkwiQd7P+cGs/CMdDYk+DYPWJi6w3n4MNVlLMkSTce+C99n/7CEAPU7Po
mizN5Us4y3bQ42pXJMzBPriedEp1EAoTBcw90FZ8qvXuTfkZuyb75roe61m4S7on

```
F/sn4T0YednconxhGorshMLRZ0aDQDwf602+8Nm3qyEY5gLfBe0JjdBnPomLo0rg
nYCi6MLwns0T9QhMQfAR6J0p3fHQ6rMe6ih9su73qqmsIkRrly4nSJL8LwhFdV8d
qPoEMFeKb+tnFmi7S0aT6m0oZREra1iyiwpZPqkha15LvcCDq1zcK3pd6M44hg+H
uk4SZ0aBGRY+WREnsmYDIT3WnS9uKJpMSx6pCwa4hhcmn0sp8xwZK1UEEKzNEc+0
ky+/WoYQ1ajv9vjRsQ8mVP2o3hpjAJg0HcvVn6BsJYS0fZykAZh8tA/MBGBzkmNj
Pm3awY31MM3MVhtFQmQtjIZYzsKKxLWb8k1N6bSs9tKFuZx0+FZSRvjwA6mSg6YK
BNHiZ3W4nf4HSc1EwhgHemDU//n30xAIvX8oSf6Yuxtpj6PZ8e1BVvNYHflesLW
0S3o/nQVSEukU1z1aZUB70lnejzvGC5EEvnTheohRrjHP88R0oz6K7HgsCw2GVS9
XT0XTjwIwmX7Q3rifjVxrju6sdmyTywLlwPWPmHFZbNWZMoaZdr1f2p6HoUJrIkK
Opk9QD34KpaH56pG0qJ3NxcSJF0AttISbfljn2FE7t/N6AXjwOWFKfMzyIMm/iSE
Yp1Jp7HKxw3owdFmB41P2FBHT/eehbfgLozSG/bhVj7pEuaY0XozKDu+00qRxxg+i
UJCfcngZP4nP5D6pG2l13sFM+i37A2tGrG1GescgQk/SgWrnkDm+FZjIG9vLJMG4
/wBjVRqF639bUrc8qrhx/jRPxkgg4Ly7+UW3mwUnr3Erf3p6ZL1//Nd7f5BC8Rcc
YXY3dR+gAMPaFE62akhotTGVQUxcVU76KxI9geFg3e8pMHJ1ycygoM1b9Gt98IvB
59nId0bbv0m4iLuzs3cSsdb0d1S/tWMqcETzrpI0qaqydrbTkwxGGv0/3vAV19+v
lFy9IQ8Z2mUF+S2CgJ9bTzTXh2QqIIugoBYT3TpU1q+Tb19oFH3FBej1J3EKaxW8
s0mKvro8GmNxR2sbhBL1LnZLWs6vAstngAZmPlj1mYcbgNU998+27/+5I1n9IZ6X
/jrQhWtuKg2QgQV0gtraDqz6/LMGKeUidjg2C1IKXo/m87hJWFSj9TMr+/2K20Mr
XReM5ER2YFKsGqCNFKiTk1+T3SPw6qynf3S7lxtxmys8z0u7f/JFILKZarfWRyIE
2qyOWmBfu6/sEuVMGOWLPbhpGevp+SMT8J6187NH1NGO29jmGO9rjh4f0B8ZSmJW
FFnwQm1PalAZCPGxlgVbbERuRZ6tnPTFIBCpE4I/9d/1NbHeKgZRjHk9jsk2Fc7v
QCdped01qwysKfMc0otrromr6mTzEZepedKYuB1TDuZMBTWIQNWf4oGiBZ1Q03z+
VuXgWhgWZJxspGZ8CgYBi9CoTgsu/fkjq0n+rd9Lr1RhoLPR/iVdhtSvHp1u/BYf
OL9a2cqXRFIze+cJfD2Ler8h627aW59SA8g566CSxPVw/Gv02Rk2mm/PCwep6lX
gpWu81riycD6VFUnSCDrw0aqpNfhNOBnx4bNqvGM2msMTJ46BgGv7gMHoUzjracc
tsP5Y8qS17FsxptAmPjP5GpFihHQv3J02XgbaAudskGMAf/bUZf5djDhmZxWqrr
TW+abp6gKjktu1Ug2zY19JYanABpb8/9oYI1AattVoAokUj1Wca02bGqeMRpBtwj
oo5E22qyEkRIhfoHrWLoUg/bt2vEjKAdbe/Xp7zb1Mf6MDksa5/IIMhB1l6y0yV4
JKeRvxji3t7bNaYzTctAcLMQRAoqrp/B97emRVQsX21ALE7puVLeZHTPDscyz7c
hijAssGK+6cb180XGxtM3VSZg3R8tGiETu6nFhTB4ojh7CG+szqAkWKupBPx0Uk0
l5zIkutYJLpFhCbQ4cj6cF1faug6POMcww7iBkqRCU2Y0c4QcQ9z706+t67Sj3oy
g62KUvdvEiA+lm3MSTJASj76mi1hi1rdTNU2pdfT4JIzPAMI6RDN0Jike6Y/Vr7z
wuHcGe8inCjn0+14A5sdgRouC0v5tkId04pRerc3eUixnVvzsXTp1jvbMcCxTHYG
rM1GsyxHiB3j47De343GLJo3JUxt+X8e/Xfs/dwDbTppYa8J67/w74YRRvgGq/A2
/c/lyk/J0kuZcbnKGJa8UsflyXfEhbFDnA6ogWRxBHYTs0s27Du95SvrZwk4GL3j
pW4KkX80gGTY857dMjM80EuxZbVDjhAyBgnC+pq4m4AyfIOzFcXKHSb6e581n0jE
Z07Agv5hPc09phCHyn3pIE9snR0Jwn7v1GaMrv6uv6DDwWix52yNrucgYCi3WRxc
XIw0TYWaGhkFJ/HDHd2gCmVbSsZPTEaU9IXxmvSc0pfC17sUe5baRYR5X4VS50h3
jNpFO5YYLwvN5CAnPRXa6v1KWZzyq34vgQhsHHiJJq40GdyKV00D1WE6ZoyGenxE
rV0yLodGch/JAzig28o0Dwnw4D3IsCbu5hCVQLy6unZsxwWRjMT0onfFrno05tt1
XYq5LHaxkJKF9aBzSi/AcNWao3wEXVYKTT1P2DQcGCmVz+6fsR1AE22e094tULy4
mSAC10R8byELOqs+W4i8GdND86fG+mRQKoR8fYsrOF1CZpLXDFG4AnmiaBF5Ro7C
X20oNKEZ4yhYoiS0Tp/yfW0phJ9iDxfX00RVHSr02Aw=
```

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"

MIITfQYJKoZIhvcNAQcCoIITbjCCE2oCAQExDTALBg1ghkgBZQMEAgEwgmmBgkq
hkiG9w0BBwGggmXBIIJk01JTUUtVmVyc2l1bWVjogMS4wDQpTdWJqZWNoZBZwL1t
ZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtYmFmZlZwXpbmUtbnVnYWN5DQpNZXNzYWdl
```


Page 153

```

9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCq1LqhBwDhdZ5qDTII2PVX1X3K
7/cONxhvBbaU1/k1swdszUtjhflYfZ80RuQ3qFC6vL/PGeWy6SCf58duq/A0EksC
AW1b+MD8QH9Yj7CFsmq1AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAE
EDAOMAAGCmCGSAFlAwIBMAEwHgYDVR0RBBCwFYETWxpY2Vac21pbWUuZXhhbXBs
ZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBSAwHQYDVR00BBYE
FKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYa
ZxxodvRZMA0GCSqGSIb3DQEBAQUAA4IBAQCBSXignLEynBakDKU68ro0RsyXWAPk
fXgQLgy7GrW7SrZeBc5IEcjoN9f/gsoX/Ht9Ii6zyBVjdaox644DsiLOQEP4YMS
7y4q94RFFdmdzEbDLYx9sfUhvdTxDN00oHz53PYDBh4zE4Nar2inC0D+VM6RGDy6
6K9l+D+b18Wj9CyGUc1ppMNURexTg+z3web/eD0du+F2MVtluLihne0Bp1GUTkr0
mJBolG6dSYa18Hw8/ANHpyEx156BJABb744gqoeuD9YSHjKK49+qYC9faFmQ+mK8
0lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXz1Ec2tUpAr4vRhZjVD6FYMIIDzzCC
AregAwIBAgITN0EFee11f0Kpolw69Phqzppq1zANBgkqhkiG9w0BAQ0FAADBVMQ0w
CYDyDQKQEWJRVRGMREwDwYDQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1
IExBTvBTIFJTSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAqFw0xOTExMjAwNjU0
MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsgA1UEChMESUVURjERMA8GA1UECxMI
TEFNUFMgV0cxZzAvBGNVBAmtDKFsaWN1IExvdmVsYWN1MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/pd0/KLpZ
bJOAer0sI7Aja07B1GuMUFJeSTu1amNfCwDcDkY63PQWl+DILs7GxVwXurhYdZla
V5hcUqVackPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TCN012DRVBDpbP4JFD
9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAelqzJOMayCQtwS1q7ktKNBR2wZX5ICjec
F1YJfHX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR+peCrhJZwLSe
wbWXLJe3VMvbnvQjoBMpEYlaJBUIKK01zQ1Pq90njlsJL0wIDAQABo4GvMIGsMAwG
A1UdEwEB/wQCAAwFwYDVR0gBBawDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWB
E2FsaWN1QHNtaW11LmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQwDgYDVR0P
AQH/BAQDAgBAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAfBgNVHSME
GDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAc4mi
NqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJ0d64roAKHAp+c28
4VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27PmhKE1oAJKKh
DbdbEcZXL2+x1V+duGymWtaD01DZukKYr7agyHahixRn/C9cy31wbqNsy9x0fjP
Qg6+DqatiQpMz9EiaE6aCHHBh0iPU7IPkazgPYgkLD59fk4PGHnYxs1Fhd06zZk9
E8zwlc1ALgZa/iSbczisqcn3qGehD2s16jMhwFXLJtBiN+uCDgNG/D0qyTbY4fg
KieUHX/tHuzUzZxJjGCAgAwggH8AgEBMgwVtENMASGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxMTAvBGNVBAmtKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlm
aWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJc0vT4as6aqdcwCwYJYIZIAWUD
BAIBoGkwGAYJKoZIhvcNAQkDMQsGCsGSIb3DQEHAQAcBgkqhkiG9w0BCQUxDxcN
MjEwMjIwMTcxMDAyWjAvBGNkqhkiG9w0BCQQUxIgQgFPMlhnhgVYfwoQAWNtNbXfp6
/cWw0vajQ0bfIM2N1+0wDQYJKoZIhvcNAQEBBQAEggEADBKP01AhmQvuL9r8u9eh
4V7q50gjztXHMfW2kcpXNAEoy6iQ9LeHjSXSmVNIIsNyD340fqIWUOztwba/xC
+qOC/4GwaG4nvqCmyT2FN19X+2XHgaLtlgUSE5JhYifHm2cfFGH4Y0bujre1NS+
tZubVHdqf/Stlr1vFhpBYcsu0ZInwbeVbUJBMd2iqG5sE702eQpMPeSdh4C1CB8
W+1n0eMlPiea/V2SZC3WCTpErF71lbYdc6jLAws0eT8t1J+DhfgBccPpbsCw2n1W
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-Outter: Subject: [...]
HP-Outter: Message-ID:
    <smime-signed-enc-complex-hp-baseline-legacy@example>
HP-Outter: From: Alice <alice@smime.example>
HP-Outter: To: Bob <bob@smime.example>
HP-Outter: Date: Sat, 20 Feb 2021 12:10:02 -0500
HP-Outter: 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

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCTkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRUErkJggg==

--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
BAoTBElFVEYxETAPBgNVBAsTCExBTBtIFdHMTUwLWYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIEU1cnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAEYCnMa5cAMG1Fedd4M7eVuZRV3TQ1Swv6zq
HizrFLVHcw2IQIXHK5qbN2Gei2g4nukYK9jX/nlflZcKwB2iyG3737Ga9ioiW3WG
9tJdD7gCDmqmuXW7u0fY2Y2czyJfxwygJ9rcYVF9J6bdq5yXxiuPCpIQEYZY2d60
HZKvDTHpCbDksSrj7YHAc7vzWFSGDvJ3qZ0Pax0782/oPI4e0I7IhpSjyi0kSjyw
```

4ibrBeMXcSokx6wn80hdJK3gb2txJiBAIKCQ4cdTTsni5kYZ1eU+si0eXLLADGoQ
g1dcw0Lcniv/iElqQEEiQitEjrgcMOGa+7NfUt8p12q13/SgyGgwgGGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGhmaWNhdG1vbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAdhLP26FYAU8560yDWy0tAg0k
r9TR3H8R9QxKI604FXSK3bm0Xqq7mWT58NTkquiB4ZEycB+eC44YS3CpPq0oUxlv
K01x9vjGq8ksFQwaZ+CRL1K+pJWP0kcfLd2m3vYbj5arKGNdJe+cqxxoX+GXJ1Y3
7TUyptqU7VRj/oe7Ifawjm0Ro8PUtctfFmNNTrd+ohS01RTw+cZmu80S4SDEVQZf
mgLFHTVqj0BfTGUDQa917N04GYBRXSYUVL3oNjBBRRS3aWTRZYUW9lp8XR13LJQ
berrHomKqkY1aLbn6m6bY9/RkyACqmcSar5HuinbuNS+v7WNUQKEfgWPDDdiNTCC
GX4GCSqGSib3DQEHATAdBg1ghkgBZQMEAAIEEDkYoCBUV2kALKjvqgmyJIEAghlQ
4G3n7gBTsLWMTbnseEYMFqoVDK2AtaC6iq1AEi7qVHvCueAQZmiFDD39N13w6+W
MnMkUG9BSN3Bpt99HaHITGsfnzKD+Cv17da/1WfWPIDI8yClA20zUK0TdyBUvrBz
wZKRCMrfzGQEGzcsjzHTP7aHezlCKU7aNC3GIvY6V+y70YARPAD+xlsdNEBLd0/r
iZCtXce5RaK2DBQxu4w0CHIWHGBx5w12iR7uPHi+dXyhRYb4PKh/8uxBo0WzBYmt
kNdkiYicNeK1u7lHFCzD8S5I1/wB9jAJK4BnzKz0Z5aISDtrsIe0v4khtJB54KVf9
Ho829bIUyUPX77MWyoR8ce/+HD0xXxrorm6f9qIk4chBTC2m1AVDtTiRvPWG4eCA
NQfg47pEwgz3cVeGCHExyGwVV13Bs0Z3azeh2IXM26oq0CrxeEmYcuK5Kletg8e+
iNecpmOUBcNtBB3ivdG1kUv1SeBmF3NikDup3G751FMuCUUUmMT0ofzMA1pcKMq
jPaQmzydKZhe2UrhYtr6Xzqxnj+WBli2iLX3VDBaQHWCUI6NgB5P3vS+3/qRUc7E
1PjQ1jzwwfMNCZQQBgRzfAdqMCAJEggaWj0VNrQ208pRecynNqavlp05pn4K2Jjr
nIV4xm1lWypRkAT2c1+Vow+DeN+HImKhZPN/kRQvs6iRx00uZ0uTe6wE+F4LoyV
REg0041JQeUnATzXIyHz/QENOnmkMa+k80QYI+FihUkFIOLzvQw3CBG4vm03sei3
mxCb0Ciy6GCVMXxk3BzeaUMifd8YeAfw09aNHnVsZ5oEzTEfIGUuVt8P3UA+83j/
VXyogQznyhlvnu81J2cj8k0qfH+yyIqAqEDjx1a3toNRcutfdCGURuIGbbF6p715
rWE3rgPOYvyDGkRx6CdvncUG/kiOX3XSP/e1R6QU08+NR9ZfgMwBhmfnBgD24RGW
ucLTRAkwD5tQrPxp0KnKrdQ5qTcFWeyirBtYzI/cDsONkmt55fL/efSdVsUZZ6W
oTh195axTi0rW+EeZkk0hYFFWGaPV1ZhJbyzYgFHjumL1SMB2dENEo1XtjHwlggM
+RhIMxfTcWr5bk34VxtbGcCszTGPJpUZh+1SiVVoIeyVN7YQ+VT2JsgDd2oik1
Z5YZ/pS7z1oIDas2cggRuAHyz3WUT9heB5+fjx1Uw14K4iFRq+RBwFulCOqCBgx
YUnEwj2C4c62ql0S7kfLQU95Z/q265wbf1sY1+ZHwdYby4UPcvcqXgGCwSGZTJvD
xMHXmfkKB596UALXefx1qb5td1Jdss18fXMwCrmBb40/Xxc0zoa8eeNs7urHP7jY
fNLEjpyAD/soGAdJcxP6o1IqItjXtZqPCRnRE1QsqU3RaLQngI+B1QSM81JjsQx9
qZMVznL+ROEUbAAdVR83oDpbA9qi9Xq07QL0coUekYLDND0Pup+zPgjQ39fDtJLA
+loFvZGrTUhTQ190n1d4ZrdJziTwBw/131VuFjvBfVbYeGhdsVyQgxP1MH1GiBA2
DdHcD3EE0MRoiqgV9rqwspp4ar20q0c/kVvh3VcA6fTASYL/d5254WWnxq9sc2HR
0GH79c/4fdjmEPvE5iwc3USMWSv02/2d0jNurBWDPRqHIkSSVSnf9xkrFWFY2p7U
DTSzkQOKQ/3mG06ke2nV33tna4EnVB8tZaL0bcoUxWgtclKcXcmfthikU8M4tbay
RA9bzhse0/VWhtkTDeoQvifls/IkdYm1RCHRcc3wDCi5VVaX9B0pCDKaFxfatb40
RTBfSYSoeFaUkhtjPBEOZUPuE6qXWGMvS4tbTuqGK7u8WAKVC711c3zqisz2p7Vs
qBJxqnIZRFbJuxRu01IoQPEUPsNjgTq0AtWzWcFQwG6hJ9CBR4uQRVmr1bRJsik3
jSvcVjbLeTTINDxRRvtPa9preDrr494Nykt7+5D2qhGh+CiAQME9P+Wbf0fwhotn
M/1X/GGPmT5XZA27ia10J3+/MRLqP1m3dR5VXDRZBtXqxPiB72aP6TsXLcSdlky+
n3mmEB4ap1Uu+F9ZKDgDXImp3cFSqqMkk0KNKi/J0omabZfX0nAx/vY0tjjS16K
KJc/j7/bo5q75WaiRUzVbFc8RmnDCVF0ceICrATgHAtsbDBD1BM2SC72w63Ic6rg
TNy4wecyaQeyP5qJFeMLENGA73a2xPCFh4Xg3RgyxLR3xUJ+1NJ07iE8EF7T2peH
AzL6+3ZAFkG0Q9uoxr748cs9p5s8r3RAaaFAjk8ZVrn2mljrOqMatAfIQ9TY7+Vh
AMPfa4PFLcm1bH1IeRD4g0jdJ4ozJLDHrb/xAyW+IIwlm7W7AirdNldCw8B7rdmy
NbiYt1Ed99MsmK0K1fpYmke0i4BVsfFGaj90uAynIBl0yUaSQ28419ejaTU1Q+YJ
FeJjDZ1o1WBbFb6j1LuZ9k3vDye55ZphlykGo31f1LtSmZ8daBHp64h2f+Bry1Rv
cHdszK1TwhBg2TCVM9+MJ4jplf/ls8pSVtoHZQUVJkm1T71m/tA6CPSRvCjjtuR6
3YwTH0vx6NfQr0vr7LSaG0sSBUGTgMepBja2uh6qR2QkJaCQgFeUFEjDtPzkQ9k4
UZTm0u4g+FW61XN6T/BFC7euKLXzhI6htv1foYwC0SE00+wz3vRYXVmsY0otVHSe
iK7TA/oUSyu+dAdBShFimJ295RZIALW3nMx2H/f6amg+n8NA9uEn33er74g+JRbA
OE78tRz/190+ub4v01spkb3osm1Wf5TKVFKpCbQpTEac422pjpBe04iekCkW+qJB
v1s2kd45S9Fke+s5o6d+lapwL4finUN0iga6yh70vjm217MxGtS1D6ZnsLPFgb7Y
uSUMeNJ5UvSwrM/u0ReWmZUX7pETCt28U+3dqnR44VYJ15M2CpWgB2IxoLph0D8G
exKvxXFYpF3xS8w7cmHpYsBkiaAWMFqYop+huEdQLNtFT4QfVL0txVkJKZXs781

0ylhG9Zl25+c/mwJj7+i500Qz5Idl3yeqrtTbk0P40l09Q274ZlkeonxfWcI4qeQ
Zc8vswWpCbyHneoYrhMREex002ikGYuK0fYhGfySTaYbQPDx6+a1trboUmXoCIth
13vbZ3KD/2JMKvctah/2Cb/2ZeQimCrvYtehTlJiwl0qkS3AcSTHlp/5juh3oxVn
eQpFKY03chZ9s6xd6Nsae71rpZ24o1pkZtAbrEC78ao0gmULuxvXgzl1984Kc1C
aTYoSbk+ay0E0RUgrvEwJEWf6MP1wRlCxl1b9r+GBjtogYvJrLFJ70ZDpkigkLKyd
nWrztRgvfWpn5S77S/ZFPUK8Ija8G8zBd0z61Bhb15tLB0TedDiC5NMVUGAVknH1
R5PtQE2NkVe/kfvn7w/Vy7AnyDIkepsI4rZUIbXqkId8xUKq1Y+r6BgaSqtztXu0
aUnr5qKU2K9F6/2AM9mZPo0VhBJU5qWiMZeew53vKGvrxCd7PodPWg0CKOMP4f9X
fB1+HlsKkd0gcMMiiazq/xoG00ThczQhpARNXaMDxzZmr09K4+tG5NxVV1F7INfZ
ADFunqox8hpk2HW2sas/8wQ3FqoGU774go1g7ldkBed2v0ETee211rXDyf7DIiTH
g1/Ty20q+qc33dR8fVgLRB4wZbuKiwb7mv0aUDXQCHxMK26w9uS/70mQGo0TJs+R
jxGhy7sL20fn8L1CLLRm/RKcc1EPIWR2pFi/dvbUHLcYcqt16EAwtUSXXXJ3q7NH
si4VPnVxjF6b/iKaBuWsXzGmSfws5PmriK3JfXK9N8SippZwwdhqGX3JavUoFH6F
swEWrsWTGnalU619B1/yYTrlB3+XDFtkGuBULENI/BJoXPA50BZpkv0F6d2Q2CRY
aUFGIFthgqnMLJJYozxmb1kM6f2teCwgw1zD1Hs6emQ5Bf6eB0iNnvFHYA/wT2c6
yBoXiGjJ9H0rxuKGpoD6LekD2dAzSzZVkla5IwnzfCd8Nby2260LJP4TAxZvkVne
1cK+/Hsa9fNvR9rh4VprQpKTcqlH7TXAy9HayqCpeggbMbxRbXGsxcG/szMjKHof
qjrfU17kXdo5hp4LowHlpl0+4FsSYXv1/zFRNFUSj/EyTrfwPGcC2WPY8JaPLYxM
KUjeKK1vH3PQ0QDgeU/0GoCTwekBa2mwfwGtQfmNPep/usTiWN5K5ymeeLbgwbE
JNtN+QqZynBqUAuVBv8J0yHv8SzcGEWLK0WEK3zQUrj79lQ62p5sFSd5fWp0v4tg
e9n65e901yyu/olkHEW+yc4SKz/V42knHifYIFVGsQ9GjQ26m578QAn4wtylNKWf
4m7bg8jLP87k0eDB5Lkr+bzfI09UdYYE2sS0/Cn/WCeU0UNA0sDRB0tGA2bJVDcW
5GhHt/qR70z0c/h5HR7JIY/JR2ekN43juTCsPypLFZthgUbHTxWj9H9/3rQnfnix
lIoolIDXTi/MotzcZwFqMVyQhZd9jgH0Y4d0lET77rpGHJv69UmjwHYqfoeiDdz7
OWHXTCDelVKT6IFlqxjpfrh/EUWjBUE1/Dzx4/ZQIoLie0YvqMaELjjedwOpEoIx
hcK1rsvBDiU7XR9VTvA7VTI1egqmcu1yeBON/d+MlPtylFYRZtw9m7837EMPuAwD
JawBJdw1M8DaznEiLm8K1PKH0MqQHjXnXSgQz9BjX6JBaQZYEMyaH3XtS0LMN/As
Ga1DIS5VMxCFPNkP3IJKEx9+JeQpUKA06uYxcHIQEAiR171wJ55JbxJnQef0klSN
xFNZbJ8HrMp7ebfsezsX0qL86HpmAqamzJb1XjpBWdujx7FhaTG5JJ0vfDWWAIEo
2L1JJxn4PlvwHQ8aCFDfdhtSGUm0ht3dAdcdxvKSBXtn51b6vr8Jk4GEX7Qt4MZN
Q6ioS/i77KNf1KUcGsH7Vs7g8L+d5Gix9yuGln39tUF6NvdKeCpeLIJR0wq7BiD5
FViBa/K4dymxQl+3zXcgvCZ4f07LOHMTkw0NtyXKxmx3/NgOgsXEE5o0ynFp36w0
/bfa4t0gHQF/t0XjF9QwNYNcL9Zl/ih440TuE10sIAiWGP/dUYVfHGtx7iri7ZwB
eOWV8An9oy6w3U/6d5gZhWOLU1tL8h2LiXqFOLFMMT9F+3ozCyxEFSIg+8lrmUqG
D6Y0XX7Fzb29bsaSqYazBAHJw5XWgqFSI/tnbR3ciitWNGj1bBUzjzRzoUKumW/o
Zt3MvbdTfwwM+lzRQyYoNZi8or/qQWls1pF4GndTUKDROJv0zylP3b59Eo3tLUPm
IH9f2dX3XnDCncAf1zmtYxy+dIJc02FD6Jzz8E9G2bMNR/6zB9u1r+pYDAjJnmi+
V1W7vfw5jPFT1xWKype4RiYXa6uSV0w19QvEz1GNnwXec1P7ZDALQ36v1v7pmDSm
OlDaIZQdbCONLwWjZnLMB670R0r6AbiTN1k/CgLGtJ+GQ8TsmZ/eAKPo00miDKaH
ggRpeofpL0Sk69vJtgXYkaWh1YdaadHW1t6SWMy2CR2HHIZ9g7jxDKOC5l9pDlo
FP1CRmJe3ZcCWFUYrabiEJtyL9NCw+jcjBejA2sM/CWEEKx/dEOwZFCu51U92dgz
jGoHP1piMqHAQYL2xt3xbZfc1Z/093Wv2huB2/eu8J3bk1+BSLENr63NUwK+PbK6
tcCF5jtrDsLowOnAYeXdj0EnxaV9LwequsKiVJxfik2H1QGed7MRYC8Tx4aCrqx5
pdMNM78438mie5/PgRpQ8AJJ78A4AWHa00Xbg/sWUXF1bBgSj+mcdyAEmbJUz0zM
v++vJw33nNmm2hoUfgfQ8SvPT5LizVnzzuN/Xd36+I1W0dsWVMBwgTH9m0IRGKI
K4Ddx1AlntqZCCeFetwP1Jpec3X7HW9GVUTIjMel3TbC0gNt/qmd6GxKHZGfN0v+
iqm9icPZjHfoWkh2NXbHEA1qjiiXl9bmYdKBX7pBr1ukr6sEc0nknQiU1aCFzbD0
Z92j40Q5ZGAFZqFieHXGRR5t10QXeA9r1xdnKocsC8mAnXRzLIyqgW1y0IxoGZ9A
wMXTSsG97A+JvqZY0jQFqFNJNEpIkmyMbEIwktu+XuUJ7X4Z3trCc2AzdPsBh/s
w70m7dm8++WmQXYfWRxey67fQCRte80QFuh0zBksVeEdisdWcAtoft3pX/Qwr4vf
/M7HR+av5lUvDsNtXA2tjK/SFfHN4Vkfz+jyuzb/U8zAM+WixSAachsLIDxYVCaJ
q9E/OU8XbdOUDIh1GxA1NcktIaDrYdGwTYb5rQEmekzbjk6Fm6lCW4IlefBKd5dR
GUx64ootY21qqxJCUiffYQtLbi/tZVbIJpsLH8zn50oRNMkkwGNprkNQpOM3NaQ1
+HlICbPpPHv6FyglYU26SaBt8fCsBSIVGSKmv0MRVHuIeuavoqhj/K1z2avC7R72
5PaUJMitj+8fE6iAvKxV6vqh3EqKcF4570J77pp0j71PR3D8VQkn93qkLFWLJIgN
Z9DGCn1WfCRLaG3MjKait9PikUosTeA3XSA4tdDyF/AaaDUSfbqseFQuOW151z8h
EhiR1wM1wcRkanCGxpJdYW3wfcv3nNma2Ehzw1fxoBXqrUKbtY+/3LjUAY3DmeF
3YjyunYL5Ij+6Jvvs1vDnmleE5DRsU0QsygfyjuwmdsJZ3JXUD2fRaZJLNqc1s4im6

```
R++Mh1jrmRrazBsgTWanqdxPLwRAq9V3JyJxjU/wAirCX5pCAXzAHiiFhdJnlliD
21SPK2RPbrJ/G64KMLAWK8r4SfbmfiiFOCJH+8F/YLiKB2W1oHNdaF4MagvgKzIy
bYdy85kUGGaRy6IhCgp4gqd80f4N3YHQhhQk14/vYHEzaaBZMTU5TU+q7jzSDH0w
T2UoXj05w1JgZy6UYCA0zN1wY0M890YU7pUXacjNaXUEhajY2zSHIKZva/1TW1Ug
1111xYHLqZ/93d68Jb75nszdbLcwnHtyUuMtiQVSVyXzIYgmTjjRZ8WLeS1rIku/
a3y1HLT+3m38318p8S5HKWAEehz1zhxN70y/A/sFYZ/iQyDkBiv0oyHTkM2596uC
GdrrSfrGw0aFGyi5Zk3QxKwhunul/0rZcrFu9VPYr5UrBcB3TQC2hCc0MyfLaDxB
Lo3JaKr1K7dfeBoyAXKSSv6K7eUYpWP0GBEmmLeb3xHMEQInpwYBuDgFX4d0zNck
wYUOUkJHh6TJeX+FynigAs91Ai1sNgwKVEQ7MZKv12MPfScL2IXs238oDx009zAH
zXNjf4iLH7fYj8k97/8CLLFncbdoGKaR1yItKcxjTxSkXtimZk5uY6yQqnyV7mf6
JHKCQ6Nvgq8NWAVU0kLeRrifiRHy1AjFMpp7o/AuWy5mvx92LhYB+uWfRhoBZWee
fmw4xcQCe5+Sp+Z3XP5r4c+h5rXXaGdmXFNb72e0EY7A0abo9gi1Vj4LgJPLg7L7
qDYpcz8FCeSgIQ6iSttk6Lhg0AZ2cv7fcMWQc03cjTU8HgRET4doy2AznzP9G3a4
jYKuQoElzfjYycYR06qCoyCCw0IF2Lfmwxf3XUbiMjEwvI0iik/epN6iz03mxMx
Zf4MmRMe6p+Xa1lW3R3AozDJuUWw1GoQ/tokMN/HNK8sE3v8Jf39xQAf6uTA6qAt
Y5BpK1lXCRYg0YLUiHBRz0zSkBA94GGK687z6PSDV1kY/pqGFhThTcR0h1lbbv0
eOT+9xqi9WckQqEVPk1D76g8x2xNw+AYObCjvPYNCfK4q0RAKm7Js70FhpJS9px
Ns2vGaZ7y3w6f7AFa3KSbyiYmbW3nj8g9Ew0yNEDM/3C/mGEQWfYk8Ay3QH/TynW
ogsx3K1kn1+LY4WpaUiZjYVXKNNVE8+eiyykZ06P+fc0TZak42ARy02+q6H/yXoV
s6C+H4xPHdq2WE7z0BrC4dmL5ihnQ3tPhfU2gU7+sYI4q0uUpuVN0s2yHwMbAeC
TctqNj7ZEDdz/D7uYhdJFEbBYxi86pBCWt0CuaEckRQuqgy6lYGcyoFkxJMhEDKL
hj3I9t3dqwaIWTKit0dE8AL89Vc1GSu6SDPQKRhJ6h1DPtXhIrh1uF35C9uwKNUI
01JDhzbX7yJIVdF7FI2sKcJWb/OARZ5sm9F5s0n8c0+ZVBvOpA2m5j0BA8mP+Jt
XcGg7SerRK6wxxkyFyF0DMcyrHs++Gr+8lY+RrPCbZYDW0sCib4nqqb70htn2bcg
C4E0+40JuW4MPLrxtIjMkQPjmynj9REM6qkJw0veYbEtJyaIaaHo/ZJ7mCaTP0xD
2ha5HLtyw458elqQEDy/JcMiS35az5arnYr1jF1ceqGyuaKYwwlKwB9+Mr9gzvKA
fqwNhON1LL0u/RjnmvVoahWqTreTg61TEYxx3K9uf166QFkIP0lQP7sHjQy5ksd3
xPEgMKw15xgyB+k7QuZoQi8QMjMxnmI1ecc7itv09yG8YKAikI8700hVtNwYkSat
xPc2w/eJlU2EiVYo5V2c35zQag0jZ/1qSkX0ZU1hPif15V7LD8hr1wpJMJkrk+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"
```

```
MIISAAYJKoZIhvcNAQcCoIIR8TCCEe0CAQExDTALBg1ghkgBZQMEAgEwgggpbGkq
hkiG9w0BBwGggggaBIIIFk1JTUUtVmVyc2lwbjogMS4wDQpTdWJqZWNo0iBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtc2h5DQpNZXNzYWdl1LUL1E0iA8c21pbWUt
c2lbnmVklWVUyY1jb21wbGV4LWhwLXNoeUBleGFtcGxlPg0KRnJvbTogQWxpY2Ug
PGFsaWNlQHNtaW1lLmV4YW1wbGU+DQpUbzogQm9iIDxib2JAc21pbWUuZXhhbXBs
ZT4NCKRhduGU6IFNhdCwgMjAgRmViIDwMjEgMTI6MTI6MDIgLTAtMDANC1VzZXIt
QWdlbnQ6IFNhbXBsZSBNUUEgVmVyc2lwbjAeLjANCkhQLU91dGVyOiBTdWJqZWNo
0iBbLi4uXQ0KSFAAtT3V0ZXI6IE1lc3NhZ2UuSUQ6IDxzbnWltZS1zaWduZWQtZW5j
LWNvbXBsZXgtahAtc2h5QGV4YW1wbGU+DQpIUC1PdXRlcjogRnJvbTogYWxpY2Vh
c21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IFRv0iBib2JAc21pbWUuZXhhbXBsZQ0K
SFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDwMjEgMTc6MTI6MDIgKzAwMDAN
CkhQLU91dGVyOiBVc2VyaW1wbGUuTVVBIWZlcnNpb24gMS4wDQpD
b250ZW50LVR5cGU6IG11bHRpcGFydC9taXh1ZDsgYm91bmRhcnk9ImViNCI7IGhw
PSJjaXB0ZXIiIDQoNCi0tZWl0DQpNSU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1U
eXB10iBTdWx0aXBhcnQvYWx0ZXJuYXRpdMU7IGJvdW5kYXJ5PSJhYWIiIDQoNCi0t
YWFidQpDb250ZW50LVR5cGU6IHRleHQuGxhaW47IGN0YXJzZXQ9InVzLWFzY2l1p
```

Ig0KTU1NRS1WZXJzaW9uOiAxLjANCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6
IDdiaXQNCg0KVghpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1o
cC1zaHkNCm1lc3NhZ2UuDQoNC1RoaxMgaXMGYSBzaWduZWQtYW5kLWVuY3J5cHRl
ZCBTl01JTUuGbwVWzc2FnZSB1c2luZyBQS0NTIzcnNCmVudmVsb3B1ZERhdGEgYXJv
dW5kIHNPZ25lZERhdGEuICBUaGUcGF5bG9hZCBpcyBhdDQptdWx0aXBhcnQvYWx0
ZXJuYXRpdmgUgbWVzc2FnZSB3aXRoIGFuIGlubGluZSBpbWFnZS9wbmcNCmF0dGFj
aG1lbnQuIEl0IHVzZXMGdGhlIEhlYWRLciBQcm90ZWNoaW9uIHNaGvZSBmcm9t
IFJGQyA5Nzg4DQp3aXRoIHRoZSBgaGNwX3NoeWAgSGVhZGVyIENvbmZpZGVudG1h
bG10eSBQb2xpY3kuDQoNCi0tIA0KQWxpY2UNCmFsaWNlQHNTaW1lLmV4YW1wbGUN
Ci0tYWFidQpDb250ZW50LVR5cGU6IHRleHQvaHRtbDsgY2hhcnNldD0idXMtYXNj
aWkiDQpNSU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGlu
ZzogN2JpdA0KDQo8aHRtbD48aGVhZD48dG10bGU+PC90aXRsZT48L2hlYWQ+PGJv
ZHK+DQo8cD5UaGlzIGlzIHROZQ0KPGI+c21pbWUtc2lnbmVklWVuYy1jb21wbGV4
LWhwLXNoeTwwYj4NCm1lc3NhZ2UuPC9wPg0KPHA+VGhpcyBpcyBhIHNPZ25lZC1h
bmQtZW5jcnldGvKIFMvTU1NRSBtZXNZYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxv
cGVKRGF0YSBhcm91bmQgc2lnbmVkrGF0YS4gIFRoZSBwYXlsb2FkIGlzIGENCm11
bHRpcGFydC9hbHRlcm5hdG12ZSBtZXNZYWdlIHdpdGggYW4gaW5saW5lIGltYWdl
L3BuZw0KYXR0YWNobWVudC4gSXQgdXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24g
c2NoZW1lIGZyb20gUkZDIk30DgNCndpdGggdGhlIGBoY3Bfc2h5YCBIZWFkZXIga
Q29uZmlkZW50aWFSaXR5IFBvbG1jeS48L3A+DQo8cD48dHQ+LS0gPGJyLz5BbG1j
ZTxici8+YWxpY2VAc21pbWUuZXhhbXBsZTwvdHQ+PC9wPjwvYm9keT48L2h0bWw+
DQotLWFhYi0tDQoNCi0tZWI0DQpDb250ZW50LVR5cGU6IGltYWdlL3BuZw0KQ29u
dGVudC1UcmFuc2Zlci1FbmNvZGluZzogYmFzZTY0DQpDb250ZW50LURpc3Bvc2l0
aW9uOiBpbmxbpmbUNCg0KaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FBQUJRQUFBQVVD
QV1BQUFDtmLSME5BQUFBY0VsRVFWUjQydVZUT3hiQQ0KTUFnUzcwZ05PM1RwUncy
MGRxcGJmQVJRRWpPeXdpd1luQ3RrRetuYmNMazY2c3FsvCt6dD1jaWRrRSs2S3dr
Wg0Kc2dyemZjcVZNcEwyam8wNDQ3Z1lEcGVBCmsrT25KSGtJaEFmVFBsaWNpaEFm
NVlKcnc3dmp2MFpXUlDNL3VsaQ0KdmRQZjFRWjJrREQ5eHBwZDh3QUFBQUJKU1U1
RXJrSmdnZz09DQoNCi0tZWI0LS0NCqCCB6YwggPPMIICt6ADAgECAhMPLSW9ETmX
Ss5CVIEh7j00Boq0MA0GCSqGSiB3DQEBDQUAMFUXDTALBgNVBAoTBElFVEYxETAP
BgNVBAsTCExBTBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUFMgU1NBIElcnRpb
Zm1jYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1
NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUGA1UE
AxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSiB3DQEBQUAA4IBDwAwggEKAoIB
AQCaLSn6i8Gi44/oAVAn5Gnck4PHHNjrSfWUnnelN41KImVaTC3D9zFCrS3i4Pa9
ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs165ernT905NL
Ff1HUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCRZuTtMc1zy++MxQ
lqdn9WZLh0A0peNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCq1LqhBwDhdZ5qDTII2PVX
1X3K7/cONxhvBbaU1/k1swdszUtjhflYFZ80RuQ3qFC6vL/PGewy6Scf58duq/AO
EksCAW1b+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNV
HSAEEDAOMAAGCmCGSAFlAwIBMAEwHgYDVRORBBCwFYETYWxpY2VAc21pbWUuZXhh
bXBsZTATBgNVHSEDDAKBggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBSAwHQYDVR00
BBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEwjnwHFwYn8Qko
ZTYaZxxodvRZMA0GCSqGSiB3DQEBDQUAA4IBAQCBSXignLEynBakDKU68ro0RsyX
WAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gs0x/Ht9Ii6zyBVjdaox644DsIL0QEP
4YMS7y4q94RFFdmdzEbDLYx9sfUhdvTxDN00oHz53PYDBh4ze4Nar2inC0D+VM6R
GDy66K9l+D+b18Wj9CyGUc1ppMNURexTg+z3web/eD0du+F2MVtlulihne0Bp1GU
Tkr0mJBo1g6dSYal8Hw8/ANHpyEx156BJABb744gqoeuD9YSHjKK49+qYC9faFmQ
+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXz1Ec2tUpAr4vRhZjVD6FYMIID
zzCCAreAwIBAgITN0EFee11f0Kpo1w69Phqzrpq1zANBgkqhkiG9w0BAQ0FADBV
MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMC8GA1UEAxMoU2Ft
cGxleExBTBTIFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTA9Fw0xOTExMjAw
NjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsgA1UEChMESUVURjERMA8GA1UE
CxMITEFNUFMgV0cxZzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/pd0/
KLpZbJOAER0sI7Aja07B1GuMUFJeStulamNfCwDcDkY63PQW1+DILs7GxVwXurhY
dZ1aV5hcUqVackPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TCNO12DRVBDpbP
4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQts1q7ktkNBR2wZX5I


```
CjecF1YJfHx4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR+peCrhJZ
wLSewbWXLJe3VMvbnVQjoBMpEY1aJBUIKk01zQ1Pq90nj1sJL0wIDAQABo4GvMIGs
MAwGA1UdEwEB/wQCAAwFwYDVR0gBBBAdjAMBggpghkgBZQMCATABMB4GA1UdEQQX
MBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQwDgYD
VR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAfBgNV
HSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAA0CAQEA
c4miNqf0QaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJ0d64roAKHAp
+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27PmhKE1oA
JKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahIXRn/C9cy31wbqNsy9x
0fjPQg6+DqatiQpMz9EIAe6aCHHBh0iPU7IPkazgPYgkLD59fk4PGHnYxs1Fhd06
zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+uCDgNG/D0qyTb
Y4fgKieUHX/tHuzUssZxJjGCAgAwggH8AgEBMGwwVTENMAsGA1UEChMESUVURjER
MA8GA1UECzMITEFNUFmgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2Vy
dGlmaWNhdGlvb1BDbXRob3JpdHkCEzdBBXntdX9CqaJc0vT4as6aqdcwCwYJYIZI
AWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCsQGSIB3DQEHATAcBgkqhkiG9w0BCQUx
DxcNMjEwMTcxMjAyWjAvBgkqhkiG9w0BCQQXIgQg//G1y8IBZR2ZHaxvjng5
wsDzqScPzmGqfXdsuHb7bBYwDQYJKoZIhvcNAQEBBQAEggEAgNAXRpWDJX8taLEv
apU0ax4C3CeJQgG2loke7SrgSqmJrNeCSuu80jF0xNY9YGiz8jUK0fk5lBii08p8
bq5MpX8NraGtWaL79iK++2nZ4D0D4C4VXYi6lVEio8cvChUS/HURa8ehtm0xwHFK
q0+Qw50A0LvYNNu62oThBLdJzfbirx1QL+q5/xLndvEZkz1ljmiATIEtJ1vvsEdG
0vXeLi0Ppa8M50V0VpzK6DQ2Ay7Gu2ebfq99jLY22Cfe3GHab/WrUeJZ7mFmaqBG
WM5HN/Dt0sBA0zgDBSymieKaXbzFfAzNcgm441x1PMWCWH1ceqgzrq20KHTts6yv
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

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAYAAACNiR0NAAAcELEQVR42uVT0xbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCTkDKnbcLk66sq1T+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

MIIfjAYJKoZIhvcNAQcDoIIffTCCH3kCAQAxggMQMIIBhAIBADBsmFUxDALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTBtIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFGU1NBIElcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAEBXJpGH08AJVfwKb9Juhai3fwEaeyt576LQ
wqs5p3GhRIBPkKrkj0mtlZb046v11BvR6FkXzBpMTkD+atU1AgwCR6v904kwV/J
8Lab/rxrhuyIYWXtip9z1gJZLq+2YVW5VwafpPyn1rP8Bv7nzzW8J6ewu3RWRs1g
XdALRLUG2vgMLUGld8Ztvztz4idD1ixj3Gebv2Yw0cPPNxT8jLe+L0XvNtRqAdHs
f7PtLnorVWLwiZmTj5lFBy8sEUxCgY/Z0tj12iVgudsxiaMecZwN2GWe469I4p0F
uEqpK0wOkiosPbeCFrFYy0go01v8myLHEHy990TiEQNn68tY2qcwggGEAgEAMGww
VTENMAsgA1UEChMESUVURjERMA8GA1UECXMITEFNUFGV0cxMTAvBgNVBAMTKFNh
bXBzZSBMQU1UyYBSU0EgQ2VydGlmawNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAoHffD4M7tWWdVj25qIu8/aMz
Gpu5MIU0I2Sz/64A0TmvrQRU4RXMR4SYBqaGiCrL/03Y8EMFnLvUNP/6fE7EQBS0
fu/bsALlL+eLVQv9HdN/2SxCxzC6GHlXCw0fwCk+QgzVcbbct3ZLkeP40ILmTQoB
ar3ZQEGRO976398AdChG9t+8t1GPAWER9QWnoS3IBZQtqLiHzZAWobHgYz+iKSf
5qfCdByCZ4jyJooEOeFTVWSHFy0ZhdnRF1JQU0X7Q1hG2Np75WDG4N+A6kEuKrr2
SK/4va7JtDE9hWCdM0f9ZSRrMss0tpGromCo0WleWujL9XIW3jvuEkyInx+CYDCC
HF4GCSqGSIb3DQEHAQAdBgglghkgBZQMEAAQIEEDR63F3Ex9ZJaQBncRdFmSCAghww
DyQUVU20xy7BDRXBlsAlBK363lgVpACqFnCDi+oR9dHUUqJ8zs09AhjeR0I/RxNo
YVx0Jy4sWw7QpFWQ+qy0tHpjfgTmr+qcMsmxxkTihbD+vn2dWMKjb07wchVOuN97
6WTJcoKz6f8WRc+2skkXioKJW2SRc/n0Ii4Fr95JN7Yy+taMKSGb1gQVGZBG+E2
zhEkug1fBodQ1UN0Ytqy0gs5YGUxXKHnIUAX43F/e9xYcNDXe1HZk2mRIUiygW7A
OETb5DIbY/EtphHfa7WMnHhgRVK8EpKqrfKYUxWtJ2VfKs0hat+hbzQ1UKc0t0ig
QbdZGYU6RCuNdvVS2tS6BJ2K4guWkK2XHPTZWFGMPR3RiAGisySNxvo585mHrWKR
hG79/caPmlchCOPZKikPXAYrNeOqlcaObsfasZ3TIFiWd9JSjik5UnStdrrsz7R/S
D1GNWUwETvcrKtqp2vrMhvHmuNp0C9dN3biCmzLc2fB/1vKAGLg1RP6LR14nQJLS
CAPHiA0af3SGxt5Wy2mU2vWLEb1D0pIX0sQ/Easx2htl+fHC+Ci07HRFgmp+Sah6
NoE0Mt/LZAYvjEl+BpzChTY9RThaa2igmMeqRyy3PdQtr7GMy1fpObsayqy+Me8s
wR6DyIXa5tF3AxjxL8o+5hrYiel8D8N/04aJHroJI/Mf6iotFxzpz134jcw4g0hv
VElBYHti7+YL4wvslb74f6ba5CHP8QjQ/eGw9U2ZIB/KpWiMmUqgxm2ANmCEwT8z
3tAfpg1E3V+Sxp89YySC+tYXtEYwf8GhN07Es0V+qx4yD60mC7NGS5kpjT2gUJON
/wiMgx8w8vzvrvwRM/QR5vzVuWRchwT7Jg/NRFaNydMz3y1TxWkH1EuqE6WoTe+XZ
ZLDhSeCi+NLcYDVtYZ0Y+D2PoBZLJvpWtJkr9mxTdGIxVG5mibxKW2YyGpJKUPh

```

AXUGqf7xwrXwfifEwpVqWbUDm1U/69xW1Mrk+TJj9C+tdb7Txwu0MEVN18oHFEU
CbUIU10ee0/H2/ENA4cgsWUvJLDoJB29sfUvcYOW+EJbIpOf1UfDe3R3XVH/iEy
c7SzK6Df/nx1GUGvIMMMuCjzrZm9FKAFwgJKHriTIdrWQMCUEhxQdkTPoMifyX+
3YuzZ+7f0VWF1fuok5esvG0131Drnvff02WcY6Dx48RhQDiRlM0rGL7tM9N3i13v
Q27dUcrUQDVaEoEJB4qgh4RBAzHkw4x0anzo/gBQIGo9cW1XP3a8IpTFfkhVrNg
8Z9I/VsjYfxgwNDnM02VRgV31GpGKNVhWz9Szcjm0EyjwwNw019uBLxseSrgaGiP
zARiqlV/SWK+E7FwR+INQtrncRs2yvMPCqayZd0n1TN+F+ASIfbWm5yaIMt0p1N+
7o/CfzXBc0M2N7HnveJXKhCysZ0osrrTaSWPT3SS/gGLxQ2dXMhMHAaZvEkFvj1X
xzg6FTTPt4xVLKDxJrK7U8xj4PF77YxuX62v1vD9cdqSb2sri2c2+SF+VBCTF1r4
/d0j35AhSFLqunWR0A114tXeoP4PN2Y/0u1Vq0Vi/uQZHQG8Xqzpztj/kHYJM9V6
yKu8NbGtxjunBW0t57QeB+xyCD8EK1gDDysuUpTENzi9T4dhijv9zVHLEWrwQ6ov
u+rKgtP1o04h1+hSeUjhCLGiJYEXst4MWKJuiRKnmbh9sFSa024dB24x+AQJvZ7k
t3lNC3Y2cMop2mpK6rMjruh8FXH4q1Bwn1CyWMzLYrjD7uld5UyL7o2rhR7mKVZ
FeosAcyN27WI+peHi4L+bkeBHulwxwrXib53HYZrISLFPuGtOwvVhY1WuX6yiFWf
l30jQ4FqNY1/qg0pq3HkWMzVn955A5H2YyegGbsVDed2lJ4UIQR1sMBkJHLR0TCW
jcTK/OqEz3XScJuXhJgAwYgagUGb+Voc8LQ0174iwoVXvdaBE3+mGFwCA1x1U00Z
Or/vty7I13Yqb/GtBj2l4t0pF9TheqsDgI1P8IJWLWKSksUmcyyoN0xxC//A38rG
zXxE186ri/ZLKfD1aCg9Mw0RHEdUOSg1K79BFHNFJdkxWgUuAT7CX7q25u0R3PKN
qSNZryUrwRah6MAV8XRCHNvtuKk8UUqbyIy7NNc02PwAduqtdM9P4u5AgAuzNuv+
v8Sy168YT6854/52dHcgYScWLxHCnYroRnjY2DUNkM85clpUBkX/QlB0yiLiE/w0
VhmT/X7i0I5uF1/eW0jU5oD5dWSmD5DCuY+qz0JKvDQKqEEwMHTKjkkyQBt6vn00
qBCBqoW0+aJEWjzhHa0M/wE7U6H1NSaORP0tPKy7Jt+K8MajdUuU3s0nRJfgNNac
rTEEnReJxC7B4dV2qtzs/SDQryQPTuV1R/2+KkgAUqiDYMZvQfdR1bJY6rid3Evdb
bLPN1w6c8J5qV/+W9uDWTofx9fs9uK0wZlIwfc1ac8Fke2aZSpG10Ts1dP6BWcga
h88avKEV/pLt5I5iigj1u9q5A2PwDwoxdlvSyhL6k0j618+B8Pun4NBdVmvNip5A
wp/ACatR0AFoPCh1Gdf+39P7STfkBB+5v7+0KtajL+rMR7AFwGHxg5NIQ+jc6dPf
I27AW8D1kDLH5SuugDzDy+S33y0j9vY754x1YrKYUwf/aRvG2EfGCdrwxjH5bsw
ukMntuWpQMhBEy94vdTNWo5xp1NvCkiJCGfY7AMhWfHgacae+uY0WqxgUxpJPBaF
c5rvZaKD5QS6udPyrrQ2xPdKpJ3Ky3Xh7NREeDYHWq/fJXIbq/AM5LqhiJWtcwH0
4YkjsYJ2DcWnrj2grNx0AVD3bK4HRgt1nSUBop5kn39zpK5ZgRPQ0fRKxZbFCpm
1cQ1avhCXwpYaFda8Q0vBA8n8fQ+GdBjRjEtyUC31M5w4spY8d9uEwNtLaJc9okm
B+TsRIbmRLaGkwfUh2j1Qj6X2Jj2dldfT9uwMkxBezEg6H0jfH1EyJ/xWbeLrGgkK
rIJ9CjbbdNXgsBVT892yvRczix7z/vhCKomUXmKQzEKv/v01+UVyCtdcPqUMB1ns
Buj7wxQHBH7kYTIAMPMIKMAcPLhpYecD+6AebpX2Bjq+i/kM+1Xr02czQTBbJYn6
jaYWD0GM84S64TJYXgsGffyysh/aBbB3rhN071BjMIwIPgtC9sD06TUNIVwr0+bM
QNaJsnpZ09qllM3izMgXzYB8DFTL/UW+aGnwQN4fQiStPPQl0JwqVtUbB4qr23n
cnp5n9gPb7iLeC0Z5Je9qqta/Uj90BPM714qXbMZpkICPSJI6VsVkBG/WMnnHjCF
+x9ek55H6XPD8e5LWWSVrqK26LY/VKtYQVtIhPP4RsZluS18Yk9TwGx7ZB0zwyuB
ZySeTTF1Ao7MYzk2wM0hcwBexcsPC5W5voWIQy/hXc+Q/K9Zm2ewbqC7q06hH1L/
bX8wjbjVYm900LSfUvtHSzyShG0tchXh9aCpoVKLybARfaiJqAKvsUMXNTFiXzF
85NUAWGqBHTKyJ+R75Ud+0iZlBjplDY0+j177iXqw0E+0YmPRC815f7x25e0z0sT
ry1xRxlQEweP9ooT5e+2XdUYQSi1QuZJb2h2LX7rDA/IDD2TtTTYg1UbRfR0ayzg
JUQb+2kbyHARQJdIoCe0YG0npFboS6ss0lgTmP7zIkh5M/PLQraASzQmXZMVJ9SR
9i0rVBdZN1A0DDJq3cM/iDrTQYjfigL8lP5xz4CA8uMD8FLQaIpwL6SCby50RFX
RKldybJfn2LD1nquQmA6yqI9d32CucawMyAsf+70qrmtW9PNzfgeAhIaFMuK0ah2
AymtgrFrH4U4qxJVweAvwrcyWtpNx1yASrYlrz0MbV8qhdLdpsAENlltYzPWtyqF
buYEMKKMFTdNlZKCJnXfW3ui1gHoALM1mRJENzAPx3nQ7f7nmpnzG3xBsjmwuXQD
ROqlVIu9PLi4NWE/51NGgvw1PCJvYIqTW50fkkeHnmnxtzH7L8mKHYYJKWMTxGoa
N0g+CxXww0moe84EBtSlw/Tz3lRtfo3wm5Haja6PMAE2oFEReXlMupow3jrZs0/R
1JGUzudUKsneDa1N9cdG7IZdFgImxZFQU+Ensp1Jh6zWOM5eYjJEohoL+XlTi9YZ
pHGoWDecs+UA54mNVbhQrQnynY3T0/qmE+1MAortbCNjCZ2TiHSxdf50RqdMxjoH
DzKpqmIcBnQTTcEfx7Mzg7WRzAMWfAy4ZgA1K/En905C3MH3+j3gX4lS0xa2mpJj
EMS1Z7Iuu+dM8E7ZSAFdNWOGJTV1ekoKMaHbfMe40iKzx7NqFTmbLAcMqmgx/s0x
tZYqsYjUTornbzK8/F48VlyGzJKbvSA2UVXggcdI881iaCuyJIDy3Pv7A7Bh8sA/
lthTkn9VWI+iDcKgZQanoh/JSfAcDxhCRDbpJrQvMMnEzvJk+c58aiHnDcDgA7Mm
6hCqq3rSdd/POhFBgeCMLYEvWu60trM45Lfte52/EmYsdBorniMbuN0G0KJrQgQb
lMmx34vZuT/cYdJvovYZXGniZodNs++ziupzrfB2GIQIFqCLhDhw/pFsrMP0jcZy
zl+iKT+P/ZWg5yMB5cWP0zZs/0IXrKpbkhaquFgv7AkBALDM0RyBDSKSmA6bu9Xc

cVm926zeoo6pNFgz4WDHLeMieAN/O+NUZnK/P1SBjIfksvTyHQY8DdPjgqrK47Tm
NjKL8k+jJh76Gcs47DbcF0KsDjDPRRDZy11LB5c/iA9V3aESjEpZ+01YnHcDft3f
b6hs08vB5caby0QBHBk8+13xnoM1/lCbUkmforCjF+I1R8vJhUFBBoxVCIZVoPwjT
kQOuBf2IijAJavog5Agf4Y9SHcQhnbaeuBAZBY9jBx98mhZj9HGdAUhuBGTvU09r
kqHirCyijyUX24RqiGSF7517Nr6TVj2JZl0sIuqcEtpFFoAjGZ6yvTE185toj42t
n8KISHFu1J1LdkQgUdVBc2Hn9VTF3wfvBXNvoIV6gZckzVQM7VT8CE0oEMdkt2RC
+xoT0IKIzER0+0QJxTG3Zgga+NPzEC6C4goHa0T5jaJmDURWnjeewkA0uWsWVzhN
6e+oVUirLt1ml/biJ8opoKdcxwHA7hwY5V/G+u05Ezr9HqXm0530gTOCRi4strmz
XQghJ+We5XcL/TXDrkU+GGCD2+rrtCMoa27qY7WUS5B9A0tmWjoZnvs5BeqDkXHW
xDnMbRvHKMmCaUwHoeBAJobT0PKQ0xHzeC1N+Q4E4yIN4gu0fjoCxsEVEHB2H/Ke
BfaxLY5dHr6NMWWR5FAZm+AYind4/pimQc60X6VgSRBnwgVlJdu5RkzpnAsrXxJ
NcAgR0m6UFB3Lmz/DScePqIL/OD1E7FyDsL384AqIP8xPkiKxgs/TrVzTTLJmGuz
P46qPFb8cmNJ8jj2dEjMfSLGZ8gIXDT08CpU622QaA365L+w77gH9KEWDDs+CtP
3HS2GPL3j0531a9w9azTPxYmuEGM3fJNCXx9Z9du367DSzylA3f+yjwR8wHnLiXn
JGT0Pfm/KD4KW2jk4EAWbAts/Msm6rebnFLWltEFbHQAFRixv6L4AS0zhFVCs3
CJj1yYwgdyJv15w1w3iuf+1oup1Q3cij+S6b0/QqG7uk6FpboQhTp0VGNw9xcV1y
SACx+7/AHQfIVgf0DNln0T56wGs0s4h0p4YTuzL7nRpaMcr3u3f+OA+DH1c64bC7
pUSHZj1TcwXkVR80C79Xwy5RTxg/dJHgcQ4IsPfdSV95J+FwkHAZtn0Ig2/nyT0
0NQahYfRg8gcei10pSCU8b/1cU4YD50WJfuGuFyFsKVKWFQrdfUZ1JyGBxnr0PIy
/kf1n1jEL04TpWdG0G41Awd3078bacC5zjPwp0fgCeSTKJfQXnG4Ai07hD3SXiSr
Kj5nKLz1JePRwd4rf9I82cyl7RaiVDIog0vMLVxvewecUjWqKa9mdKDUcvEGMyt2
gzcd7171pdr7NV9/1mAHTeoWSPg/iIW/Cd9T0BeLMHiLnc9eujy21E6zWSXkKEBr
YP+33rFKeSGa11/8ypUJIFL0mz3tDCZRYB0/uFSDEKZ2VGEy1fFS8qemCHNm1CP
1yP2e3V1fJh0z6C10MSf1AbRQ+J60FpbeMZS4U1wIs/AVdsirMcuT9pnHrkYH6W8
DBLIdoUttGTfH+54ipKUg1WrkJLxUmR6CCJd095jyzB/p1iYhNWZ7etGSND5/mrZ
6sgGGXPnI7LCwGSwtEPazcPBqfHEy8nsbXoYz1XNqxcldCGmi1RJsyxqcY4izgu4
0TX1hDDJZ6hoPU/bFXVtds3btPwNy0uFGX06fu/t0pznWGRa1ANSp/21n8j0d7ns
wjb00u0AZuewj43FgJWWKgfi7tSMbAQ14Lth6XF2bf4cFHvegg+AUnc8cmL+Iyd
Y1RURBUJBVln30iD0q7Kz0/OQntLUcrt02wG+FbW5Zp1deXMMY9Y12yxcccAgVeN
RJxaZfsPPJobn39ZI8i1EU/W/6NZFXUSk30vbBMB/dlGrP60n3ig3DeDR0flvqS/
2hLZb9ER0CzLfimZ35TxbUoPm430H3QWoIM28+mr2sr0brCeJQe06SFumif5iXe1
j0cDRbm+jjUVC7Jdwng79npdt71Q3jUPp8ge15uiKr329S6qwYtmG1phsACYRCaX
hvx8yzb9ZjFykP3VaVW9GK3AJF57HIIC33LF2YmEBWwa7Has46k841o/HtNZhAn4
ti4ogWH2YJTiBzfQQVYv7L7BAnrcEmsdONEEYdaHKHA1/jR09so+5sxEiyRTNLta
f9Qco4NR2AFYYRfMgxPKPr5pL1hpmcAskIrUvZBELXvmDTwoZFtQR3/DWQaFUMnE
xXLtg1kLBtB6z2FJfy1RFJkLm3Cr8Q0VitUbByDtBYkK668SLEU7r5gKcvtH1cF
ih/QwMiAXygCU0k7pxUK0qHa1yNyiVxeBAvUtTER+S/hk070iwSliILbK0ef+8pL
RLZucZXC5TWn3TCTSjeSI9XjERRF3P7ueM1jsfhgVzdtCxaXqgDyNeZDbTHM9Zu
KYIwJgrpRK/UQG17uKx1IBMECo5UrVOht4WwxH68G100i1ENsatV2oBjNz9LhCnh
aqb9YAqBb+0EopDuXhIhc75P5CB0ccn+u6S+PU7myWbL0nQVVXh/d1GJSZESDnie
tW0Pbw9o/5hXT0upX4uFAvbgkkQ0D016jc+5Wqn665cEfm600ehNQmToSr00DF8T
UbV9QWvz0c/6rvjm1ymIRkHUb1C/91JzjJTPw3gBzfXmpKENyPniBVAiKa1NtWrF
K22LNDI8mdmSSoIyTrD/2Y9Z0VCbx1LkXBSnKHNmUUDHCSdQZe7DPONQEY9Quu
a3qtEU1mcOGK3HIKQR8XeaUDnlvs9gG5P2AxQEZs3dP1M30J9AIwKjpwHy1jfPuK
qh6mJTVBYkJC3zY0rfhJwkabIBaQjdTUbdUokVU0IE/wMA2PJZxbG9SFsQPU+mBv
GQv3siLE0iUyUw4ICox7IhMDetWP69iaI03jGQbuEm0dd9yvI8fjCcRoUbw9PbB
3gUHSSqm+sqqfb02LCWdpv1d85uZC+VE21Ch2LQIrINhinH9ZJiX+iLAjthx55m
GMCORoWUmNMB15aACuaVf6wvm33GxcIQDMWWbL69IAUmsu2g85FrBpuUhe8IFokk
VF7053IBFw/LF0830rDzE6w5tEr3NM2I1g1LQsvqL+bpgGkixVthBh35I54shZzyk
wUJSTlQDrxQRrm2HTuCj5JNkSnm3W03DHdmiKMLD0LIyAuRIRuTLMUEt1gqz328M
o/6k73SPFuAwpVokN2kC1xDtHS82Pyvw01m3a9WFiSoVG576XPDDTfGtyx2KYZdx
YbE9WNd9euMYYGQdaGheQ9SF2U3+rQXaFr89GUAe1XhU/24npcutZsA68o6e+NU4
e8pThbPtgWhXyX+NHuWjArbnuSo1tWcwaNXcReHaKfdoE9Z0Uixr+XYuHfgYDgyE
0/U+N11UGys/89wbEK1B/08JxW5TFzEQ/EER/Q9ZB3/RB99pL8sqqlLJq30a1+NI
i0P8KEmrOSjGmXu3ZH6CHFcpXj/uTTT356mWiGr+SJAYN7DvjYuWf1MA9S0p1V20
rcZN96+yt9c9CubQSUDU0yUh+Xbzq9HTM5JaHACxjSc3RQB4CDaAp/67toJQCsf
tHHwXf88Sc3WPPXAJAnaSHxgsJu1nlo7wPj+jiJ7kMwD19B1/BPrHGc+aeUtvIVW
D8Fu+XvTFPnywenrYnooqky0FkTbck08MYDx0iiyXhVWKL1CnSYwfIQvDtEN/bq+

```
ObX1YQZKiWLCQajx0o1Dr1gEEUMDLUNYo66MjRfnxgtetDg0jAZNWNB1lwVv44tH
Z15bb2QdMEBL5cSaEQz03CtuLNUnPjHb3NiJV3YuWuLeBtcwJNzTup4GLD8kbwqz
IJD4aG+bCyWs6epTifI9zhLorDJUrmxaxy5sxHDrzufAMNfZTV+nTGGQ6iVsLvc
RmfiQ7b8varVDVtrBHX8vzI2Quier/gNLxn4AYnFtXQjbalYOp5ySOG7Fx8GGZvW
+NxHledmmASlubNLYBre42wV60nGZ/eZJtkoH+c3spaQ6UjSp8pZiwE60jfwNrB6
qHRxP98ftbEdcB586Tv0x2zYNbd6MRMGQMxo/8k6YRvJTeHfAdJ69TsUI30LVu6Y
drxpGcDKK84JEt7W7h+6v1PfG8RzK0X/M3U2EEZ8CHL73caVcPTQ5FSm/rGj1smU
ZBja96TPY2JYv4YB69drCTjhH+nR9JAuhbna82e/HKN30d0fU54JjN3C1FurhiAh
1k8oFabzoF96YVdg/mSttI1zh3Sw010NmyuagYNcoLELq1mgWM7Kd2989KkX2j8
/bQRsJx02Bz2IdNbD7E+hBjedywDaqvxfTqQBcoQePfMnAhhzVCrAB6z+UfjS9Qh
us+CcqS4z+3YXun2a+Mv+qayDqVjWcZy5sDmXXtS7rxHc0dE5CwD0oH9quLS9N4k
aoZHnZ2jc1ksQ9v32jimBKQfmoMohIvAwVkrGzCBxGRJj1xJsROMK4bmAaCiY1pX
eGbbwfTenscaZVY50Ia+pEmFIj1Q1UvX10D4nhQGGskAJkzz1u3FD6mH7MmtDJV1
pf0degJt1w63DyKRB7zXAY4KP5nCdV+PGiJa8KCyVfDyrm0+/U1LIvpmUJP/akFz
H8g5VEv4CP/Wa69P72w+xZcbRaEwvg2ZZ9fdQ3EWNi14yyB7utbf8kdJPPBNGutH
/F19Xy0tzT1k0HUETcZ+jE8LBCSjVmLU2ELMKFmWNsST9cM1nmA/NN8ba9ijvVA/
cMTAloqLf00dXnzUNrdabQ4rxvQaIeW2iyQjyJQEFKL00Kcqwvtu4WY9w4DibfP4
U2IY6QVehXNXveg5x0wvfxH/gMT9Vp0N3xCBw89Bh30S1x9ViXVObJDLWw0/ZxC
BGbFvqM/RNJ0ew6MUYDU6Tre6LAvPcLgYL2dlywZGWG20JC1MOajDnRH9iRgBZdT
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"
```

```
MIIUGGyYJKoZIhvcNAQCoCIIUCzCCFAcCAQExDTALBglghkgBZQMEAgEwggpDBgkq
hkiG9w0BBwGgggo0BIIKME1JTUUtVmVyc2lwbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtdW5jLWNvbXBsZXgtahAtc2h5LWxlZ2FjeQ0KTWVzc2FnZS1JRDOG
PHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHktbGVnYWN5QGV4YW1wbGU+
DQpGcm9tOiBBBg1jZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NC1RvOiBCb2IgPGJv
YkBzbWltZS5leGFtcGx1Pg0KRGF0ZTogU2F0LCAyMCMGZWIgMjAyMSAxMjoxMzow
MiAtMDUwMA0KVXNlci1BZ2VudDogU2FtcGx1IE1VQSBWZXJzaW9uIDEuMA0KSFAt
T3V0ZXI6IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcj0NCiBNZXNzYWdlLlU1E0iA8
c21pbWUtc2lbnmVklWVuYy1jb21wbGV4LWwhLXNoeS1sZWdhY3lAZXhhbXBsZT4N
CkhQU91dGVyOiBGcm9tOiBhbG1jZUBzbWltZS5leGFtcGx1DQpIUC1PdXRlcjog
VG86IGJvYkBzbWltZS5leGFtcGx1DQpIUC1PdXRlcjogRGF0ZTogU2F0LCAyMCMG
ZWIgMjAyMSAxNzoxMzowMiArMDAwMA0KSFAtT3V0ZXI6IFVzZXItQWdlbnQ6IFNh
bXBsZSBNUUEgVmVyc2lvb21vbiAxljANCkNvbRlbnQvVHlwZTogbXVsdG1wYXJ0L21p
eGVkOyBib3VudGFyeT0iODhiIjsgaHA9ImNpcGhlciINCg0KLS04OGINCk1JTUUt
VmVyc2lwbjogMS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9hbHRlcm5hdG12
ZTsgYm91bmRhcnc9IjZiZCINCg0KLS02YmQNCk1JTUUtVmVyc2lwbjogMS4wDQpD
b250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Ym10DQpDb250ZW50LVR5cGU6IHRl
eHQvcGxhaW47IGNoYXJzZXQ9InVzLWZyY2lpijsNCiBocC1sZWdhY3ktZG1zcGxh
eT0iMSINCg0KU3ViamVjdDogc21pbWUtc2lbnmVklWVuYy1jb21wbGV4LWwhLXNo
eS1sZWdhY3kNCkZyb206IEFsaWNlIDxhbG1jZUBzbWltZS5leGFtcGx1Pg0KVG86
IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiB0YXQsIDwvZiAyMDIx
IDEyOjEzOjAyIC0wNTAwDQoNC1RoXMGaXMGdGhlDQpzbWltZS1zaWduZWQtdW5j
LWNvbXBsZXgtahAtc2h5LWxlZ2FjeQ0KbWVzc2FnZS4NCg0KVGHpcyBpcyBhIHNP
Z25lZC1hbmQtdW5jcnlwdGVkIFMvTU1NRSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0K
ZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lbnmVkrGF0YS4gIFRoZSBwYXl5b2FkIG1z
IGENCm11bHRpcGFydC9hbHRlcm5hdG12ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5l
```

IGltYwDlL3BuZw0KYXR0YWNobWVudC4gSXQgdXNlcyB0aGUgSGVhZGVyIFByb3Rl
Y3Rpb24gc2NoZW1lIGZyb20gUkZDIDk3ODgNCndpdGggdGhlIGBoY3Bfc2h5YCBi
ZWFkZXIgc29uZm1kZW50aWFSaXR5IFBvbG1jeSB3aXR0IGEGIkx1Z2FjeQ0KRG1z
cGxheSIgZWxlbWVudC4NCg0KLS0gDQpBbG1jZQ0KYWxpY2VAc21pbWUuZXhhbXBs
ZQ0KLS02YmQNCk1JTUUtVmVyc21vbjogMS4wDQpDb250ZW50LVRyYW5zMmVyLUVu
Y29kaW5nOIA3Ym10DQpDb250ZW50LVR5cGU6IHRleHQvaHRtbDsgY2hhcnNldD0i
dXMtYXNjaWki0w0KIGhwLWx1Z2FjeS1kaXNwbGF5PSIxIg0KDQo8aHRtbD48aGVh
ZD48dG10bGU+PC90aXRsZT48L2h1YWQ+PGJvZHK+DQo8ZG12IGNsYXNzPSJoZWFK
ZXItchJvdGVjdGlvbi1sZWdhY3ktZG1zcGxheSI+DQo8cHJlPg0KU3ViamVjdDog
c21pbWUtc2lnbmVklWVuYy1jb21wbGV4LWhwLXNoeS1sZWdhY3kNCkZyb206IEFs
aWNlICZsdDthbG1jZUBzbWltZS5leGFtcGx1Jmd00w0KVG86IEJvYiAmbHQ7Ym9i
QHNTaW1lLmV4YW1wbGUuZ3Q7DQpEYXR0I0iBTYXQsIDIwIEZlYiAyMDIxIDEyOjEz
OjAyIC0wNTAwDQo8L3ByZT4NCjwvZG12PjxwPlRoaxMgaXMgdGhlDQo8Yj5zbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtc2h5LWx1Z2FjeTwwYj4NCm1lc3NhZ2Uu
PC9wPg0KPHA+VGhpcyBpcyBhIHNPZ25lZC1hbmtZw5jcnldwGVkIFMvTUlnRSBt
ZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVl
RGF0YS4gIFRoZSBwYXlsb2FkIG1zIGENCm11bHRpcGFydC9hbHRlcm5hdG12ZSBt
ZXNzYWdlIHdpdGggYW4gaW5saW5lIGltYwDlL3BuZw0KYXR0YWNobWVudC4gSXQg
dXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gUkZDIDk3ODgN
CndpdGggdGhlIGBoY3Bfc2h5YCBiZWFkZXIgc29uZm1kZW50aWFSaXR5IFBvbG1j
eSB3aXR0IGEGIkx1Z2FjeQ0KRG1zcGxheSIgZWxlbWVudC48L3A+DQo8cD48dHQ+
LS0gPGJyPkFsaWNlPGJyPmFsaWNlQHNTaW1lLmV4YW1wbGU8L3R0PjwvZD48L2Jv
ZHK+PC90dG1sPg0KLS02YmQNCk1JTDQ0KDQoLTg4Yg0KQ29udGVudC1UeXB0iBpbWFn
ZS9wbmcNCkNvbRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IGJhc2U2NA0KQ29udGVu
dC1EaXNwb3NpdGlvbjogaW5saW5lDQoNCm1WQk9SdzBLR2dvQUFBQU5TVWhFVWdB
QUFCUUFBUFBQFVQ0FZQUFBQ05pUjBOQUFBQUFBQ0FVBRV1I0MnVWVE94YkENCk1BZ1M3
MzluTzNUcFJ3MjBkXBiZkFSUUVqT313aXdZbkN0a0RLbmJjTGs2NnNxbFQrenQ5
Y21ka0UrNkt3a1oNCnNncnY3FWTXBMMmpvMDQ0N2dZRHBlQXJrK09uSkhrSWWhB
ZlRQUmljaWWhBZjVZSnJ3N3ZqdjBaV1JXTS91bGkNCnZkUGYxUVoya0RE0XhwcGQ4
d0FBQUFCs1JVNUVya0pnZ2c9PQ0KDQoLTg4Yi0tDQqgggemMIIDzzCCAreAwIB
AgITDY01vRE510rOQ1SHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQK
EwRJRVRGMREwDwYDVQLEWhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTBVT
IFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTagFw0x0TEXMjAwNjU0MThaGA8y
MDUyMDkyNzA2NTQxOFowOzENMAsgA1UEChMESUVURjERMA8GA1UECzMITEFNUFMg
V0cxZzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIIBIjANBgkqhkiG9w0BAQEFAAOCC
AQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQJ+Rppw0DxxzY60n1lJ53pTeNSiJlWkw
w/cxQq0t4uD2vWYB8g0UH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6
rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXm
bk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmswqpS6oQcA
x3Weag0yCNj1V9V9yu/3Djcybww21Jf5NBmHbM1LY4X5chWfNEbkN6hQury/zxn1
sukgn+fHbqvwDhJLAgFpW/jA/EB/WI+whUpqtQIDAQAB04GvMIGsMAwGA1UdEwEB
/wQCMAAwFwYDVR0gBBADjAMBgpghkgBZQMCAATABMB4GA1UdEQQXMBWBE2FsaWNl
QHNTaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQwDgYDVR0PAQH/BAQD
AgUGMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSR
MI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAA0CAQEAguL4oJyxMpwW
pAyl0vK6NEbm1gD5H14EC4Muxq1u0q2XgX0SBHI6DfX/4LDSfx7fSIus8gWVY3W
qMeuOA7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMx0D
Wq9opwtA/1T0kRg8uuivZfg/m5fFo/QshlHNaATDVEXsU4Ps98Hm/3gznbvhdjFb
Zbi4oZ3tAadRLE5K9JiQaJYOnUmGpFB8PPwDR6chMZeegSQA++OIKqHrg/WEH4y
iuPfQmAvX2hZkPpivNJYdTPUXTS07K459CyqbqG+sN0o2kc1nTX185RHNrVKQK+L
0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJc0vT4as6aqdcwDQYJKoZI
hvcNAQENBQAwVTENMAsgA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAv
BgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydG1maWNhdGlvbiBBdXR0b3JpdHkw
IBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElF
VEYxETAPBgNVBASTCExBTBVTIFdHMRcwFQYDVQQDEw5BbG1jZSBMb3Z1bGFjZTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0iehY0BY+TZp/T5K2KNI0
5Hwr+E3wP6XTvyi6WWyTgBK9LC0wI2juwdrRjFBSXkk7pWpjXwsA3A5G0tz0FPfg
yC70xsVcF7q4WHWZwleYXFKlQHJD73nQwXP968+A/3rBX7Ph00DBbZnfit0LPgPE

```
wjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZ063dKvIKp4cQVtkWQH6syTjGsgkLcLNa
u5LZDQUDsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0
zEoj0fQxgq4SWcC0nsG1lyXt1TL270I6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsC
AwEAAaOBrzCBrdAMBgNVHRMBaf8EAjAAMBcGA1UdIAQQMA4wDAYKYZIAWUDAgEW
ATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsG
AQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQUu/bMsi0dBhIc164papAQ
0yBmZnMwHwYDVR0jBBgwFoAUkTCOfAcXDKfxCSHlNhpnHGh29FkwDQYJKoZIhvcN
AQENBQADggEBAH0JoJanzqmgasN3/ggSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNw
YyTneuK6AChwKfnNv0Fb8lV1iffRTF/KtmVEDMR/sYeqAH83KM5p3e12lVh40Hhy
I0qNuz5oShNaACSioQ23WxHGvy9vsdVfnbhspLrWg9NQ2WbpCmK+2oMh2oYl0Z/w
vXmt9cG6jbMvcdH4z0I0vg6mrYkKTM/RCGnumghxwYToj10yD5Gs4D2IJCw+fx50
Dxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDD6hnoQ9rNeozIcBVyybQYjf
rgg4DRvw9Ksk220H4ConlB8f7R7s1LM2cSYxggIAMIIB/AIBATBsMFUxDALBgNV
BAoTBELFVEYxETAPBgNVBAsTCExBTVBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrO
mqnXMAsgCWCGSAFlAwQCAaBpMBGCGSsqGSIB3DQEAJAZELBgkqhkiG9w0BBwEwHAYJ
KoZIhvcNAQKFQM8XDTIxMDIyMDE3MTMwMl0wLwYJKoZIhvcNAQKEMSIEIFT1fYL9
gAEHvzGwOrKYPQPsCdQ+Dvgh0flzrEz5H3UXMA0GCSqGSIB3DQEBAQUABIIBAIaD
09L9rNPSxDuaCb1sG0VYYWZmZ17BoLp28exTLU4Z2peJZiipmAZUaUkGeZ1CdLEC
VqQ+t2snrG6EbfDad8TT0xmp3BXbQdeIO+hftHNYM9B6MkRlaWiCMHzuW3q62w6d
9dMRg4G/PxUWWP7L9c4M3t5zsf3S88JcWA5zLyXxScvYtT6Qccu43HSXciTWb9rQ
vkEwATVblSzmhVA2KFICXRw8s60diLy9q0l/80dXZ8oZBpRgPbn0s8Zp0yX2bldF
w/7Rag0W1j+d3uefP3kxLm62jnd17H3TLlpqNqK086Ho0TG/Tuwqi30sBVn0qrBD
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
```

```
iVBORw0KGGoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcELEQVR42uVT0xbA
MAgS739n03TpRw20dqpbfARQej0ywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+0nJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/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
BAoTBE1FVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIENlcnRpZm1jYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAAh8BW90JuemYqxwwiLjK0/1puC5akUSDDzw
nwIP1+zCjV+RBTnuJbc1Yt80deysj0W0ADJQxHdJGLqhqw7tYChAopgpvEmZIFN
9G0ioUSRxGhbRc9fG+OPKYhTqxy/sPWY2E69RjE08wgh3+g1NLGW968F2hQ8T955
aWD6gffqhVHGug7ZyBV45TwaqJhtKU0Nykp8fM7QMTLfAlEXwhfC0XDg/edowQSZ
+8Akm+Q6Z0Wc+f19QSNVUhs57E3Aj0RXeUzVND+uaajAyWEv5IrkiZsYyqoA3346
1bGfkgqa1rZwCr0nd47+L/JSIEigsEs4B04HCL/3152nd+uJEiwwggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydG1maWNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAY/JjLXmn6Nb0t3TjrWIQyj7z
UqVUusGDtn0vGzlmr3aX7MAGb9gcbiJvbEi1qBddKbc5hBy5M0Aaa2eahJW32e66
Q2YcvCrj56tjKGHnKCKNhEyQaBIJwa586dT87MA1hCgSA01PRWInWkH8yjHkxgF5
VXw2UuH1zk2momhA0c9dkX2vAXihIaldSQXrhAKcaUYH23VcelUtFitlyo3jbs4V
sSdYOhfEU7agSSCuUghB2SYTMe88nrh/PUuL9BCx2Yfmu/U0q6enkK6zhGGw2hY0
zMACnCBtdAcaXBCsdXdd0rJQdD8lvXE8G1R0VIdUAo2KVmww6dD0XpyChiJccDCC
G04GCSqGSIb3DQEHATAdBglgkgBZQMEAAQIEEML/LZyVd/Cgei/1+M1kHF2Aghsg

```

1TX6aXgTAJEAbBbbnV1Af5NLxsa19GZ9AKi4pWk+1l0jzvfxxAOpeMH5z4jH+3r
+mss2RN+DVdfItsa72lXat6FdC6+RFU5RziCGJdbHIvRzw29BWRQW/eem+RXhi4t
VST7l6ND87C+BbWwVZ0JDj3yHXWxYGSgzNNHb2Ix4wnf2DWbWqtHl+7SniAh7QgE
8wl9K6M6Qi40EwyAEPBxtkGnrGYgChBrchvcjsV/TtQx8WeK/0z1uNDwbVtUPaep
UIM0uIf2vCcp27FkWyh60JdwWVeRg3af81vxfStN2GbKATt9fh8RwNACtGfVc+u
NpjL4Qf8FMGbfuextkmlq0U1nsGZP301JO+VDrpkLRPoLk4bjh6Wk0mEbvjRFeNX
ZUVMWVbnDH4Z5+t0IXNV3T59fsJ7QqnHOKqGL1y09fZTIc6lNA3bELXM0nSgDP5Z
iDQLyTcs0nk7YooEIUX0lUMt3FBS1SR+ieABPj7lZCn/6bg43QS6tbtvx/12bJxC
C8ZE+dq08TDiWGSn3vPfADbt+7reZaKXNAH+tFVcW9Q6GbgAVvwNynjRySTfzK8
HearG5r9F8ZtgV/Fmedod4s8/VxGdq9gl+z0R0nmE8P3k2PY6pAWbBRb1DGfDMwm
A62aiLz5cc4Ikri1jexndSQDowQpn1lD+RYLWYEni0NhE8ueM0iN7Vfv4b8Bxts
iisQ7M/lcbrCTQqJR2GNpq3WD756ARlaCIO5zqXmKE6I1HxsJFYGjQWYo/bRqdK1
8nzEbRL0vcNSIr0jcH6lbizum1otU3bDdqBXlTeKW/4CONB61hXYwMaoG59z3YVaE
GoazwiiAXaFZDIZ/so1sQAHy7LiwoDD0MY/Fx0rgCQkN4E0CMYxhW+3Zv/lSpli
2IDnyaMZ0BoIIZLw8uJvHw5XeI6B7vr0LKgd/JyEuhqtHNU+q4fW1hUWF6rFmP+5
88I5L1TmKYHAS5wNdI4RnhZ96nFdjz2sG2Mxv3aChuzrfYmCM+/88NSB8QdZB5Xd
H5FTwjizYdFoAaobAIyme8x5HRqjd+GTy/sqq5aUgs388CCQE22F8qExCE74bL0Y
YT2NX28Sp6C4i9ULMxV1Yn1By5WfDbz+3kd0vI/+c7nkxjgfmDCZe0Vlrz1JM9yJ
aDvc0IRrPjn7X1PY0aquxzBgE9wz4zrS7IUCnezipoNiunEYHpViJ7LU0T6zuE0o
Fu/dcXmeb7nj0s/R09hm7kipEpM75kz00cYEv1NBfsH71lPMoKpqoTK3K+c9GXyA
wBbXL++MzgRfNubhSq00uaaXRLYiqkpGfmvFkUYzNGsgyq6+Bkwjit0XG1WgySo1
3uoQ7GDzmxE9Vn1SVKPDSPiuDPQccdfN+B1D21VjrSS5Koon+v13McJm8z1X+UaR
wA0dhVjs0JJvpyoMI6Vv1h26oYmQpDwvp/eBBiZREuDPdDIyefD9aMnYokY7iua
KucdGoryEc+wnBTsnTryf0tU6UwmjqQexZFeLrce9FJ65SAR0z1ln9p1NjloUauE
YpIQWtwfW1NHG7VEWjvKd0711fc7zJcFUZUCHogMoo3r16WsK6QSKNf/k18/FUj0
/icChsKVWRWcNn9MuXchhEwr+QvI26f5/CD5ErXSy/wxk0mm6V2fbd50ei+H1Tz9
hIDYGHxJPjAq83YVPQ4r1Ndy682QNDL9oNz4ENFGYRj8Q8G20F4IDG6MD0xSBNuu
uRcjTvE5b180hZvq0F45NyKQZh47XtF6ESrYI45DkqpHDxNeIQG5Fowfzz25SCy4
CNQcibLe4cYNYlTqfAHa9FHDMBW3kJJDHtmaX17Zbtyz126S9QvJiIR8x7W811SB
IEbOMmZ6rNCok+7P5JB565//+T18y8dNxZPLtSbBx7X03b9REiTR2s7M8jY0jKja
/7CWWX/fAQeivjy+9jFk/fD5x3w/Sn1uFQCBUMf5YflkzEqqr0jq0ZjxbzawgNkx
QmtG4GtUr3K49MaC/XJ13/i00NRng4Y3q1h+4mdE6c1n+CpG/BrRBb5bxZrGcqJJ
swlvoUe1HwyKXoXloc/RhoLYC1NB7NKJASm8+J09ugcKdfQBREg/4dIV3SQufftG
xJyoESXAOg5TUw6a2vDhfLZ45WDDuVBuId4uiZX0E/5xT5SzW1ZWfZZi2ZHkRWDq
F15PIfOXXfHXh1PUJ0B1x+fwKC6mrQV7oRMRVWunWPwk0tSxuPolCIKtRuodS1Ee
9RzI2Xy9QLX0AjUSr1iAjvCmcfIfvxnyX4KRvwHuAx0FTNJUxR7pYRwJz7xbUeW6
JjjjCb+52/jmC6WmLr/aSsNq7PyawHBR/N01Kt0Z3T/fWdQ3+cYgnDTw0wmvqR55
xJ6a9qiYytowff0YaDGwaWEUpgisrfVNei9sVYLo+4pzT10Xx2pQ31NweMn17rm
A/9xue4vauFZ/FPQ1G1ys5FemIO5z0COpXrceLejBb+5ZozQdHSKmxuaEHaReu4v
jR7j4NYDfP7LFB3nRB6I+QbjuxHy+xl0bESB7iAL07P72Y/4dR+6gbHZLngirHQE
2RktRXo++8uJ4jqfmlBVzszG1C5R2AG90hA7VLZs7LU7V6E3nzwZ1l1cgxCSSR+gN
e4f6d261oCkJPt4JdCM0ZbrpfxFBitm9R7QuTkrd3dTbQ70VU8t+3rzY2MeIt8R
WNgTc58ThYo30ABAGB4DspLRIywr7Dr1osj1du90vIWnS1LWWSqKQdEu7E90ha4M
qvwrtktLmGgKVijKI0PgxuxXWSFS98Na29219ZytbtXptKpWI1G/rNarBetgNVG4
J0ohqz0Zd06F4CQHfI+1dE/a8g4xDcdZmnDDS4/fr1GhhS3HZVm4csjIyB+YSHmz
cMIIt1LW6aFj1/PS/ofQJ7eEjme5lS1RsY3CjAeM1EMJdXn9SLXtntPDaAm9Q62Wq
rgE+NSeWtyQyJ37let2Der0Y+rWwGtpx9hD3v/np/VWEIwSop0RrnbNXb9VU6ILI
1kfRe2mjEgtU930E/4d9l1HNEu3JFe1+13d2m04NrU0QQ0x2bwIT9TCWvjYDqaw0
OP7C7/Dyxgkfe8f+BKsARkoJ54h20gA7uboeXBEjEeHwsIdZkM32vQg/tP4ftA0d
4Hk14ZxHqJF4ETuQv1KHUht2aJQmQJJWpB5UoIe3/eiqKvHLuJfSbSt0vidaeqK
x/QSDxYAYVCByJmcfutA4fJbC7AJvkJPTYdgYqWFIMDCgu2QmtX8nuwDZchrFYK
BGBze0PdcR4coEh/9d7fqlo6AtcIZKg/9ofWnzPRqA4zgL/Q0JP0mGQYWUF6G4n2
aUNYAZRbfoPLNXWDY3cKy7kAHGZ07qU3QMeqfIffSDHHbaZ6CtarFBcDEwrLvK/8
Cap0aBGX7BxatCLjbb4iZpQvKKyPMZzyRD5oIgW8t74Yc1KnLsTKkp4JDDKcMQLo
k8h75c088PDo09secT3kqCkA+2a7I4PS317eTnjxa4HmGMDQa7ulso30/LHmHKHG
TyilXA1Q0qluw/QmyVx8jA0EkDHsrVTA1KvF90+kA1+9Zf8zg2riX3RrAaGXBCFz
w4M3JosnZVCMRHEAXi0DNJfwlZ87MfrsvDwtLHzHayajuDaaCfbcPs0CARxHtTmH
8qxz75U6nL2PNTB36aoiMWMhUxA0d9J+e413A7C13NtSye9B6hwxUj1m1ik/ENrv

Ma2xbwJfEQKyT51pm4Dg1C2ptRbrka7/33XHNh8WWk6VbWLNf/jlKoFxs2qTff
5j098PdbTSiUKBYh5CRSCl4NbsFZt17Vp9QVWRuK1rT8SCeA/Ev4HVgdX1lBTcX
2phDUZmWU2pi4A2BsJ/bYQHkaaxhGNSF6dr1cRNfRzKExdZLK7ybaFQtJPnzQVL
HOU0mzMMOS2rktQghpqwDrm9cnFjNn+7ZYfrqYq8pZ7I7w1lMBRfnzC3emmNbabN
XQh+mm1LudlDoi0/F5KFV5g1lPdjrB/+dMjifWIVo6HqiXSYS7VwQTgUwPuXZwf
UKYoMQqJfZ5VfIOWiBV+lpXF77Ihxp54To5BtpTI2asTSs0CtfRhpGamp6Vug59a
L4GtPFutrR1x8W6nv+YJkg8d7bWgebF45xL1Da/NNr47rF79bzieUR/kvvnvNmMRR
HIWqYaWcMoGV/RIYLK7lMVVIn4tdkXX/pnafaQj1r/swA5ZG9cq+maBzyA7zq8S
nKhasKLUBnWuPYeqkZyXgaaxIwWVJnKw+YYRCGXvJNYhh91FNK0NXvrAk/TPQ3Th
9skjLzc8TQggBQ+0K3GZ/+oz5U96F5kf2FJj1hAnA31TD0tqp5sWLUkjcFWXJMJT
HtlWuI7xpViD7HRpV+YmpuCDrjwBe15ylhMb1yVj/Fm/sBx6Ta4hcf0zybJsro5Q
KmIroLxeBUDet/aE/GUw8rK7/4eS9IintAoZbng2eLTIrBnecieXGxzjCP1pswTK
4ynBMZCsrN/kFltskTGCbA2j3PGUYiPWYvtZCTEBS1D0LWlflklUxifCvugYtPnB
fnsDYBw3pM4oi1Y+C08LsnGou2aqEyVUKxwX5ow8UriHbrtntN0fUYybUJZ414ZP
9UE40w0Yava+QPv1y8mJlhqidgWMYgJF0v7lFgjjix2tM5T781pjGxj7gMEKYn
v4t/De+30UgprRwpEPZ91DySE6y5XD1cKzrjzaUU6kMJ3ttyK4rDd0IYqn83V8zQ
WXuONNqZzF49SzC6RInvoow2ipvs3/ZDwgVwhDYgDHTfQIvj8ROewB/ZiUVMiBS
/NZbdV5ArfWTum2s54sCVEi3+1ACeLiQoylQQc5mjI9lVQvqwjpzM0p13EQj1tTb
rCU4jZj+nRCqj6c9oe/SduEVxfGBZQ40vG0PoQf6EUy/S/yBBX5eiUA13HNj6tJS
N5uV6LehkQuuN3+0xKH0A53c+AlGJePoc8L8XUCS5XxutQEWf78B1p5IwXElNI
5lnG8xMR4XpcIOK7H1b/KWYJ4szYN/+tXGo8vCy8azYZDT155MRzOdBKicj1+HQW
T4gkpK3/uzxitioEeQbvhDN9LQEX6xpb0vok9MVPBh1nImm5pQIBB+G8X9cb3x0
Nb1P7Qu5qdp3LJQMm+ME2eTV2dKGSrffe2botW9LgYbq8DuR00iC5dGjkSNYx4+8
GHYB84Fox0a/7o2w0+1n+ujCGgEOKjvBtgMLfy1WGw1s4xktp/OrqYdit80QLV7d
kPJhCkpS6MdFeEtn4U0vSh+2DWFNtvXqkJWww1CNN2qupeKhA3afYAt6W3HkUHvr
DhgawnJz+0Q/iRlrzbu1pe7r3udX7zxQ16eV1k4R1kLJ6+v6zxhn12fjRjJL7Ufh
euw08zxtYlvbwq6HW+9iKmc08nxGhitj0Uwm0m0WMA3sASsuMT6FefSiQpu9nt93
TzaNiS1fn9zLlSr+6D9sLwcobNz6Hgtq1/d8u3hIXHJxH0ZTRbh3KmB40HyrFsEB
Drxf9Brn6DxM0eGg2VEgzoie3dn4nvdHNvs6GqgAjQ8pWCzFrWijTJ11zUYa3aT4
CFpz2no5GsnXFfCVyDdXwNuDIhhf+Yke+PJ6ss5YdujZoRux1+C4l9hyoRTnYF1z
0LE20LdFUPBqDMoPsjJy0oxncdF/vCqVaBcbMuAFypxsiPYLSA46RWjd0PasPTfN
Zalwzps/loBuMHNuMx0Zkw62fF81Bzu04Eqld3Gg0wwn4Gy1EATQGC3TfnDlNGzv
mps8qen5F9ER8xv2gyUtsxwLY3RMBsLQp0KMK4uqa6SMq5cw1u6aCPy7wHkRRJvi
Y46Iax6rMcZ0WmcuGqEotZMo00wkCF9dQPfKtIMtacfFqMqoPpDtOw6MnHm8TC2J
/Tb1X6o1tpNDRzwg1I1HNIOKT+c83eVPfnd5FRqLK3FZqHXKkeGwP8YnQkrLC08L
om3dcdznc+giDxhkVjNnG7jtf1m3ytUK3aouJqGgV09sZ5EVzps1LiTJSgbQYoQT
NIKMi/ZQXf8xoffhv7tAGQA9tfrpmq/BNu5FoA08jucgw5EjPqqX1NIivv2ce/wr
7eULcsBUCgnT5/apRBZBb/fv+uZbVrtXajaf+r3dsrfYZwVGeHr59X90s1EY6kEJ
qsSPGhR2iMJBUSj6haTGWbx8dsyodtQrGjtn07uy29oJ4i5eX7e0a0az2fuAfdoX
JkxmKxYCGJIq5SVmfjynb6rNE938KGQu3kwPDIPzamZ5e295y6Z/BLi6zLe8myCi
RGHm/1mx5jX0scQL9s7p+UZPGdQhpfGZQeXmMgSQtS48cBGMdDdXrnuWBOFVMQ8E
gjrDRsVd4hMCKvOMh2bPUNq8/FPAPNRDN2thRts9ZZTz6/ug86wUu07a5GkdLLmu
uFc5Qtu+3kj6FhmjZuFJ3IMExKzQs15T3aUEL5YJpOSfUrY3ir4CECZ9Q0jEpffb
3Xs52uHXP8QcdtENVNX5K1Z1XNBkpJW8fWmuYcLMzHVQ8072kEEz287GoqqZgRMC
wG26oS+yTRMHbPF2Jc+qenFwi8nfcuA2Sjx2Gw83eXGRABvxBspdrjFFc+pJLJcw
RnU0QfVa4IoSr6xCg3e4+ZfveKS3BSQ79ubHoD3cTo2/W1PFXhHH3x5vmL8gVXZo
zAFrrhDfVp63SmqbCngwkdLZr/myoN6oMWh/EyvNiWgRfxpL8d/JZBw6rdm0smya
wJ9k8BzEg9a5nvHPjwwG932xy0HR3eevzuqH95H8vi1ZLnag3UaCgXBQR06Dy0gz
PnAwG4hj0Tz0/Cxn0FMQYr1ZxgeTgSdhtJblh5TxfSsjFEXLWYguB+KBgoryMtK
Z8Q6B9jtVLNjAAcowjpyhFuqZsMk4diKco6xx7g0aen8Wc0oapIgOtifZ2YLHzk7
zh0vQ0MHLiFKIBUyBQWrtPrhp1k6hBwuCBCjsDYSbrFvtroeDem0ZLz5eBd79hJo
3J2uN7kQHjKEPmCAPmpqzPBRbLrzc+C77cBjImtOzQXZC7pRmwqUUKfC6Hht9pz8
Aanfaa06H9z8ShHB0Gew0hYf12M8mmx1Hb2FEla5VsU8knQ07hRav91P6Q5+MPN7
P3vF/fXy2RpdigEEo2PirlQ9DnyrtP60voy/31QNP7ntj5tic2ywV0+QAn40Ex/8
ewy5zUJAe9Z8qGsExZh8opjsjoXCThnpcU43vgYwHLPgcSVxodhMrKA42YS4xPEg
v1wU4VpTbjE/Xx4oNKWiC7ppJsceDIDrT2iNIiri1hjy6qVgsNh2ViCMAyIxhQK
a8kpg0R7EF4ChPkP2SZ01qMgju7IIt0zch4fLxel3rKR9AKKH1xi+rXsovti34k
hbxaQCESEHIkkGgXW3Pi6o47N3rvTCZMfQUOVBMMyAbxVykaE44kdLp33w525g7ms

```

HXo6I6BV5pIP5LzKgqC+grcFKas1HNgx/Ulc0xdYR87eB0pjrvu8Km0AabzMqaIU
c2MaZiZx1p081hpkwxq49kE/gqzRUeTm2gCS1piR6qEvDuUjetmeCaBH+b4dvVRU
8J6orG0hKFp5yNv8pTxmVYHl05JcjfQ0enjbCn1Vt14ro+yuYcpBhjYlHjJN0sK
yd3ceuRRKbW0i50TbK3TwG19I+1JnUrTq6rYKk/FUanQ35DWjpPavdhBcTDgSWQ
zqJJlQ/ohh14T1KMvzC7hVHiAWOIGAn1kgHF0I5uUoz6exhrN+iFg7fkCkxJAjsq
KlT6lXlv/eLwmJ9yYcbYAlU9DfJISIBScD0AmY45Q1Y3rQsfHPSB37Cjam5M1eQY
q3cc1lbskiaMe0SEHHdxdoFyTTN5gDCHMOUBgTsFn6nr+LZVj15xECpjxgTigBCu
Da7i6F1c0yCPDNX/ktG46PFzMCvov+IisDm3E1GMkH7bjQeIpjJ50zyzAlNKhpsL
wtr5PSW66oTqeF64d0egwLJDnvoa8NzN5hMzD++Gy2YkijQ/WeYhkWTDQMch7Sq
ks0kVKvNzx1T8nfC0/QDU6a8E+UnejBAQi6wS1BU5nQ1B3Xiy6Cda76PNppslyjp
aY0hifDuxfhLfu18jftimC0m8WkX6iGtobaemLcq6hi1rAN5c2GwaNu2uYPcKMo9
iSTTGAfgHHbfp5LsZy7J6bUBRG3lWrp16zFJ9vhNWJ3Y9ppk0eMEsmwrINNAu+S
a0+Kx6Qae1b2cT7W6CFMUgF15zsxyXt5MHDLIPsjaRb1C613ajjLeirCT2p82U19
zPqw7+YxLEp5RfAQRUJ46N41cr09mr5Jzf9EyFqZMPXjwhK8Bn7qSHM+3lTk0qWv
QWRDc84Nh54ZV267GbL1VK+Y2IzmDGu/gOs8FWo8M0tiMh0BDjPVO+H78yJjV3dk
V+SkImA90VxjMCjdd70PUDYpzaTKfs+7D+UH7MCGFUVj7aHwYFaapX3f5H8ZCoy
N2sa2UQ30240J62YV9h0FunyciS0rv58c5JwW0/clMEUy6uh6rEcOGTi0+glS+I+
M1W8R1srDKScPyJ90l2V0tvFMqkIGKce1E7k/Gwkkx1zT8o0SEKJt+XQk7p8APwu
dkeH0UyqxoPrbKjhdKwzaK8+8e9yDY0PYWxRATikaXqEZtJ3M2Yy/KVY/epiFPf
5k+INNrdLe57zvP1Kg0c0Nr5mq12QT2jcr2rdGEWM0/1oNLlesmKqm7sCxp9Yky4
3pagPWZ41X2CHJ06xJ/fsn1IUNTBYPdzSHtg7DNd+AWVkMpvge/JwZaRjoakoRAn
PrSvDF7QrLu2hKNTq2L+ak0LAULqET5wMRoih/h4PWf5JNziJDSHnmNY3jmR+e7K
rW0SeczSjg/3dwx0Z2j148TjPqQa1eBZ9/cakgSaxY4nsH4jB1m5VHRyCNmCVMNk
iykfrVnCdEIYIRI7gdECv06yGKczwXTZtHADQC0BkpzrLF80zQF9wKwTG7x/nGki
lJR0WcwUtZyUI6e5sT92lPG2Q0Q0pcAtqFmz3/GMxrT/18L5GHIM6ynAsqJ6JH16
J57gixKv8spUkYT2bzJQWbSdq92fp+o1wM/AAVurRq0hq0tVFuAnpK/xWzcDB0/i
D11Y1BU3GUK0Yya2RFHA24hmDJdfPgT/7DiCG13y64EQ3WUo8vz7KnYp2UKSLqAn
N3/2Vx0wpnuE7SwMUCQP1Kz+Q3fZZZkKtgW739NT50V63zPb1vzWMBUjV+KYByoF
hp7RNLon0UKRGy5/vX88/DDyoSs2D0i2NZb/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
hkiG9w0BBwGgggl1BIIJcU1JTUUtVmVyc2lrbjogMS4wDQpTdWJqZWNo0iBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtYmFzZWxpbmUtcmVwbHkNCK1lc3NhZ2Ut
SUQ6IDxzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtYmFzZWxpbmUtcmVwbHlA
ZXhhbXBsZT4NCkZybz06IEFsaWNlIDxhbG1jZUBzbWltZS5leGFtcGx1Pg0KVG86
IEJvYiA8Ym9iQHNTaW11LmV4YW1wbGU+DQpEYXRlOiBTYXQsIDlwIEZlYiAyMDIx
IDEyOjE1AyIC0wNTAwDQpVc2VyLUFnZW50OiBTYW1wbGUgTVVBIFFlcnNpb24g
MS4wDQpJbi1SZXBseS1UbzogPHNTaW11LXNpZ25lZC1lbmMtY29tcGxleC1ocC1i
YXNlbg1uZUBleGFtcGx1Pg0KUmVmZXJlbmNlczogPHNTaW11LXNpZ25lZC1lbmMt
Y29tcGxleC1ocC1iYXNlbg1uZUBleGFtcGx1Pg0KSFAAtT3V0ZXI6IFN1YmplY3Q6
IFSul15dDQpIUC1PdXRlcjogTWVzc2FnZS1JRDoNCiA8c21pbWUtc2lnbmVklWVu
Yy1jb21wbGV4LWwhLWJhc2VsaW5lLXJlcGx5QGV4YW1wbGU+DQpIUC1PdXRlcjog
RnJvbTogQWxpY2UgPGFsaWNlQHNTaW11LmV4YW1wbGU+DQpIUC1PdXRlcjogVG86
IEJvYiA8Ym9iQHNTaW11LmV4YW1wbGU+DQpIUC1PdXRlcjogRGF0ZTogU2F0LCAy
MCMGZWIgMjAyMSAxMjoxNTowMiAtMDUwMA0KSFAAtT3V0ZXI6IFVzZXItQWdlbnQ6
IFNhbXBsZSBVUEgVmVyc2lrbjogLjANCKhQLU91dGVyOg0KIE1uLVJlcGx5LVRv
OiA8c21pbWUtc2lnbmVklWVuYy1jb21wbGV4LWwhLWJhc2VsaW5lQGV4YW1wbGU+

```

Page 174

```

MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQKKEwRJ
RVRGMREwDwYDVQKLEwhMQU1QUyBXRzEXMBUGA1UEAxMQ0WxpY2UgTG92ZWxhY2Uw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgWPK2af0+Stijs
NOR8K/hN8D+1078oullsk4ASvSwjsCNo7sHUA4xQU15J06VqY18LANw0Rjrc9BaX
4MguzsbFXBe6uFh1mVpXmFxpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4D
xMI07XYNFUE0ls/gkUP2Gxyzms02kaYWTut3SryCqeHEFbZFk4urMk4xrIJC3Cz
WruS2Q0FhbBlfkgKN5wXVgkWFfi0ucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog891
9MxKI9H6l4KuElnAtJ7BtZcs17dUy9u9C0gEyKriVokFQgqQ7XNDU+r3Se0Wwks7
AgMBAAgja8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCMCGSAFlAwIB
MAEwHgYDVR0RBBCwFYETWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSAUEDDAKBggr
BgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYDVR00BBYEFLv2zLIthQYSHJeuKWqQ
ENMgZmZzMB8GA1UdIwQYMBAAfJEwjnwHFwYn8QkoZTYaZxxodvRZMA0GCSqGSIb3
DQEBDQUAA4IBAQBziaI2p86poGkd/4Kkk0HG25nY/0eNARD6/oF0/sYonX2doiz
cGMk53riugAocCn5zbzhW/JVdYn30UxfyrZlRAzEf7GHqgB/Nyj0ad3pdpVYeDh4
ciNKjbs+aEoTWgAkoqENT1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqGJdGf
8L1zLFXBuo2zL3HR+M9CDr40pq2JckzP0Qhp7poIccGE6I9Tsg+Rr0A9iCQsPn1+
Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz0KypyQ3eoZ6EPazXqMyHAVcsm0GI
364IOA0b8PSrJNTjh+AQJ5QfH+0e7NSzNnEmMYICADCCafwCAQEwbDBVMQ0wCwYD
VQKKEwRJRVGMREwDwYDVQKLEwhMQU1QUyBXRzEXMC8GA1UEAxMoU2FtcGx1IExB
TVBTIFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69Phq
zpq1zALBglghkgBZQMEAgGgATAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBWw
CSqGSIb3DQEJBTEPFw0yMTAyMjAxNzE1MDJhMjA0MDA0MDA0MDA0MDA0MDA0MDA0
S+1eHkWHxwhKH54Bov1Mmxx6FJnth3m1aP2z+DANBgkqhkiG9w0BAQEFAAQCAQAF
sIpGZtBsgrjVl9N6sQu/kU0dnbGSU9JKm6bXL+1vef+4jDckomzjYI5A1sKXxfSk
nBWwgEsEv9V03839X1gMAUc09cx1wwcg4LAUEDWgscC/iNJQo6Xm8fTs8yBMiM/+
0yMrreXIGeXR2ikTG5ub9mPrnx0xaeFDnx6HMTh6jGmIodN2BAPIW2KahYYS0BQZ
g74NYeBJX1euT3/ZUqLmupQ0bephgj14pNcslj0qPSRmBf8pZv/9tzY0uSj5CwK4
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

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcELEQVR42uVT0xbA
MAgS739nO3TpRw20dqpbfARQej0ywiwYnCtkDKnbcLk66sq1T+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
BAoTBElFVEYxETAPBgNVBAsTCExBTBtIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIElnRnRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBADQPKIuG1Bh1GBvHWV+5XhSHz6YEXDs0Ghxo
lwaqsHHut09RMi+VovM7fasvln4F4tpKCfYbV5kAkFrNFB7fY2thHH58YpkABzF4
oA0kDcWHqVho/AVV1n0Kf7kp1DCR0uPfibSgWjJQcsRARuwB0aRAkUMJK19EcZgX
KWz54wcwKZkcKgn2SxhWSea6HqhB1no0Q0Iexgz14LdEW1cZWkQYfWZ6VAY8r5tp
h0txgujzFUFuYLebbKS8LC2G2jurs+ktsSGDwnLz0qSeQyN17r1DnEC+aQMmTsRI
S0DMwKAb/P3z5u6jk3Ryu2HRBIZsTsJhIhgkuoZqEFG5/ZS91I0wggGEAgEAMGww
VTENMAAsGA1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQUU1QUYBSU0EGQ2VydG1maWNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEGgEAR0Pqih31TIW6ROhwnDGcMz2i
5f9z+HpFsjLj6EJ5LU3DXhsdT+6XcF2fqtCJUjvIggVBj/5ixRYR1wPzypgz/QI5
MYBi2hrr6ch/tWyUDSV5R2FKLD58u5ZLlt5KKW6oyW3L30zB+h11NEaIjUFyMSJm
Up6/JEPDeJwg3fAygH9XHUXE1ocTgWuVyVqFsyzAja3S2cvU0vm6smEGdPYcBxc

```

Lr1zALPmct3Dikn/pTZizIDA1zQR78mwbPYJ2mJsLYxGAjoPhEh5X8y9PrzJNGs0
gQW1UtLI9dDSjrijLV1vKWWaV2coMcsXxQiLAVoVWDJxjEDM2UoY2ymQAX39HzCC
HR4GCSqGSiB3DQEHATAdBgIghkgBZQMEAQIEEGhYozFbuzK33IcI4CwfeAuAghzw
eiwNum6ghKAi3x/wM+7u99irte7m5KiQwuC/6W88BVZk+Xu8rGHeHg18Py8Sdfxx
e0MvM1Bdc8NwsUAJK4PphSZk8FPKczvKF7kV1+XzBTQRflesQido0IOKfLHDBMS
NKbvK8haTRiB/4EBAPH2C7evfTYfKeN6Wd7GKkzph058dB8t9ABpJP+mCG+hvuhv
v3iLc+oYLFfCbaI0c4//GUX0G1a0209Y96m463rYQyfneK1KN29UysTC4ziEatgw
PhZPf3kjleEaSfxjicrEjR6d7kT1RDhEyH4Q0exadosQYTXo+Fg/2m2NZc539z0Sx
DXSy4eyDDI85wWQIsLQ2fh599Vhag0tXk4+ElCzdSy+UqXwmX8hMBHZoWU0j65No
PgWcZQ4IT7qctJd9NDBi3a3R60FYJSPjNEu1TmW6kEQ1E+I0Pt1xiqTDDJu9odKt
uQzHsQBEG+kDFTvtPIu30cZniFN1Xhm4cc1izMdc+fvwom9SX18R3fik3zFb0ZbT
C+/DQWjxrjsbCduk0fXqI1o72SQwgLuHDPfs2Kzm0bHrM10RN/RAhKKem2Kb7s7g
lPBbmp9zkvErc85RU06EXRsI5SVGOIfpC6B49tXJhr1k8Dmm9v+vsQytrco+jX4
H4S138a+9o6hJBQT0912hBdD0g/q80z8a1V40hGw1R4H50jMVX1EJp+ksfIS2HV1
/HVEe6BNkxhD6q9ti7Lg3dD0Dkh8meLgKaXirmSC/IDwY4IzVepKWnENn5iMemf3
8/nZ6g8m7xph0riq9NLXLqecLqQrhJfUEvBtxw0bm+0xZGkPel/5ib941dSNKexk
DZ2cq4gAifNoAWu9q9S9bz7+ODD68hRdoQQuUvDyV2FzB6cy0BeoB2tWLnkn13FN
rYiqz/1S76XP9duGIf5rmb4rhfAJlnrvKipWfGJ5cUSm641Dr63ou+Ha0MaXf7wS
p3Mm594E+vI9Z0ri2A5bmbEV3dC1121YFX5xfbU346akePA9V/KzkHPNji0k0j9
2RUVtRA5FmXizcTri2rdY38uIEvB0j7jNLzGERG6F/li40Em7SiwovzvUuVsSSON
tswwOz2xkJb+WaTc6obJCWycUUm9Dfdmcl+SGwCMf+i6zMgCNUf4TBuLw0HBpCdo
zXbBmbiBRn9UD0aZkn1xw0VevKq0RyPV0/u9zRcSgHzSPM5KASpL0417prcfZhL4
FcrmpPdisDWYS3WN67eyXyWtM2aM7LnoU15kPNYlwBe7qIaxwch8i9k0KBVcU52gY
mfJnMP8okcU0FauGPZBN1M96/M35mrj/IRiQJod0xM0XaqJlZu3A8T1RLfaGnleo
JZ+a5r1Rx2gJ5/QMUv5yd+Bsv67DYU21/TEtveLnfJmm2/3kFN3bmHKb2ibpkIMP
PNF9LWD+7D3qr1vzKl+jp3eLYsskDs/i7cd+MIZ+z4T3I8WAmpBP75LnSHk/V6rY
nWyC3MaB40xKWBsu7iURIv+hoD8wqGenoiG4NsEPNsuhyuPz0BVPkEFm1aVh8XzZ
qbg4yh7g3I1X1JPMW4QChsPo6lKOUPhaqExZucEgKQye70HA7u1DI0smiUZBNSz6
Mc6HqK031U7akhQrKNZj0I7pqr2CK9pQVVUW66DYSV6wI/Ms7mnr04G3H17Nvt2Q
JD0pLEGGEBdCt2SibcXxrRglS9CWPrV2+1bjG6tgwDRwq/lFaFQMt16SHB6z22U8
ZLmlk3Awi8m21EoEiIMJwandgQ8KURItgba2XRgiuE7R0b0XqODRT15+au9At6b5
RP8NZ6qlpmIEVT6bCZ1oyQbMT1pPpdM6FXW4fGZzQI9kd73gbhg3kMnqmEuxqLvV
e6jsqTr1a7BH2vYTMFQXfqYSoof6WTac7IqmC7Wcu7Ydkb1liCJ/Ne4FJ0mlx1Sq
9Poz/zpgjgbTLQ5QLjvMqkdVJAQpQa0QWh4ht0SKgrMbWbybZHoEYTHwaXudlw6h
TmaPxrDL1bFYRPF5l35e9VoHufhjE9wAEwU08adShmvxPbGzYSSWCU20zQ6F5GdE
07L/OwtF1+f7b95uv8M2FT4HDNPRK8LrdqvFYow6++1/2QsEgGZny/lT0zbcZ18K
HaGT3rheElAD2sr6vvCALasiXWmJ15cZfpn0rYQS9V+cYo2X+wi7vZ4SWQsGhoK2
yLMK+M3V2Et/4gfsCKN5uBg4TtgHSFYn1TQuEvTjC1iBPZTL+JZdi5YhBhkhSNwI
8Ka808TE7aYrKB1U2SLT3RaTFU0NP7uOdCSxTudwShB6yeBPYSDcv8U+CYN1zuwo
GAR6Db9leIE5Wjzd4+1KcP5mQ9ht9X11qqqobfGxSCfzLLkSoJ9PvBwNoFn1FwPy
08G1Am/rJNZI8VKNILQhGfiEazum0lmE0IiI/0GxT6oqQrX+0KQfmqAUG20VMXEG
LQRRu9W2QzX1fcF0ldjzM1PjtwGpsM5so+yLfv/vKiFnZfQUgUho1Bq/cJX2ISy5
TbmljK7/zCwzGoBjQrJxykFGD1xHZwWY3TEhpQoewduLE1nX31ZtHBHvV6bt2CMD
ld639Jczp5QSAq4yGtZjZYUqHqYGIgNqov8GyLfiNaLUhneoj02V41SL1kRISf5U
EYfjDYXv/MSorcMCi0x8/B+0qxtyd0R05QE1RZnSftQ+appE8XKLVPcFzQ8x+P9g
1yW/+CumfKFKZakp12qpIIPJ6kAe7Ig0Zd3uFgd6FtXbVMUFHqBHGN7ZFC0JwlhJ
NQBjvZbqAymfdlcsDgqAm6e3Fi1uhg7i29iuryC15icudXoGhdzR41vvqJu/hIjB
tvNW23j19JZuJtu7IjN/J6eqw5nu4UFG5LlhiqjsKx16Ae2r2kK8N14EZ9hMhMv+
UOMldoHTno6dsbXkCA0HI5+Uy5ZbweOLOP0gi5ZemoyECyWJTWsCLd22N+EHbdx+
0+G/WAX9y2av+0VXTPqCs6PacoeCg7Dbah0hp/5Amw36ADIWYKjsa6jUFdZtxi12
KDqY69q6dCZm/Ctfn6FVOPhft/jh14bqGlmRTy7YtxHM8aqoC3bPz4/x9/WuffQG
4zhj8TXva4QHmQnJ/bhLemNz4b6SJWnu1NcDvkTetwUrcI6X6/UWpMR0LqKmJWbH
ZfC2siIAPZRWsovSNbq4VENFWiP3NUwUUA0AHVZklDg/sNJxbiZvAUBCrMsIDK1S
4RuMY5M//5Zc7AyFiCfmUSn/l9G/Jhxoc6jQhyZQGAK+e0P2WdCrybn4dPeNP2Cv
czxU90kFJwnyre8eN37GL46o7cECX33d60hgL4hPB1wYowczrW+VUDNUbpU1RTGn
Rj+rchVHRgEVjEgSasFb3S5Lb0aY75Wy/pOumQYxc/5Lm4IeF+i2sJuMvJQxuPbcx
gw/J0y0H3VZX0cLbin6GEqC0rkANi3thkU/Ljt0UzXHm5vkmfANXMvXQMKuK/gXW
UP/W2924d7VWajoidXXE1S8XHE1lhrT4xkxZ+3Lx8oB8AycEUw8AeGfXx8rd0sri

VVeG3x/Yi5Prvr1gJxFeNv6Sbwq2RDLeP/GJBxIY+tcuTy4Pd7CtBmokIOHCuYsB
q1KR6WuhB8/rdfcUa9oooJUpr2nB6EToNAUvNRFdhqzWvvuxT4l4CurGUwc7pM3w
PFaeW5xxadBIDTehRXmoUc4b1fa7BAfM9H0IH3r968njQUwFC2XgUh7wpfOAD9NJ
yYUMxfy8RRRwmBwBMA5ja0SZr0myCvEHkK2L0hFFhKLFtw1tocNVP3unRY9UjrgE
T+FAgqqhZEWgPvaKJFDz17la/T9DVfvpXyTAEX2n1jvL2UYpyV+0bjP1/7cEnvTD
Q/KvrQMsZNS8Ams2VZiqQfrV9odGf+OXG00cCXNdbWJtRC8TV4+mSnfP07f3dHvs
f0keN7ArJmiZIUevxsgQe1mCFGp6+L4/XPa1GV6LzIUy7kS4HNW7gpn81DYw6Jwv
TMwvJ5gUJw7cAV4zm+8Syx3IdhyT844J4e8s1nxiBwYDSgfMDa3tJVxWZk7CVaFQ
lSH2e3j7h1WDL2gZ0BZemstT/snE3UgSlQY0y39HohGIffuwVxKMkcRpYk1ADHU8
GB8wfDAsSDQ0s452ucbdaY1k6iG2XxjBiovNUIJs/IYgj3n+Lq3MH1WpkRgDRj8D
4vd59gm9YzXa2lriellU2I+qdxTf94P7QhwQitrsvmPmxA5NAG9ola6bXAvUJqi10
q0wr1B7l0tiaHx1KIHQEVdQB2rTSNZQ5EtcEgAYGs/Lh3FL/pm4Rcv+DrBuFormk
YVTElDSNesh8Q2EmOPD8zaUU86bYboz0bDtA6Ry/H7RpYzirBr1ymwvGSeCnLSnW
KcbbXS2ntv5ohU/Ksn27t5pJJ1n7bVbTrwoeJ2J4kev54vbjupoR2am97I2Gz1cs
G+1K8vJ5L/ECkdZQx+4BU/5a5be3eMe5TpNDmMfT0WRkSC5CLfj1/YqXAIjmxVDo
CJD25BaX0SwSooHr17hQEvax9oAEjgsG1xJTYU0C9gEUF6abW9hravxxEYgWvu+z
11q0rwhWavVshkk07DPjpcZP6FOvsEJNLfmw+0b9Rc0paQUJh9xpW7avQSkeQ/hk
K7LElCxUXZJYGEKlu20u1vuczDFrJob3xPn/3DE+vfopaQl1XFxFhdKfTk630JX7
3gouMVNfmdBgnsiIoe7CutNayFoNiCeSbUNDPs0FNiWR/PGiwUsF0p0s2fK64yh1
dCwHijMoBLN39jj+LJSnzMpBB+lxixqTAFrcBTc29CDK94V0ACLHs9fhUdMmWMu6q
Ms9eTzWZ7cHZpPZTVNnXlVIKx/NfKf1/QMr9ZYHX5/sxxMXNjjisM4zvnxvysaf
z0B1YzVgKdc47IvsXYuvN6+jZXoYzNZN65yEKu6ZS51TpOyvl+WyA3JWYGm4EZ/E
IIJhnxhm1hJfD18GztEvTzLkqY183BkxPdsi01j4i23uxWiHx6WBUUph8hcjq7+f
X0KdAA/ObVcE1QQW8yYbKagulN+WJDU2LENgPeNbX217JDgmWgX0pZht/fIzBucD
Et6r+leFWvbezdnANcj0JeqRshjz/wwaz9u7gckF9YBR1XEQNM8fePXeYGNzn1bZ
qQYyXivDvFmIgxwebiLTyr140A4y6ZmbQPut9ne26a5r+tmzpD6/Ehl6EaH4z2Yg
IYIGnwRy3Ri8u7AuAZTEvv4hzsUj7MpIV35mbQNKpKslDgfd1jFsWAlLo8SJ25iA
WvKuYJAXFqBkksL0ZIMuG370/HjVHESyaahCBY5M2I+Bb1ReyH4dxdZB4kdWBUJW
jwoN964SEpypk+tp90R1IBHpIuu+Oxvg8iZri8JG8sWjqF01LSSdG5V9An3/nX1P
hpGa7sFpQUIxRuV3RH8VuhXVRqeu3M1ciX53W+Iyuonjlv82HvS9bN44uE3s02h
PT0N0gPZMqG9Letybzt78iwxS1qQ176oMDFfx1iHS8n5y1nSkzzedvnGNKz1Hqdf
V3Qc1zBW6T8mPrqGp95uBTBTDSC6EPFZ5QG7E8fw+8d8GJjCHQah/DHeEo3fRQAL4
G0z+KLHmkjockZTWVLTVw2sHmo3k0wCk0TSUEjjfSQE2n7Q0ds0XQLaAMYvyfw5x
RGfPCPyjMSeZxosnGftHp3u6Z1A8QW2CV/WLYai+Qy22z5jvhN+duvQbEI+6p4RU
BMdDZH4xGF06aPfpeD5f0eH9vsXoRIUG9TUB1xZ3yYLRpQh+AXjmEWzG7b2pa5Zt
fNC6J0c9aKvdLY+HMtdQ35Gq+wYVMMyZLDRDcs9sDnzubxP5loaePKahPARYhU9
07/cKG0AHZP12ffWGC0Xr9ay0T41LVL+Q8TM5syZ6c1ZAanK6nDCWf2iksIrkQQt
/ko3R8s401/ajye3AW9lWrW5eUOE6/dF41Ec+znHd8GGk9wH/rG6uVeet1TfsrkZ
004v8Sy/bgs/KFDZH9p1Tw7skDdF13ER5202JrVgcBrVTTjrsW1PIFb6lFCyoguF
z0j0aBRgGkd13IhezPlrr8t1fPppZvUKCYxgv/JPoRAXnTrjTtGv6z0R6P0V0vZ/
MZBPDnm0lPa1mFidN7lRAmI0VGhgyY/1+tWKWdBbeV4Nto0heRXZgqGYK57qTkMS
1Cg1YPADZvwyVcGtNh0+qVwvjuIYhRSL+kthY6pxDRrFwerzyOw8wGCJXp13Swm
8Tjip93eMjniZ6k8e187E2iW5ykgZWheSrKjQKFVj/zUjbxwiwfw9W1TUY160+Fu
Nkm+qWTz0lhxmm4PoKSTeTn3uMBaFh25Vc463RGTiBdj43Mtm4/SMWfKEJ93kFgC
bISYo3n3MfXJZs0/AuCDnHMvy1DmpdsG+zKbR5+YS+RgiK4Vf+i418xempcJUfP7
zPlNzSrRt0lncnHij1mWSmQuSR7nAOQtqYWdsasx52Jk8o0XPdixWcutEQVc5vEM
MdaYHqvy/cRXBC3tm0B/JKnbdO+OzaHgUcgUW4GJyKxf3iRoK5CIZlBdW88L8rXh
K+xxjyTes9alqza9rFB/YaB0Ziz7PCZ8mgYIfe+B1DH23KfXtaZVLAQ9CQFF09vX
3Ydu5U2HSCcSmt/+KcWWP5B8RVg8a8ycoF/ZEETp72Uafx6FFKbji1LuL0Ir7JqJ
Vkn/9wjQ+NV0zDN4+bYI9kPFi1LzqTE953xLm4UfBhGFStMeGqCmdK+K0YcA4iZx
MxIhLDtCbOrKsPVxguaom7iDnNkL8klJigpw5qr9SuHv8cTcYpmgY/KlxDcDcV8R
1V5WYamz6KPwdfh1BiigRU6dHBrvNY+fBHEV18Pe1Tqm5TWD/ryP/KebvIsLgQhf
VVF1sWZHB5ZSTFiGmXU088isDjJSjtQ27m0Ux5JS07G1U7RTK9N1ZQwmqg90rXrM
EntLIIfVAGwTg10cX8ZV1IwojAPTBDfYLeYjzDdkZFR6c8pKDtrKqx1ExdUrmj4E
c0gIjbnnnwpgNbQXhfYU25F6opEipOCsTQ/Hh0eQjpbwnqaDsght67NNouKMWco+
T1gKXuaEF5VFMPeIo9YTtWOPrtcqtSmulle9vP5jA6QKn0+1zX69ytxwMUy3fe4S0
FefRP6E3taViJv10oWqifzJtyNcsBLn13619yx0ug5WBvA8UKWXLafF5BR1ZYMJp
KG+hrREH2o0cojLooFg182H5bJYIqiCnv8pb124aghXsMWap0t6JcQjjoG66Ni9e

```
JrfixhUMDKqBMHvhKTIocysMLjAZs3fUlkZyByexP4/DceJ2YLMd0tTD50Zx15av
kh9jGBrKYDadsGfunLFFyi+aDhDtC3I4kDYXWE4dLUvVwjJn31sBz7qzICYfly8w
20gZy7Ao63BHTHX3tGjNer2I4Z5HdYlv3NeCIXAKjcFVuWERF300i1r54nfcboVy
p5HVP4ZYZGKqcTaXNTuuCtkTBwYt3SBXe/dbcn7PCwkgW9Q2uwQk2z4/+3Frq4YP
8lcjwimFT01Q0DAaQNZaQAzMk00AAxLDmxZLQdN6NAwgcF0ieoG69uu5fgZG00NY
qQyP4aWoY7WfX11AeVoDiuWcl+N5WMviK9uBbI+gTem3AiE70dr3roxFlHcArQS9
UZHGS50tTI/4xf5qerK/B9rkU750sQKdvbAJZkXaxg0so1r4qpSRivsHGfBTZjP8
00H+7T2VRaBQSB8vGTc0NqmzhvWrkf2HUswPFjLtlcWszbHgnhusb1dOPPwkr8DD
CjElwQcg0m+6WPQqIH3QBxt+a0ndZ4kHEdurcjwa/AcVHykc/aR8mR0+bP7KRsv7
SVG+hD6h0L2cBVL3HCWF7z/K4f+YSQ9KTF/efP/Kbr2o98zrQ1IhKDIPZ8sJVPVz
WcK+GU0JUDreuVmVnWrvDM3Pk2/3K1/23xGzfDF0S/gF90PHX1jH/KTnz0KHQxFE
sTNJox/80sTqIsuTiW3b16bG5KAGgeiLWSAzU07e0U5goB9QWT+QsBlMmdumGhzF
jQFGmNL0aaxJa1U/kq6T2NoiLetQPJDEdr6UHloASF/mZtbPlQlgyKxbs3y468i
tVQWEHyePSzvIYfknfnCeeJtQNaABfICfYBedlzxk4zuyRUSlrenW0RCuCMuIOQL
uRXdnuB2aC3Gnb1KVcWilR02C+06Hh0dXqDNwWSQjku0o2mhbCZ5TAL87GzVsdI6
9FgMsFD4GyH3LnHQDr9jjFqhbARBWqhCJoy62ES8L1Lg3E41b1/TEeP6c1IJ54uz
j3H3nhzCpEUa7w7jc324lioLT9QtiWnKSE40kNarGwxGq+lJxAZ3qafimRe/DGC0
ysAysJQTLN4MgsAr1RDvnXY+UD/J2HrZZLYguTLc6Qz8NclJ00eHYGec8hbWw4Ji
OvpVnpqSKi6aW9atAW0NoQ0c6YJqetNab1lSWXSYLZTwZnf3iSlgC5x2k2zrQ0kv
kipyixPl+BK0cP2gzXZihacodnfl8QJVZuNdCzfM31skCehMV4moXBmQe0GU/z+J
y2jFdZk3APNq8Jc0fDpqtGedriwBRnmG8RysfS5vaa2pdZdtpLb+TK90yGcDBLb9
2anQNqnaFUxZ4AKY5j8C7+eTiWt5bfUtN9zqVUcMxcjpPitaldyG0xMrXMThftq6
PaUFS6pEnw3RurZ67gp0zBia+ajmwFj09LqPC95JH+PJttnrztgc3B4eD7xuWiW4
AWybutvWGY9bEzwNHR6Jn2XMx4T5Cad0XGzid0JcoIu+/SpME1fWLBnr9H9hCC+W
drz/lwkYij0vW6RPdsp2Go10W8/DXRdcscs32WZyfr1RZ9S+BfJs01hQmVh8cs15
/aQhCPIxtmWQUKXHCzWwKI6J7LJyugfpImWGL3Xt9dvwIz62Ma3AECrPx3Ss0LMA
y5Mb031ft3FX0D+ZQs6kxcS/E7NfM2bch3BjY/3j0k5b/YxZeUxvXAWJ+W611hva
D2fyDbAfCZTtIJGec1vx0/7MxzDyYnLuFavEPHh0YWB5S4tbz/2nWQ23SzoWazo3
s4RI03aPl9ogTraNAtkrB0BPgxdFzUCBAef7guX816wSPeW72Iess7TUyt1TK9wV
oC01TEfuggTR0FX7/VGfduLQCjI/8xvfQguvYDt4NwUAdeIu70a5Tn01D0xPioz8
wwBrX0hzXEd1oZ4Xmc9rxqdCsQ5s7bI7M/0FpSs53nuQrLZDqTrJMI+rW4jhIrb/
xJmDE2/0i6fUy1eZWMPoDDcD20m7S5vb0quhsuyV8RbiPXnoCJsNMbJIIlotkVMR
5yEhltLdD33cwnqKKqWcHKU05fWtegP+ZIVxIG226U5itJbiU+uj0TUZsbCu52uI
9RQp3Q8gMwkQ3PAaXqHmknVAUeTKSU34RV9kn/r1n+1mFC49ribsHUVaPz1G1sMg
Cg3rt243Q2zMmdwdokmUT5euga4Abw9xhTRgoSCEGoQhLMW1P03ZVs+Nmr5QQW71
ITfHV2UGUm/F+b6iZWA+TQ8RGHTVzHWUSLJuCqpcFxxY/ezzeB0iappZTKGN2E9
77owuDPHV8CyTQvJs+v2YcP+rgBXtCzIPxVjz0v/mfNvo7fXo6y+709LXj6hhAro
xBPAaVxvnB395oaa+1ZMCD0zxmSynpMj1qP0pnwYdvGsFeUFWZa2004gveQ2qMc1
r6WYj/48a7roSpjBTI+ZfQ/5EnkdLBJ0DoXi1zncQYPnH19VdXDuucegLLkEHf7W
dhiRCnLWYwqM9o5+WwAFrUq7IQZy+g5Ar93Ymwitawv7XsMw2SIEr0Nisf1r23Ai
0qFSKIh0aJcncNFAgcV9fC6/m66B7gGba5y4SA0qm7qWpPuVAZvc/k041v2gAPL6
GpZyX492SC9oN3d0JZELsQ==
```

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"

MIIUrgYJKoZIhvcNAQcCoIIUnzCCFJsCAQExDTALBg1ghkgBZQMEAgEwggrXBgkq
hkiG9w0BBWgGgggIBIIKxE1JTUUtVmYyc2lvbjoGMS4wDQpTdWJqZWNoBzBwlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtatYmFzZWxpbmUtbgdJLXJwBA0KTWVzc2Fn
ZS1JRDoNCiA8c21pbWUtc2lnbmVklWVUyY1jb21wbGV4LWhwLWJhc2VsaW5lLWxn
```

Page 181

```

WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExB
TVBTIFdHMRcwFQYDVQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAJqVKfLwLajj+gBUCfkacKTg8cc20tJ9ZSed6U3jUoi
ZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbmadXPmrszyidmbuZmOpB5voVQfiLYy3i
0x7Y0QzXr16udP07k0sV+UdSNRFxrfKeoQEFXg0aGdmnx40G/e3p1fIKM0dPzZLo
0AJF5m500xzXPL74zFCWp2f1ZkuE4A6141koaZXCN5XL7wWTLMLenF9Byb5ksKqU
uqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWzB2zNS20F+XIVnzRG5DeoULq8
v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAAaOBrzCBrdAMBgNV
HRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNh
bGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB
/wQEAWIFIDAdBgNVHQ4EFgQUo1NB1UQ8gCkVfAEj80e0r83zdw8wHwYDVR0jBBgw
FoAUKTC0fAcXDKfxCSHlNhpHGHg29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCC
sTKcFqQMPTryujRGzJdYA+R9eBAuDLsatbtKt14FzkgRy0g31/+Cw7H8e30iLrPI
F1WN1qjHrjg0yIs5AQ/hgxLvLir3hEUUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMG
HjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7FOD7PFB5v94M527
4XYwW2W4uKgd7QGnUZROSvSYkGiWDp1JhqXwfDz8A0enITGXnoEkAFvviCqh64P
1hIEMorj36pgL19oWZD6YrzSWHUz1F00juyu0fQsqm6hvrDTqNpHNZ015f0URza1
SkCvi9GfMNUPoVgwgGPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmgnXMA0G
CSqGSIb3DQEBDQUAMFUDALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdH
MTEwLWYDVQDEYhTYW1wbGUgTEFNUFMgU1NBIEIENlcnRpZmljYXRpb24gQXV0aG9y
aXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQK
EwRJRVRGMREwDwYDVQQLLEwhMQU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxh
Y2UwgGgiMA0GCSqGSIb3DQEBQUAA4IBDwAwggEKAoIBAQC09InoWDgWPK2af0+S
tijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHUA4xQUl5J06VqY18LANw0Rjrc
9BaX4MguzsbfXBe6uFh1mVpXmFSpUBYQ+950MFz/evPgP96wV+z4TtAwW2Z34rT
iz4DxMI07XYNFUE0ls/gkUP2Gxzyms02kaYWTut3SryCqeHEfBzFk4urMk4xrIJ
C3CzWruS2Q0FHBBlfkgKN5wXVgkWFfi0ucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfo
g8919MxKI9H614KuElNAtJ7BtZcs17dUy9u9C0gEykRiVokFQgqQ7XNDU+r3Se0W
wks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAAGCmCGSAF1
AwIBMAEwHgYDVR0RBBCwFYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHUEDDAK
BggrBgEFBQcDBDA0BgNVHQ8BAf8EBAMCBsAwHQYDVR00BBYEFLv2zLItHQYSHJeu
KWQqENMGZmZzMB8GA1UdIwQYMBaAFJEwjnWfWyn8QkoZTYaZxxodvRZMA0GCSqG
SIb3DQEBDQUAA4IBAQBziaI2p86poGkjD/4Kkk0HG25nY/0eNARD6/oF0/sYonX2
doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZlRAzEf7GHqgB/Nyj0ad3pdpVY
eDh4ciNKjbs+aEoTWgAkoqEnt1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqG
JdGf8L1zLFXBuo2zL3HR+M9CDr40pq2JCKzP0Qhp7poIccGE6I9Tsg+Rr0A9iCQs
Pn1+Tg8YedJgZUWF07rNmT0TzPCVzUAuBlr+JJtZ0KypyQ3eoZ6EPazXqMyHAVcs
m0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCafwCAQEwbDBVMQ0w
CwYDVQKKEwRJRVRGMREwDwYDVQQLLEwhMQU1QUyBXRzEXMC8GA1UEAxMoU2FtcGxl
IEExBTBTIFJTSQBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw6
9Phqzppp1zALBg1ghkgBZQMEAgGgATAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcB
MBwGCSqGSIb3DQEJBTEPFw0yMTAyMjA5MjcwNjU0MThaMDsxDTALBgNVBAsTCExB
UuDiqUQkX8Y6z7GoBK5oZgbF9o0kqf0xpi4tDaKThTANBgkqhkiG9w0BAQEFAASC
AQAPv1BIItCWJndtkeHveM0hBpLsosoAUG3bMHg0JNi89kzV02YK9YDjFSG2nX2Wj
pYuKJV17UH1aGCmyA0D20umbcIuBqtWXX+W4SRhzNGR3P+1x1VKMe//qP1TgdZTR
t9Eg+vmJwrIuJVcZk6+tagN0inCl5watJ0BDEnQCqgywe+5EvT7+kRrIV8eZWj1f
7e2ut4x0MYV0KwWB0pBFtY27rlu8rMjqf6JT1wpvGvaX1lsTsBPqxFOPe0x321ma
HGAO/tnCcm7FXtFChgFR6rfrRDvTBvFtr81ldBk/vPYo/PevKjR8mX5lg00GcFwg
30JDp0rABngu4wItcNYBsNPN

```

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

iVBORw0KGGoAAAANSUHEUgAAABQAAAAUCAyAAACNiR0NAAAAcElEQVR42uVT0xbA
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
BAoTBElFVEYxETAPBgNVBAsTCExBTBVTIFdHMTewLwYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIElnIcnRpZmljYXRpb24gQXV0aG9yaXR5aHMLPSW9ETmXSs5CVIeh7j00
Boq0MA0GCsqGSIB3DQEBQAUBIIBAI9iPH5/b2KLsDb1+Gv6Q/y0jrEsmu76Wu0A
rQu6BKFkeKtgemTUGvvcbc//DMQLqFXrciCBw2LNPzq6pxpgaaS8xFcvHttAt4j
pci1n9SJvAggSTzU+vaHUEdGf/PTP5mBDy82PbZx4cZbuIM4prBq6/haUnmxARs4
xSEbfQliaYCSFRt+3GAhXLSI2y+6odiA/0DxltHq+PiTc2SGn1BVyNyxeNpxbAkm
G38L96SPP3lgeb1oV2F6aEmwBKUeMoHoFPfGz3L7aCKCcbaXgp+phC+8q1MPJxo1
sPgSToVMCakQBk/0aveXL5HaMHYd63p2G5vBUcjvUsEsyP5N0j4wggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAnQrNiuXf9Kn9FiuopsfQYQT0
L6euHqh4ENdEQeBLZUsvma098nqF0Sc6Pe9QKLIJbnFFBHLGD/52Sv5vZH5aLUGh
BCeM5YiBg6J5Di8EmE2071tptn1+mDCo1CceMsCpiBiSohczFNY4ME0Yd30NsYcY
qEr1TbT8/CqmSBtJrkVVNAi+XCYPYo4yQTLRjneBR066DaPvMsR4G1YZSb/xCKih
5w49gWQ04qf7N7CH3t79Fo+OPRwRDF1MwVMTK3L4BAZzH//M4+h3w3u8XzM2djUK
/4YQ9EyFfhoTGrbi1o7KsZV/fMlmGxaIdtdQ+zny1ZzGijJG0GjKbJ7fxjCHkzCC
Gu4GCSqGSIB3DQEHATAdBg1ghkgBZQMEAAIEECpxXzqAYIhfw/zQN9X10hiAghrA
gmLziupytMbQFUjii3dvaXG3GoyMPL4f+eEcPVkk+YShdVj5yKdvuD+Ck4hz7YAw
GxVYDWVf1W5ofL+Yd0iW5/0YwJ/6Q1i8gEmf13JTnjSA3vix9wP1bu8K5hS4eyd8
dNbb2AwprX/Fwd1hSiTsnJ0eov9RcdmmTLhyD7yG6VVMZ85ZhJE7i6IygHxq8M1F
Cef4x0QJf7XHmd02Hi4t/7yjSf/HsaSNct2jp+XB43tNtYp11r3acsiB0vP4lAp/
XZuR3tvUnEXL/NTp5ulMqfIQ1LKc9Ah0znPX8H7g9ccTPig09nm8qWea0MyiJ9Vm
/jPJPN6xPTJT3jxEMXj9V0DmlkG4aHhkf74vfQKPNt/lx5Tl79Cit73Sw0ajCqgF
IOPEyvUww7u4kGxHtXlv+CirX6W7wPGPdQku7PXw15r2I8iBWFa0iqPhuoluaWnK
CRN9QQA0PASCdZxyHB+Z0E4JMgzt7rwDiGChcZn/0wYMYEgZW75N6kA2Ptc2pfw
+9l9AXkRIJcU0t3p3Kk9JiFC/AinLP2XfseuQYvtEUviB1D6snMquAkdKvlsI1po
SjJNHyPqC1+x/0jVqquEpDVhHQ7JYci4CfzTaEGxvtpGMtAYgHX01Te34+xqvg7/
Vwjs+NJOQVT10j+bQAu1IbtAdg1hE6PhcWy2S12Ej5wWvbrtoy1/9b8hBoGGnLiI
mRDKj2PiA0dGKi0q0d4tIzmKnzRUPugVwjLEpW9BBP6p0BcNYBbBKd0Qvm0dh1kb
V2rggBQdIUeDvb9bgM709oCZiokmJqUDVrD75VTWPe11hPv4ab8XM09y81C/+4R2
8X8NjYlf2RLGmRhvvAYi4LYRaP4db7pEDCK3cEZ+hB0MG20LfuZoe1RmOtU5Eu+4
8DUUw+7aOM+72/px1p3v2Yruf4vX9EZJJidWnq0XNcopts5oIMjwvKfpW17fzrBX
JUhpTgaycis/SAHAPdom02aS6tDMYS1hv9hLTCrsTnyFB04A0V+j8R834An3VRZV
S+Qw8M3j1WD1TurHPGpQAdmvRUjKzX0nXA/Ior2MdeV00b1uFHTvCqC3HRx1+eV
IwuHNTcWedC5EYfIzIfKgjKf3gq6MRd5wfjqPCCN/WVDIHGCMs3BZJVAX+1aXqU
5Gxgij0n9l3vliknqGz+FqPBRNS2kGjEW+6A/3fq2+T6R7xbM10wwcziXZAEWIYQ
MmhqOpy4FqGKh8Xd9RMZ/w+XEOLFY56FzvlkWoL1tF5gvpCnTinfszUdvyvyyWB9
mT408LwdgZap/bvH0eU2JsfcxLd2E51ssXhqYaE89mR11BZ2hhyU1KRwbsALwJhr
F6jEyqtWAKn1v55ZyoHBKLMvCRkvi8iQ6lV0KZ787sCmVduFEieMzzw40hupwpqX
nyKAdiFZca44nw60vHSUiALT9umlq5mGnomqI/Ka13/fzjz9dKJ6NcCi6C56ty+p
Zho0CuMQ2n90474Re5t1q1QjwVZwAPnSKBchQUW+tjbn0TWZ/QnnpCuKtdQqqkdL
iLQJZZk02qE55zybR/PFELI53Xj+RqL3ZzcV+FHU0u9Ykv+fmRMiVon0Fdlh/G5C
/je2+oFF8mmKd2Rbm8Jh+xcRAvXeXJRkNSz2NVf0ofMrCzydb+WeKF4c04xIRi2
fhhQiqcW7WcDpBVg5XtLJKLGGkx4speD0f4HQ6RatuKfm0VfHcHnRDTzahdLtdoJ
uiQDBbn4ymQfBVTR9h21VcncUz1M0BeCTVh9BA6kUbVxoctzKUonh10r6pKWsTD
MODLU1RJUi0R5EsFbMkA9nRaMflcvkD0FRY27PPqWwajgnBNUIZE04gMXw/yM1gc
hmTw6iWgPREtmAXfoS/rDay3sH5GKZy+Be7kdVINlGFQjEaLnaLuedI3t0ZQ5cfcF
```

rLpAM6rD8to2o+Kcd0hRF3US/kPTV0cXxVJhL5/k4HpPL8bmnlS+qzoQojJCfFkR
zt0GEUVlNxoHyRPFejr2UQ9s/+edUwXwTaDbWA+JPaaDkxC5X9Asbxain9tj322c
8u08KR0dqCMtVo4ihyABJhk8dlhETuzYAegeSXT7/UPoW01P0f0006pVn2/TG+os
v736v8ty7ytV0yR1XVRaTmxSH0ZhamStm81R1mwIqqbYcYT2lJrp5pTStH4GpyVd
ave/jH0GXIE5R6RlJm3kzmkWHii9Z5FKBpHgMksUHM0mtlWAGa/DrsFqFuG4tNVU
FRIPgZbGXPGTVgMzfhn0/C0BjnBuFMggGpYSX8MTu8rznuiSfSoRffSLMP3VRD8P
n+nCqncj9Z+k0c9y58Sg61ice7iiBgsjFzh49HH04h4ft19xtyS0LmIXpCVR+cY+
SIAqgRgXNnx+jMPCKf0DQMqAE0C5XmztisG7XWLE3ufS0Gw9zSWxoHfBPinbU8nc
8vokU2Jk7rJujoNjwNeLc6UgnsixtpQlU1NhC9apAZo/6QzUiVkyZh30I7E3GNZp
IlvBhD1pGbbxBkewC7L3rfA5TbAci7tNNX46beoEfbI73HqtN7+EnAkxCVsE6mH6
JUNSPJI7RJu3/sFyq8KyV2EzYfwhb+ww9tPYhKCaokeluvmeqzb1qMw4atpSBWU0
lNyku3ffndau0W0MVPmmbtlVMqz2NFJcfAm132PQdHSS5Hxc4XiStJBZ6/EeGn/a
lbhjdpyf5Df73zb1icUxU/El5Gkws+S2oloCa2d0XbjY0ngr/9l28xJLEyBQDV9
Gx1sULqjM+ipoQb1PfhH9UQ0H3HGTdd7K03YcoiGhN2Fx/mddOvbR0JWbx10sV49
aLxozsMx7/CTXNB5IQz0VvyF/8B3ChncqJTFBETrfU02m1p8MehfP4ZKSVCsSnRmJ
9gasDKfK7m3etaqc6Vd0X0deV0AA16AvGv0/cXymmyN9Xdw1+Aet4StR12Yz1muR
SkXmXmOUWIZ1s1jqCz5plFuKkDaPTMFdqE5MIUBewJ2E1RIzKjkgW62YUm9tToGD
z9uaIpxFd17Y6/kmeLrVjiesHDPvA4dfkCtIek0u+Hp0zjV0ruI6rJC6a0C6nURW
/qyQZ459RU0A1brtE9//7aBqhXAUzzgZ5C0u00PgFeNikBh1UJNeCceypG7kFDn5
EynDYo7WAGh00EaurGB0F+Zb6QBWMGIYQpauSE18BZcXmWVKGeGdVA9oW/X5pvP
nvQDvgJ2TZmBUpZ4bIHgi2dtMab+oXnkYREqAYqc+nxqFh51M+gdVstRL248njRW
P5y3NAXRxnkGb4lp4rUQnb5i9hrtqeJruqWFK1bQ78rNc5qjbyFN2LARRmDDtXDZ
UgC2553rSgZycE050JkC7JVD016V4qGftBx1npXrXS3WEJjNyP8ZkwvHKXEG9xyQ
hgYf27vBcss2SPws633HkXmyCRpturu5J/AQGzfjb2kvnHh3s7usQkiUqcP0/AD0
uQPaEXqLhqfRsXkw4m4ZD3YJQbVNQ3ICa134CqA7bwjfp0Qrosgzpx67QG9+ksTH
Wyd4hk8Gfcec0MiB8vPNcg4j9vBli0xw5Ip1WFBY6TL4PUAx1RnUQeUDlv51Xbt/
EzviUnnBaPsnZsMrMYZmj3PRsCKLr118BAXgWgZjrS4b7wsahkTZiVKRc+/bXmv7
7Ta16UYQ2mTLM9qPG0v9gJFZtQEs+HQdJ0HG3on47coqxudJclPSLvK4Gvlux0i0
0GyIagZXndQkWaXGy4KHcyM8nqmwhAbmhlTtX70egiI88pkj3i1d0X3Gi3KEXL7D
6zHlQUYQ6bVeq2NB6byFKGiSZz+9i4J3vgfW2l/1Mwu26fukAs1L7cBsXyREjTLw
tYgbw5EWOH0xr8Mgj7HrhGPLXX/gmjYmg7YRds9WWte+9FsRYnUTC9oVEGoIcE9b
JPxUp1uJe2b0eqz4dG20LSdk6UEL07ZrKZGIt0TGKgLzNb4Vag4z1d2RD105w4wQ
CzBtH8nERP09Idx8IabEpLd8t/E/W7hVjWj6pJEqPB9Wp4Q3gGts6xiZ8IIs5Ihv
x9NMmrWrtpg6nuTZ931PakPyVeZKepmvQgKk0LpmdKXwn57W3IS3YXG6Jvufaatsb
tCi14KxiMbPBpEbZ5vNzuUzMUjF12GLii3AlRvMNJNAkbRc4T4KV2cK08LZtk5c+
sY68S2ZsRrPjKNpSiI70MRpSBfaQ1L7gGzCNUdG86geJ9kUUw0Ri+ww/PCyXmYQX
7P0xtHU6WwLnxKdViVpft2juS0Q2+LD/p0wag5FaPsBsSm4b4a8kLAzfNyFyrdGL
SnzL0CipUe09mfbcScMtAJEyh6zvETubiM0uRCC3iZDprXPU3TDUVT9Vmfbfa881c
hCwKk+4Rz2QU1EjdaUJwsbW3SufT02U231x71BRf/D+LDZmUy/BhSe9+6x+Z7up0
v5BCrEb4F1MTyenODG+JU+Vev7rZp4A6eJT0GNDpq9AkI3rI1GrTVFGg18cga7P
EQgqUWIstSL2B9HpZrTCuor3g1kzQNFcCDpo3KvbmJ0FcLG3N1m3YSFcXrAipbhT
uz+4gmThKBi1ncX1Kp1p5NXXbnCD7JF9h0vfdVMA+eIYGufu/YjaVrm0jfhkCEsk
k8rhAae91JqXKD+tUXkRPV361LpXVAhnohPQnbWwnVdJ+gPchJS3RyABFzvni2Lz
309Sjg2r4N0bt4xJm2F7T42373w60JpHJ08RFnSNppqyVX3AD/31lgAb9kTB4xy/
n10+je8faJ2zvoD3BZqDF2/8gacvEBU3xBUBJi68AaBlhhciNY7SicG/SS/wRgRi
nNj1hHX/2SRf5vGb64/4RvN4WqUCEMG4m1Zs1e9352A9Mi7gs17ITMwDKCrCSQs5
d3fbhcnis/29E1rxMxu3LNXAzebs1bY4+NYeR0p79rQwGFFH11vJw6hwdLxjHE+H
HjJ3F01mIwj/TSD56JVDrdzASZEFWoTQ0j4Wb+dnvLRFYQJAuLgJUc4But5/rYPZ
BDSbuGRmstktzJmgs3bPX9QhWscGoDxFTYvFWZsG0Z2A/Q6sBC4qMmTxuxUfQA7A1
LsjZoTjRQLjIN6jkQ0n3hjW7oF1aX5ZbL1hE2YrBei5K8K/32Xxh9rU36kn+mdyU
fcFdCSBm8Jw+4utPG0PcC913tEP/apykXIU0EN3NFMmuQC4wXGLEQSprqFWIZrKq
OHD0TB+OR1ATKGhvzJHnVUHbW76t+MUi0Dpn0L19eQuuBbABWLvSbX+z/JVCy475
3LxsIxrLohS95MgkpszqtCrjCAW8vawfLDOHSJNAMx1Yg+9WESc8INI4YGzrJP77A
8L39Js0zxiJ98Wj6T8QK+/MrLj7paOcVMMvVVB2fyUH1+91171UOCNHS1NMFvYu
uTptL82CogEZcYawyMMYV0Brfeqj9RkBG3uGJdo5h+mn1jtXqKxFVp0t3gYaylXM
Ap7yZpZivcQ3cs/uVcAdX7/ohHm8JZaSrpzCeTe3N7yUu8RjcThYptJweNutNxcm
olh+n4mWcSWLAXs9suKqecReWfJhNfeeGgJsxRNDcbxm2/Pj0p8dSWcdsKie7KdF
PuFApDm3vtsDpEyyX60cfS8J6xyQnJdzIqyW0c1d8FU4/dYJIZNFNHtEmoC+Vies

ssW5H7zPZFPuEsMzGfJtnuEHhkWNhNavbsVo2jK+LPXfQN0Z+c89Bc2d85pyFNeQ
kyAw5t10YMoav0WqBrb+rs4dXS0A17WKJcPypn7c2tZjoz87qFymre+3frC+oegc
WQyMEP048xuFqRB7J3+usCv+7p0Ur90MnVb1364N9hxfDjTJ3cgDoIgx5sssp1n
Z8GyaDmqGqo0uvneIys9+wbYDjNYFQLXUwL6Fgzj/qldPoF/YdrMBnSRSUm/a5E2
CPG0JgJc/krcLOYkSF3gJ3verbcoycX99kU1o/HlGL5DLro1A9o1D9HaUg1oKPY2
pA2k+yAiv5zoj/4es6UndtxnlJ2CEun0oJzEGQy46kVkfgyVfx76UnWcx16k/E1C
ZKu4gOL4N+jbDwu0Pw3j8eW3Q/3esPTfE0AJzRTtgkGdI6UbrNkNXVWxfKDLchqW
18U5RMrvD+zfv4yyK/jjy7YDd508ildX4R31LcnzSFJeDF5mSnhePCBmWSEr0z6u
62/LoPj5HHN1U/LESRAzNuQLwLWe9DzaGaeyfBHBVvFvUn/BLxPifGPsBZKbEPg/
9q8UPNh+vPFRdQp9YAU0UV3VQZXhQxRNiIaoFF2x+6MEA+VoKH1ANo9zbzkPsCtB
EdeK4Dw9t2KXJlMm/fB0C7EdYX5UbqVr8VM9GPt7DUndG4WaxGH/70rVA4u0MtDG
YS/eHjpHEkhxv81pguuEuV3pXEQw4h5I/DUCeMhYt3zEhxPPCXRK0qCDNfZVaiyg
GjOV+wDYTg0y7SpHdXNxfA7Khsc8NFK5w4Cx9PLGQpg310c4HNxCSDt880/+pBsr
eTIs5Ym9NZLqzXFPnc8ixFCHXvg/eZEP9iEbZEW2pMDePzOCwHGLouYpgHmlGUfr
/gn72roI+uT/gYH8Lc2SYNR7g0QqEUmZ79MzziePg8fyvxd8Ii0SpUHMlkLbQdjC
YislsKmjJsqWYJrsSXXB/jomZuv4V8Ix68odD6nAlT2/FLxH7hq7YFfdFaTeUaU9
vCEugvW5Z1+VdXAWp3egdU3fY3yDgrIDqTfkH8mlk/Sk8XEhhMnYFeYPQ8sDmkT
8Zwi+P8D5RfP0fMRAAg11rCPm9woeXA9JEGnfBtKpEMEez2am99nKfIbkl0xvj+e
yZTOEkjDVXtugIbUf7RMmGoFj4oHQA69cDWDfMXPJoXtF99LUI62Dr4rDGrSPVUt
dgVwS8IWPahbRPn09Nix01rb+Q1+3UyUcovJuNwia8RT8jh5z11SL4s5CwC77jLb
PCzez5nGqm6tUFLQ48togUaMbkwMgXhxE3mLVD10h/rQ2cndcvHNwkhUJpo3A9Dc
mn5wb50YXknZBjqv9Zi+6xufiTKUpoFXG7YvyKp2Wj3xNSBDDLi2ovA6BVCNsRn1
jjWeVtjcCg2cmm8nKEix2KXb7VbiYkzV6selYCCZ2LTprlJxIwzRH8oKM5mmR0UE
0mXtEhiUbSPRIYEJKgBS9x/541nFj6zPR8VDWPBC/z+Jz/+pQGj01tn8Cw3yaZoH
aNAg6NWu9Z94Wdi0ras+rAXsrccFofWL7NDC8YhQ07a4o4cLz9Y+sG99CxMrD00G
L6iachPXUyjpTxqE1g5U9bIGqoZkrmdkv9ZjGxidFA/ofjXZ/kV0zfQ0R1TZ8g7
/EMhFMLtcWu+SCP17ixBgGK14wEUN4gJdBvWbNvXItyOSSngCEBw1G+cqZxtzHv0
S+lRIETuFP1ziPKXisDekRLJ2n9ySsGz3ff4SQYHvv2f50JpjK3ni0tzXrhzjqQR
E7LXJlAYxc/SdKkB2N8aj0G7vld5ydA5dDZM1cbdNkeGgxaCZd6hDb08Lc52H1j6
B9NQgygtF0INFnEUvrVsI3SJKSrQaeafppe7/RrC9FsuwDe2582BKbX9NnCXQamI
ND3HDvVFLi7tnaJ7luGtQvqV4BHsF6WNBjTisWxTJtuhqQ3N7LvyBG08DJnwzUFj
D0vaWHTdeMmsvkQz8J0/fMxq1GxGnHkjjg8BmmkymS2sA/RXLPJ4FIgPg1eNymY
6IphFEpTwyow1IYFIROiW6KiVArA4N81YpoMepz008I8MA5Gf9XoRJRpLmo2z0f
hJ6UCY02rgunUaa4kMbpSW+l+7wUPEgbxM47UQKZ6FRjU0lMnmYNxHnoJIOCHJ4R
0nP0200dEYk8qYe+YSGsVa6d/dGskOBK5YrZeXmSiTHiZemAyahE38rZJIZrwC6n
Kjm1MDaTiS0QhtNSVctjNYqJzkesSjr7ihxP7M8uvB0NV9hs3dpiJr7oXFKPR3gU
mE/Jj6gtBe+xcuhlqPvWLPriM6rZEHsict8KYVzSFhXMZ/LqM/r4SANDThOMlp
PJ0QzqUqUSDrZp6FefbzrHMKvmh/BjCPYVYrtRhncYeq90h6D7pUjsdKV81MzX40
TeiFRAlpv5VVJlN9A7QitE9sCvT63b9M19YIHltZLrZI6oAuRLVux0TphgJnuH9Q
nrDVLhFYzmcIIZ5zeHcSRLAnE4xhHY9eNbBkfr+0kSmzY01lj/z0kWs82ZxFSv/
X8m9r88mMA08UjvSSdaXaU4QMpgyJqjIDYp8bzX/sySZsSwue6Xfz8+HV18Km0/
aurM5Cnt4pPCyechH6d3ktp0atLfAgkvXRY1qeB/HQ2FpH6WbZTxdq0AKKsPHpJ
Q9E9KwXmooTajSKyLamS/e072pQ5G715KDaEkaG/07LRXS/gmKhk+yrfULj2uMAF
3Z1f/irjt2aDlY00fpQtK0396ZjRlpTb5Z0YwA9Z/h8nDiKils7wm7aOr4MFU863
64FshXZDst8UhD2fg+FErcxLn0cBsgBAwoQ/dVyAThn5yg2/RdQUXb+lbUdoWQsa
KjA2/fCE+MWIvNI/7kV0Ju1oF/kIhKb2GMS4qP+mL7iyGRexfKuXg9t2ZPcrzDVQ
DJ+U8ShhTwbwXKow+MYEa6tyNr5n//R3X0PqWEh2Nm4i3RHsHAiyT5y4XAFV4bqw
8A+j/IsOYb6Y0nXSmPcAqapvfpBkmFYVmKeKenX0qvurU9WnWIPUVex2lZORXWpm
Z0rJpkGeJ0Qz1+lUTlyzDv3F0Yfu2YM087UwDjusFXkZx4q0us0RR1H0ivRhsSm
fVPvCEJpPP+IkbKC9rntNDRYHZXe0fwL0BayXeP5vzu0xhTPj2scw7xGGQXSV/K7
rXZiYp21dUgWPvtC6GsnaqqB60u1Y7Z4RyGIROF+dpIqGPa7cT5DWaxFZxA28zCe
my2SjL2+P8Ci000cynhFSW+RkxwemTxUIcorFeRbwY/QGJPx0t3zYd8Ac3xMUp16
5e8l05xVK4nonot1XfxBEb3KLU5szkNM1KzoXNFxjvnfiwrSX8UNGWAvmDWiGWut
7D7b2mazbiAoTME0mX43as1FHeCo3oDjeoEiYyc8b/6nLj9/SMSkxzgnrcrxvEEAG
amhJ49wnRgOUWYkZzy00aCQqA4xnG184Dj3tQy0afpE=

MmpvMDQ0N2dZRHBlQXJrK09uSkhrSWHBZlRQUmljaWhBZjVZSnJ3N3ZqdjBaV1JX
TS91bGkNCnZkUGYxUVoya0RE0XhwcGQ4d0FBQUFCSlJVNUVya0pnZ2c9PQ0KDQot
LTiZMC0tDQqgggemMIIDzzCCAregAwIBAgITDy01vRE5l0rOQlSHoe49NAaKtDAN
BgkqhkiG9w0BAQ0FAADBVMQ0wCwYDVQQKEwJRVRGMREwDwYDVQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGx1IExBTVBTIFJTSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cm10eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UE
ChMESUVURjERMA8GA1UECXMITEFNUFNgV0cxZAVBgNVBAMTDkFsaWNlIExvdmVs
YWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBou0P6AFQ
J+Rpw0DxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+a
uzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVe
A5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShp
lcI3lcvvBZMswt41/0HJvmswqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5
NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvDhJLAgFpW/jA/EB/WI+w
hUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAAwDjAMBgpghkgB
ZQMCAATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAww
CgYIKwYBBQUHAwQwDgYDVR0PAAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8
ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkq
hkiG9w0BAQ0FAAOCAQEAgu14oJyxMpwWpAyl0vK6NEbM1l1gD5H14EC4Muxq1u0q2
XgX0SBHI6DfX/4LDsfX7fSIus8gWVY3WqMeu0A7IizkBD+GDEu8uKveERRXZncxG
wy2Mfbh1Ib3U8QzTjqB8+dz2AwYeMx0DWq9opwtA/1T0kRg8uuivZfg/m5fFo/Qs
hlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpFb8
PPwDR6chmZeegSQAW++OIqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTS07K45
9CyqbgG+sN0o2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdB
BXntdX9CqaJc0vT4as6aqdcwDQYJKoZIhvcNAQENBQAuVTENMAsGA1UEChMESUVU
RjERMA8GA1UECXMITEFNUFNgV0cxMTAvBgNVBAMTKFNhbXBzZSBMQU1QUyBSU0Eg
Q2VydGlmawNhdGlvbiBBdXRob3JpdHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5
MjcwNjU0MThaMDsxDTALBgNVBAoTBELFVEYxETAPBgNVBAsTCExBTvBTIFdHMRcw
FYDVQDQDEw5BbGljZSBMb3ZlbgFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBALt0iehY0BY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LC0wI2ju
wdRrjFBSXkk7pWpjXwsA3A5G0tz0FpfgyC70xsVcF7q4WHWZwleYXFKlQHJD73nQ
wXP968+A/3rBX7Ph00DBbZnfit0LPgPEwjTtdg0VQq6Wz+CRQ/YbHPKaw7aRphZ0
63dKvIKp4cQVtkWQH16syTjGsgkLcLNaU5LZDQUdsGV+Sao3nBdWCRYV+I65x8Kf
4hCxqqmjV3d/2NKRu0BXnDe/N+idZ3X0zEoj0fqXgq4SWcC0nsG1llyXt1TL270I
6ATKRGJWiqVCCpDtc0NT6vdJ45bCSzsCAwEAA0BrzCBrdAMBgNVHRMBAf8EAjAA
MBcGA1UdIAQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWlt
ZS5leGFtcGxlMBMGA1UdJQMMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAd
BgNVHQ4EFgQUu/bMsi0dBhIc164papAQ0yBmZnMwHwYDVR0jBBGwFoAUkTC0fAcX
DKfxCSHlNhpNHGh29FkwDQYJKoZIhvcNAQENBQADggEBAH0JoJanzmqmaSN3/gqS
Q4cbbmdj/R40BEP+gXT+xiidfZ2iLWYyTneuk6AChwKfnNvOFb8lV1iffRtF/K
tmVEDMR/sYeqAH83KM5p3e12lVh40HhyI0qNuz5oShNaACSioQ23WxHGvy9vsdVf
nbhsp1rWg9NQ2WbpCmK+2oMh2oYl0Z/wvXmt9cG6jbMvcdH4z0IOvg6mrYkKTM/R
CGnumghxwYToj10yD5Gs4D2IJCw+fX50Dxh52MbNRYXTus2ZPRPM8JXNQC4Gwv4k
m3M4rKnJdD6hnoQ9rNeozIcBVyybQYjfrgg4DRvW9Ksk220H4ConlB8f7R7s1LM2
cSYxggIAMiIB/AIBATBsMFUxDTALBgNVBAoTBELFVEYxETAPBgNVBAsTCExBTvBT
IFdHMTewLwYDVQDQEyhtYW1wbGUgTEFNUFNgU1NBIENlcnRpZmljYXRpb24gQXV0
aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrOmqnXMASGCWCGSAF1AwQCAaBpMBGCSqG
SIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE3MTgw
MlowLwYJKoZIhvcNAQkEMSIEIJqUXzqD6DHL5QxaWDH8cjQd+BnWEDsqfNBB2TB1
TAOKMA0GCSqGSIB3DQEBQUABIIIBACxiU0FE8dQ6qbdByg97uCG1m0thKkgEMr50
RkpoX6ntzZW8Bzj3x0t6fe6wwhxExszASuxN0STebics6GRcN/EzXV/SUDE0W7Y6
gK8c4LiuNfD76ZQLHbPhIMYDidhYb5lD04MZCJosGPFCgGitf5V089h6WjZMY26F
YpL5lQfXgVAP0A4Y+2f8RaEP4Fsh8SLcV/EzniT2xCNCEuZwsETA650nGJ6A6ktM
ljaEywaYkm0bVFuJ2m14x0YDd/pZpr7CIgDtzh/97x39apqnN0nzTgnGgZi2T6yK
4f1YxBHvYI53lUd/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-Outter: Subject: [...]
HP-Outter:
  Message-ID: <smime-signed-enc-complex-hp-shy-reply@example>
HP-Outter: From: alice@smime.example
HP-Outter: To: bob@smime.example
HP-Outter: Date: Sat, 20 Feb 2021 17:18:02 +0000
HP-Outter: User-Agent: Sample MUA Version 1.0
HP-Outter: In-Reply-To: <smime-signed-enc-complex-hp-shy@example>
HP-Outter: 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

iVBORw0KGGoAAAANSUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739n03TpRw20dqpbfARQEjOywiwYnCTkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+0nJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/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
BAoTBElFVEYxETAPBgNVBAsTCExBTBVTBTFdHMTewLwYDVQQDEYhTYW1wbGUgTEFN
UFMgU1NBIEIcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIB3DQEBQUABIIIAAI/dYMBzc3ZeiYx+UrTZSpSeD0wGmzAeujC
jAZv5gFxb62n5NLR9K9d+shGjdaYbpCxj8JfQmFg2j0B1M1Ekf06RXo/3A8M+1Y
DTEbcZxJSVsoxWD5GFybNQm1kCUSaPtWJd0PdXv27sdv4y1WZ0w2AW1ecaUnK70f
Lz5ge+Uz8gSOU+nHnxES0AMqUASg8lgk16IWSnm+Vnt6YVeaVfiA+DL/+lG3Ijf8
+KvkwSasTh0Bg81RJ3QepmHqyZcJopJz/T0sn/6zp+wk4VEeqF19ofd1004Eyck
h8PN2ksrWuj+8xts5CxdYBnAn8kAiA5yusP106xJz22AWQY8oo0wggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EGQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAQDa6AeSZzIQh8pQjC1WUIK5a
FNESnV+b49enYnj4vuGEHnnB0TM5btNCYLoI62CvyDsSMYCWdLBiFPBn2w8H2IiL
m2XbWwXDPULikc01CGEmSmJJI/7GYScU0naGyrKxT0BefjovgQwFqJmBFIAgo/xc
DyS3betIuuvZ3PTlQPYLQRTHIke7WfymJw80dcdgP6bY4JQp5Pf9ErW3GvdKx7wN4
gGyqFvCm1PGuc00eH00jb40Gcg1fzqabBQXax3Vr+XxDiiwwa50R1nPgIhf/mYOU
07B+4GH30ogzveQ8KRQ1Ry2By41b+nF042U/n09bC6FAebCGj7qNq1x9G4dpETCC
Hg4GCSqGSIB3DQEHATAdBg1ghkgBZQMEAQIEEHdJN410uotCGn4QEUssJjWAGh3g
30f/pefDZUamG+tfMmvMOPZZOznkpv2sR6nXwJGpqMzgnUv35t8MatduIQvjL/vj
1wkZ1W8XgKKrC+PI1cz2HaJioFVglFmp61Vuzep4gZZ6coK/oq/0eZfm466TiaXt
kUaja40Fs7B/BzyWI8LzzjRuZFWJeilfh4HHEXFFNJ9n6aTaNcUW1AsFCyi1y3H+
dP0Y35mB9o9N06L0/B95yJj5cJcF0f3clANxMBZWvrbof94epVrOpptl9dQMCNiB
aGdlvI1lg2pXDyeNYWR5jpdTBAN7Bfmg9MPQBWzRT6Deq9qkD6aLwOJW96dMW4hh
fLCOEWGuMe6UEh8hvsx3gVF7A5wZ/fbs9pZvrHSDDU49+Hkf9RBvBepPtqXt1dxC
kEXd1sXae1z/ZrUVkBjWLoZ8HHPyEhoEQz6GtxR19yffDA3eRBoaaTPUJJaU620L
oJwlGb9efDum6jmbG5cHTBCEjWAja3NK7ZX0RmG+kxa4nDZuK0w57DhbtVJhHsTU
0cz0vZK/EqRDHXiPnxXysHM3V092vmW1Y2GKhNCqFGL+5AGiGcZ9SxgZ3tbMWVmi
YkSSf/pU4h+MCPYKIGXs8suP8XaLyvk+nWnAitf+emaI8bootKazLEWSGtIqC2M8
6DwNaRI2aZc9RkgwFd3MU7uYhM5qhp5cvgLxWc/Rg30Ly0m0V+GLza+3AhiMVPo9
YNuo02TxfastJeC5jaEd2212Zm/0Z0gbvDw+1AD8DC3i3uDgui3xtc0Ljc5DziqA
/usC5p12hjw9vcG1puqDW0z20iDwvtasiR9m7k5CN+ViSSkt2brNAX4aqbU0321f
UcsxeDZ8pUDs+SAm+zuHMUCbWczHW1bRYlo0Deh0vaPb0X8qxhJ98JnNdNooG2ko
5U31i23s9rTH6/Ebcsn5BJe0vHk9DFX+Mz19+k9phWiihxn4zTRXvgDC+L3GByl
EIHwRE2hgG32fKmgGeAa0ptLW35RPYZDNidMQzD9eEc04Gn9kN01Jq3E1vwLixx+7
PcgTdVuyPJvMrpJ2TaLJFM3bN+ywyUY8bVFswaaaAXzr4onnC2HJShKaUGu0Tbn0
RPJ0gpZ0B0ujNdqZsJjnyeUTlkwg8IxzsfIP6UljfJNHR78quPmNJwgrN+9ycEo
2GuHtfYixeBVucNptDx708p/+K21MgGfCdCmubVzQzm82QW3xvBaU0mVQuE0mqd
xnC8pc6UvVnXK6LBqyDzbBwk6UxqHDiwmst4P12K0Z/MJVmMBOWyyef3PcIgSz
5D5seDL/ZkzEmnypKfCMYPQMrrLWwcSiYuCXKKqjh0eKwkt2ioPrPdPUDNs12aU1
U7Lurqv10b+ajNQ/uB0BmqSwGlsot7Tz9+x8sM4ywWhJ/9kAZt0zZ01VoIcbX6y
XW8oNC+A0k/nSyHX5vbQ5c9paHif3s0lDxalc4T5PmZ7vsG3TKr97N7Bbas64rz
zjL3YlsY2sxSVhM15E+Rzf1bcJXT9vqS2n6tZmQdLIK2r3xEa2MQmj1D0281FDF2
4ckMsHxmhw+IdwS9JHG7mdm0LHYMt9QLMsxdb9ptfUqZw8jpwIXZ5gjCIw9PLGgQ
n7ZTm5eNRZfyCi37prI3oR6j8s8H5NS40eygduGjkSUensap8iovsRmb+SX1y67k
Ti7Pvtqc750/1FeInnWudpnbSd4ZTnfHi+D6Qe7UUmz80JKF8B6Z69+Y+v6qCS/q
jF+6JxVz3SoJU6yMJQY/EXCwd5Ft+kyYVbCpc/YK4Rjg5XGAZrIdHqorqXJDLs7+
3DPx65mIeyIkFoJRsh2U0HWG0w1W+e722h21x/gyG0ron11tcDqfhIZJHvTER8LY
w02qWpWMZxoSRHxyfcdJ3kUmdjXUHCmVMoKAp5zuBNiTLH6Fn0+iux4qQMSM6sg
nTt1rRuH/9hc7hBKfHbCdXvj+TJzs74ChntNCHPzZqsdPup36y9YUTQ/CC/pLU0HX
FEcIR+PayJIszHa//x90kL+gzhRf4HD+vTuc51M2hpScoZyj15yFZz58LWkAG/1F
fYB/upejDYznM10+bNwYh3pJ1NpPfcIwVZ2DajxMS5g71T3JJfJKem6FxAwno0AK
vgCjghD5rIIEfhD2gn0FZphYmbakpDcijFFIkmsMzcAWLBjn6IWLbQrJZs+S2q0n
xdR/d5CS0lSNtSSQVE9KqwpID7nt2Ux2CDJRxi1csLhowgDM9GQ+iEHw1RT7JzcP
DeminbPX0GmE6LumgKhNY8wWUxc+HUTenvHw9/x3+0wcg31aptvoIjexN9kklMx
8U854Za+/o8+3f+Im6gpz5orRwsl+EFDrH8ChCM180vuT44HwIvW828zMxTcBfU9
/Pb8dSZNNb63zJbx39PDH9aNSFROXQNL0dfvQ6Rn149NGMqvaHiNuJ7y5ZUVqK
S6HTusbiUjitQ0KJo91qEu7wQxHLP7STTF0+sLJpST/zm7H0L1uZd0/vGZrzz0Jp

WzP8OUNAk2U2kc5kkc/dhsmTIQdxN1GmN0Kdv7L6XbWqHt+JjuK80C5WgnCYgrLW
f0IfkyLdwT00P+vf1QJoY5c9ACvHr6m/mrzHDDai2xxrilQRdxuFcoMF0pG01Cw1
IcucA8FD04z+F/De4bsVxf89HUauVFIPmpv2QFfF576IS8/VpJlMtUhb16R/I5QV
UcAPa4+CbT8Ldm/mKDDH8JfH2tK4x/c7i0tSojz+vJ8kFB0wi/rF9PAsaA0XfCDL
9zhdoEYBogXtPggz0fpWRi/ksW3P2SyBEZKHHn9mvyyLSFKpqNKSqRxJqAb6o8/H
OyM7mTiIWZtZM84Wk1raN0TCFvkHGT0sMILxf7+ukicoNevX6ZVHjzu6jl68MS0E
TjLMUzZlhXFLV0eEsPBkS1P/auYqKaj1c0g0xSyAvjoyE703zMurfxNjoGBGsaRh
I0lwL/DeDypkNfpcTnyqBK8PbrozDSuSZ0Q6zVSurHvq5PQs0fb8yKcKkg4yztPA
stv1geh/ZI1loQZprXVK7WE90HLhg9z0a8AWiyvi4tMfDwul4P00XyX/HzK257kA
OwtLZQXUfrfj5PK6u4QZsfaURH0d/87S8fhIyskmAjzjFbd0VSQqYFuECW5RWwnj
5+q0a1mwJV4yRPSm44bcdPXHBiZHKqQ2v/wW8YfzTWSIM62VX+VUZMYriyIXxq8d
VJKPfy/177Jfnf0vLshh1DLwt87nZCrkjXlEazUtcZ0kbgXb6VJw1Wt6CY6fsTjy
YtVUNaPuw4u+0qiFiYdHlFIEF7ERvqEN9HcQZpIVJ+txy0lyExLViz6MYVLGMEa
EvKkDX/aFNQb501wi7sDivcL6M2c8hAuZYzF0x8DuPiuEovicWQASsS/odhsfEVp
tKMqB2woHSX6J4a0QDfQ4SUDUrXHqCTyqDiYgX1cYi1pHZ/vCN1MQ70VrgDyCq13
5zisTrvcI1KX6Hu9T4UnyeK5HPP5SB6KfHp2Br7VPe1GARo0WXGmR7FnI+hjo++Y
ZABKQRj4ky8iq2uzbonTgmuQNTM0MN5c4sez4xPfJE/zFk57NM6VXvt9Ya7Q+2p3
RUBz5ZqI1/1M/FLf0KN2LDyL/FxdHx15t99dwoIieDJD012V6xvpQC0Zhg0GGuMQ
RjLuXzK+0KZaWmV6dSNVH0CW+yrvwg4oyZqoiRaCZsECxYe3ur+coIz0MPb0i0f
RnKYVn24AqTZ1rTcuBUxj70eSLGCFvZKLGLZli8bUabyCKr54gwaxrQRy9UZxTXa1
1XsyDz1fm5XkcciuZn6rFlwvNxbYDmis14s19R/7w0Uhw87k0Z9Bt1sDg4zp0r9X
+UstTySGKWS/NTh6BaYrAeNuJz6ThXTghrW7NhNn5gcPht4jwbAajgcF/tIBmwZn
ad60huhtokK35b5EoNI+xYgAsntzccPCmKbQ3wHn2oaziQQ5pTGB+XYA0fmlUwUWS
cWuemYfDQntdcEGYleE4U0dWpszd9bXzodgzH0ghzI8RnpXDQ5heYbWdcsNCKm
HcdUBeUegEBnMgSzIC+ae5DNs57kqQGFah01/JMQ+ek+MdrXcqEfHicuJcE8D9Cb
WX4UpITxyQ71F4/BPd/Wxc1eK70yGSCGEYSg366ywtKB9DHVzJmyAtqxAcPPJkpu
DcJ9kIKqtGz0z9qmNrYopT+hztcsZTNwfiX96bUyd67ny07dedM9epPxdSiDtn0
PtedT/ep0TrN/wkX6N5uyY7uE53m0XwQRUCV57cTAdHRPAZ7pp718FzAwnM/9p/
vk1dsafHwL5IpbfbUTTX052WIRiXqYXPfeFV02TkmCwFv0QLtK6H88DRzVDUF+IA
DVD1QrVZ5EBKopm/AF/cNqfkWDwSp2hMA0I5BHFu9nhLRQqzRL6TZo100XAN0UDe
17AKdmHgSUwFuIwocdpPULqKV18eIw0tUKSZre8uqhlPYu5SsGQ8V+4jitMD+Equ
ctdTPsTafX/8v+186N005XDKbnxMTNe1YbyMETw4HQmeaYGzjbFqoc4LzQhKh5W1
VjeQ0ZxKtzUgtKuKqI2rinI+lWPd56XbsCJ2lH+pa4tAB7thMYiinf91v86GTyCt
nzzeLdHiW6F/19WGmiKBNk6aMG+C85Bk/GbMmHcC+Xdi94NK012kPyIE084N6BNq
kdCN8z0f2kYQLCwnhCV6t9cEsq6XsIIfzL5ULbaPY7Dq017XWH5T2+2DZluEII9N
LDY00ocZhiCHp0GeiEy4sX8b5tWSgZvj8U3uV05PfcMePCXpvuFlxf3SWswElhEJ
LAqpWlC1sCS7nFSxH7M3FVALw/egqd+TSZ3hPEu1QaGY5EZ4T9gdF65MCEihsC67
U0yS5C8BKXZkmsL++E4J9QkjAnRSj1Poxvi9ZUvmIiTd0Dx3Mn7Gkprqm/WJwmK
KbazwoQtBSYpooNXcJQAut3lHh15erm5sGwtRZb63uA5kNBty6/1tVsPDVntVrQu
P1L1AQ/XUu01NA1V2L0Qck6YwF3HusBeCjZ1xNZWJC3jbUhsXkwxx2IffNcfJREh
fuANjE/GytAK1Z3VdJfQKGPd3q1G8t8xGWLGrA1T/oQdsqAKhTVR0rWSHj5NKaoZ
P4MBQz8tWc1V1L36tlirD93YIcqu0fVJvHSV65MCZMnoe67ke1pdcYKB0Wzvd+r
RBu0e4vbwGI5YstRAKLSLdcQBxqfiVqChxKPQdeXfEjKoyL64vymFuHibrENpaP
17IOXz0NKoluj55xyTUzdzBT0e/WKJRpdPa112ZknrUkcXIzLRpnqC53EmNRJ4Qv
s2B1hFpYrC4VWSBppu2Du2B1TtVD0xqad2woWordPIiex6dGb5+dqa0LSV6DH+Wu
IRc7gCfT07KGHVTZ+JkCZaoXG4qGFIRqEob8MwydAKTos5L47BVxgPZxJW2T1m5H
nz1W9CJrJ3kM1IdagWUweiCj qnhgC4W175qoRvh5DxV3DhM429YVR4+0oS3FwDxh
/1JgNTWq4R0ZRI5drPfjUdaS1XopMJ4GJPn6Dm7tQMuoGd3Sk+2Vni5fEgyjMw4a
en79UkQz9x6KD29n0m0bpN0zNhjBfps13bYGxqMIZMWAwpY2yq8DR3QW06Z2BMoZ
Tsbs5THzPbR0R17s1X4rmjg/X+1SAFzTxxhpyrULS3VF4n9NYB1gKyyNWUI9S46G
F6rXrxZaxZ1R9EvpxULATo3ZV94BhP9of5z0drytS3zAXwT7E4ajJWsSGL9rvdx8
83PvvVisD4AhqzfHS3DPHgJd9bXLMaa0t+bL tQqUT56d7R97A0fgnM4L1C2xRT9K
pobr29Nt7bQuKluMoh4NHjexc4QiU2DZiY79G880AuUDf53z3NYcbY93foYKXhYk
/WfJD33tao1cjFbCcrJR3/LY8FTdtY0APjPQwfmp967y/98yvrPqvJvHeuUFW01r
QmaCVLgWKEG0D3q+hs14APAWMBHc519UMJBq610bMmsMCw7VMKpQ3oCghXabyctq
WJ1akVeBo6usYSnnknLN9+6WMSqiNmeb15M052iYyZaU77jeDFRfIs7+B+yyycdZ
3x9N7XyTbqGZr6UUJYubInE6Uc1B00XSRiBsm2/VVFLBJRfckFMvPKK7IccmY4NL
2e6quWM12fadmb0JaM0ztUjfRCDdoabB0Sw24fh4zfHyyGJYzbLoznuCPeCg0B7b

E4fJg5tIADSJivl36YIyOCGqpj4768yvjjzzjg+rz14lTve4si5GhFgXADW7LtkFb
o8EGRwDDAOxCG5st4HmZ/1YEjm90jyqRJe0V9lDt4rWjzmADiOT5BZnbVoso5Ie7
+hB4WqaP3lN2eipERlOSGHiMN0sibXgQyvvz3Immstq5u70U5Qe1qPI0YjNF19dv3
tcxIz3mOpaTMQRzIBx0QdF5421AUx1jPC3dGktjROPE1pdgPzpfPHX3LDda26ibD
9c12AZFCsxap68AFiGNPpx9e2EzrAk8BM3L+T3DszTAM4jb+rp0gljEJH/pLnT4H
hRYhCU0PTMUXmf3b2WJU5UMuf60M2ZPT0woWYBCKR05LPoBu0gDQdCpkHrDEDtB
UojQaiAjJ2But/ox1qM4PREt+1Bw6JTVkZ0ZdttdBmTA2nKFbVUFHX2Nh3VykRN8
50917c++CZX7Gg3F3p6YBCzkqIIC0VVS3bkP1P5ZimETngRSTJ5DWE6/5N5zhM3J
sUKfM0BaGQGm3D4cTrYpcZaomPrnFmkKyUv1BkGt3oyJM2EENfX6z01kod3dZ90
kH9OBLRjR3siJfUuLodi5iF0Pn0gZeHzqHKM1NknAwVVg20VnpXuujy42NYNwnx7
askd280vZAgF24osGkrZCX/zQXfqLhNEFseKtGQEqZhy6/Ew+rkk/w2Z7gkF00b4
xr2rcyYW2JsyMtErWp6KQPvNEdYzXi+qJBwWPXas3pzH16hMjHD4d2Q8pCfUYK0S
YGW1xU69cEMtgSs8Qc9VCIowLttDKBQOBU2eH1MVRG06BgowKqC/WgtmA9rRanMA
3x+rEaxPncGrdFOU0EmXEN/Maw61V3RWZec2oSe9geH/AYj5Q0TDmHLp0j3iiQy
g3CJIsUXhKPGjSRnxPYqY0FUUACNaoAXD9PYRZqem7G6zHIiRqGCx7iMjpiSBND4
IUVWKWiuC2rvSqBmB6ohuTRt+tWshZ5Ksvi31eCCJSDB48XY7pU5N5Itfo1k8V1
F9j1bhzuAnCczqy6PHi7H05+u1WLbeh1S2EMlziQM+MziEiFUHoMuh+isfM48o3C
Js0v2o0yUz6XhmXxQesMMz2pM9Y2Lc+tcXh6QsX+RXcDMHZY5I1aNUK0g0V1o2cs
0+h6v/W/nRzSiB3f8YzJR2c2hUt9EAUj9TvcQA8SrPTen6K9WFNH0QWdd+bqbdL3
QiMh+8pLNBiIQfonsPgW7UXi8M7r5K5PewR1+VHFU89UVNU1hnu+JABh0CVF3LCb
Yi+jFiM9uSeovg0ytMrqa9qUtcNonoKP3Q8GHh0ZQrX00F8S7jG9E1le0Y1RqJ4J
0Ys8sscjjYYF515ir0V7t9R5wRdf4Syr/rhZeHBUANGevqyHkH91nTUDs33FAquc
nCUPUGETHKi3+pEoV9eIcobGjSiCwd+sh4M5akRrquUXvcb0l+6VeI/yZrUfc+tL8
Z+RE+qzLsGufkf0hwbwEprtuaSQIPfe6v7G1HMYtS7W9NA0SZbJ7KJIBktd0c0
CMtiWxcAszutTu1sst5ac1syV8TwgsPSkitp5qlJW7rHl9vaf3A+wLcDrn9kxCAF
/IzWkFgQkJbRc50vN6CZwD2wGS2e/AaQn8XVHXNLz7t/SuBiP10BpJmvtRtnEsE8
zWivISOrTh5qpdDbp3Gylec/8ltglYu9c+NL53R3KEq6AkzPRwC44yTz00PBLk+M
HkPCnWorX7rMGy2NPWaUa40meEnHeAQYVRF3I3KdKIEi9i1IM+hpjjftq9+8SqH
OVQ3l5+s1C0y5Rdsowb0ZZDF/MISYHa9loTGX6Dry0W6c39g4yzn2tyf6carMycq
RqQYR7FnBMGvbhQWhbNn1joKBkQoI2kiTrdn3QA7yhbeoL02fug64A0l7VtdR6v6
d1FXKtCNFBjiTkNim1X9Evk3F7E8/FOWKQqRNDW+2wsiKCqFbGu1LM1rjJDBdnV
xh1RGzz/LRz66skHMLnOgsNM2V3Tb1E28PZQNrmNqCSiv5eK+XTl08q2yp1MeR5
KeupsCiu/2ARCMtHePc04ZoQ1lXzQwquc19p5jca+1kIQwFsNpM41cI0XCPzMVCK
fT6OWJNL41TYzPK3rHqN67GrugV98BBY6KfpAosxtMgZ1Koe1rCA1D68BaIJJBcW
sXy4FnXgslZLs3b+R9y0uKbrWEli45/UUIW9e8zvB5pceNxWSg70WgykOvnBmvcc
sgISnVgTD1odlMa8gJwohbrryLzFbtpb6dbp5tBMP9tESizLizWre9UkBPtx9Q+P
p7MT2kne9Bx2XB2kZqb2uqhTo5vjFgsVRwzjImJ9wfs12XZGChkeGqKTyK0Q859G
WJxGUJCoLt74RLLP0JTJEgBibmGvs/fc4PmQcqxucp2Fs0kMZ5WYItF0DzPmbdcX
waNzhg+MauksAsN2tm7D5a5yd7uTaSoTL09gfBr35gRBdKmg81z4ux3bttYYSQTF
9ioY7srrLj4QbHLLCfTqh0+MVvifbizFmNDuR29KuATR1391X90enKKpIm0S9ipH
aLaY41RR7PDA+qjtypnNr0N0ramUOP7MeAaEPPczIarmrz1K5KbJrcUz0qiEDLoA
ZggjdwIpYYlAbpCY3FYksI8l8Wo75sPS07scdUTIf16FwhwIJ6nqLIG3QG28ovpN
XCBdcdSvc3Ixt4wsoCJxguuUA7twFZHfoGDu7f7Dc7bdwm9UBJ38QL7frr8/UyQQ
Ltb2xTiZKsMFEc7q3KiH8y2Z1pjRuf+0ylkb5XI/5mClpr96L/lErMb6nn221qg
PldlVNA47EWriCXnvbCuf4ikKoh+h7F7LpmDpEmEj7JPgJLjDE8X3ShdTzZ0BN0eW
1JucBZVnMsVse0lddvc30X+BqiizXsNQ9c3atc9A0avuhsl0cANQoH9x08VRkZky
m2iHfeL1HbjRw+pchbdVfXxwlg0/+Afi0CEVKMHkB03mbbmFa9oFh9e8zQ0Uia9L
43TQo1X67p6s6KPi9o1r5/bUzNYtNr02jVd8TjCmg7m6JkustBXktJDs/iwCJWCn
ZQI/ghEtYaBtDGHfa18xiY/B/g6v8YkezPf8VXxlIU0rGTfzk3zk/PD3TnbRLy3N
ot49sr1uKpYYdofnGflec1XBVbvAVZsm3I58Mpdj0CQsLCxYNgxVPIhFkptUUjKf
/4nQ/X8kdmH5Gss97JF7P2+pw6EimubVOvHTX+gKbp1rHzWUEUth4JQLssH+8v+H
hoJtKrmhoEPysT+tjPJtbWmsptslap14bwHCfNrt1QnhsE6jrrPFIUB7a7DNL7D8
FDfRazcq1w0JGs4un6GaJ7d1CYzHrOVKR0c1T201uIwzJOyXU3+YgMYfWqIYViW1
AGWzj1PPXM8aICmdOyVpWomBq2tUa0fCSHSD//lltDpr3sTGahPvbV8clhQZzhKf
jyYq5D83dsNKFbcSnsctx4SP71LMaKZw9ttsEzHRRU0duUI149uKpRU0ciGPsSEc
gHhBEgKruGdxX9zWeGEFuBzrgpu3C3LXRbh1GNS7RbFLIIR8WZoD0cMPEVrOt4Y9
pOGMl1/8LiwQFeznZhQVIjLbjWcJdCqzqxscBh1TJKrj126Le1tFMmHaY147Sfi0
PORZOLmnvQxdAaFeN4c+U9pU8DZPMZFa3f3EmoMgi/t16vnw0F/eFyWz4GjNLqEt

```
d27PzhPuqYPupgCu95ZLV03727BMwF0+Z+Noqv/X5RFA8W3wXX6Cw0JsSYBp6Xn0
/HP6a5LoHU3yku+sC2C9EvVuPVEY/51uk7oIyT00pC6T83oa/mQ7xMMSfuzVcsKK
YLvHwwvXZK6kbyNS0ry0DE0wwXoC1UnJ5PEX7V+0ondyRxe0D5SnIGAIR/Sy1lM
qzSYcMRUGBmK56IirKZ0XmoM34Gv92Z7TNMUZLReIA01qUHMioIfaZ1Tp7gbgBZq
5P6nHYB/zZ7qHM/LPSZdWA==
```

C.3.16.1. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with `hcb_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"
```

```
MIIWVAYJKoZIhvcNAQcCoIIIVSTCCFUUCAQExDTALBg1ghkgBZQMEAgEwggUBBgkq
hkiG9w0BBwGgggtyBIIILbk1JTUUtVmVyc2lwbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtahAtc2h5LWxlZ2FjeS1yZXBseQ0KTWVzc2Fn
ZS1JRDoNCiA8c21pbWUtc2lmbmVklWVUyY1jb21wbGV4LWVhLWVhLWVhLWVhLWVh
cmVwbHlAZXhhbXBsZT4NCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFtcGx1
Pg0KVG86IEJvYiA8Ym9iQHNtaW1lMmV4YW1wbGU+DQpEYXR10iBTYXQsIDwIEZl
YiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW1wbGUgTVVBIWZl
cnNpb24gMS4wDQpJbi1SZXBseS1UbzogPHNtaW1lLXNpZ25lZC1lbnMtY29tcGx1
eC1ocC1zaHktbGVnYWN5QGV4YW1wbGU+DQpSZWZlcmVUy2Vz0iA8c21pbWUtc2lmbm
VklWVUyY1jb21wbGV4LWVhLWVhLWVhLWVhLWVhLWVhLWVhLWVhLWVhLWVhLWVhLWVh
OjBTdWJqZWN0OiBbLi4uXQ0KSFAAtT3V0ZXI6IE1lc3NhZ2UtSUQ6DQogPHNtaW1l
LXNpZ25lZC1lbnMtY29tcGx1eC1ocC1zaHktbGVnYWN5LXJlcGx5QGV4YW1wbGU+
DQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6
IFRvOiBib2JAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAg
RmViIDwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW1wbGU
gTVVBIWZlcnNpb24gMS4wDQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhb
XBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDwIEZlYiAyMDIxIDEyOjE5
OjAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW1wbGUgTVVBIWZlcnNpb24gMS4wDQpIUC
1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6
IFNhdCwgMjAgRmViIDwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW50
0iBTYW1wbGUgTVVBIWZlcnNpb24gMS4wDQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21
pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDwIEZlYiAyMD
IxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW1wbGUgTVVBIWZlcnNpb24g
MS4wDQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI
6IERhdGU6IFNhdCwgMjAgRmViIDwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2
VyLUFnZW500iBTYW1wbGUgTVVBIWZlcnNpb24gMS4wDQpIUC1PdXRlcjogRnJvbTog
YWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViID
wIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW1wbGUgTVVBIW
ZlcnNpb24gMS4wDQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0K
SFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDwIEZlYiAyMDIxIDEyOjE5OjAyIC0
wNTAwDQpVc2VyLUFnZW500iBTYW1wbGUgTVVBIWZlcnNpb24gMS4wDQpIUC1PdXRlc
jogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdC
wgMjAgRmViIDwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW
1wbGUgTVVBIWZlcnNpb24gMS4wDQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUu
ZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDwIEZlYiAyMDIxIDE
yOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW1wbGUgTVVBIWZlcnNpb24gMS4w
DQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6I
ERhdGU6IFNhdCwgMjAgRmViIDwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2Vy
LUFnZW500iBTYW1wbGUgTVVBIWZlcnNpb24gMS4wDQpIUC1PdXRlcjogRnJvbTogYW
xpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDwI
EZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW1wbGUgTVVBIWZl
cnNpb24gMS4wDQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFA
AtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNT
AwDQpVc2VyLUFnZW500iBTYW1wbGUgTVVBIWZlcnNpb24gMS4wDQpIUC1PdXRlcjog
RnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgM
jAgRmViIDwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW1wb
GUgTVVBIWZlcnNpb24gMS4wDQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXh
hbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDwIEZlYiAyMDIxIDEyOj
E5OjAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW1wbGUgTVVBIWZlcnNpb24gMS4wDQpI
UC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdG
U6IFNhdCwgMjAgRmViIDwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZ
W500iBTYW1wbGUgTVVBIWZlcnNpb24gMS4wDQpIUC1PdXRlcjogRnJvbTogYWxpY2V
Ac21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDwIEZlYi
AyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW1wbGUgTVVBIWZlcnNp
b24gMS4wDQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT
3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAw
DQpVc2VyLUFnZW500iBTYW1wbGUgTVVBIWZlcnNpb24gMS4wDQpIUC1PdXRlcjogRn
JvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAg
RmViIDwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW1wbGUg
TVVBIWZlcnNpb24gMS4wDQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbX
BsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDwIEZlYiAyMDIxIDEyOjE5O
jAyIC0wNTAwDQpVc2VyLUFnZW500iBTYW1wbGUgTVVBIWZlcnNpb24gMS4wDQpIUC
1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6
IFNhdCwgMjAgRmViIDwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW50
0iBTYW1wbGUgTVVBIWZlcnNpb24gMS4wDQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc2
1pbWUuZXhhbXBsZQ0KSFAAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDwIEZlYiAyM
D
```

Page 196

```
iffRTF/KtmVEDMR/sYeqAH83KM5p3e121Vh40HhyI0qNuz5oShNaACSioQ23WxHG
Vy9vsdVfnbhsp1rWg9NQ2WbpCmK+2oMh2oYl0Z/wvXmt9cG6jbMvcdH4z0IOvg6m
rYkKTM/RCGnumghxwYToj10yD5Gs4D2IJCw+fx50Dxh52MbNRYXTus2ZPRPM8JXN
QC4GWv4km3M4rKnJDd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk220H4Con1B8f
7R7s1LM2cSYxggIAMIIB/AIBATBsMFUxDtALBgNVBAoTBE1FVEYxETAPBgNVBASt
CExBTVBTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFNUGMgU1NBIEN1cnRpZmljYXRp
b24gQXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrOmqnXMAsgCWCGSAFlAwQCAaBp
MBgGCSqGSib3DQEJAzELBgqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIy
MDE3MTkwMlowLwYJKoZIhvcNAQkEMSIEIEUN8MCE/gE8VaUW0ZYNYiuSDKZahJ0b
CB59LQgqpU11MA0GCSqGSib3DQEBAQUABIIBAEk7y6K+3YZB+tri+EVQFLmb1N5K
CUsnwbyLw19bH3bv+8MFEYqYmiATHzim0xdQNB18c6HR7GqnMQVJIZ+0EYiL1fz/
Ej7Up3VQzyR1Kvb1L4Xt1W7+ITh/6iAx1j1W48US9pMR+05Rz+cfVATn77voVNs3
fN0B8EsjPoVM708f/xKD5lwHv/72Mg1fUTs3YMaqabplXdABkdp1lQhZ6za+N3/k
yEYSmxz00wd4JRKuAIdbzdFIC57BIGFICQX0Nr1c3aZ/wHvNvH2x0Ap1cQ7M6Nu3
KImZs860BQmc0Kdk8AzE4s0o8mtf3uhU+eJ/23FWjMYpGdgHaUu90GMnKnM=
```

C.3.16.2. S/MIME Signed-and-Encrypted Reply over a Complex Message, Header Protection with `hpc_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

iVBORw0KGgoAAAANSUHEUgAAABQAAAAUCAyAAACNiR0NAAAACe1EQVR42uVT0xbA
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

MIIbnAYJKoZIhvcNAQcDoIIbjTCCG4kCAQAxxggMQMIIBhAIBADBsmFUxDTALBgNV
BAoTBEIfVEYxETAPBgNVBAsTCExBTBVTIFdHMTewLwYDVQQDEyhTYW1wbGUgTEFN
UFMgU1NBIElnRnRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
BoQ0MA0GCSqGSIb3DQEBAQUABIIBAAANFe+QhN1IuF/acKoQk/CrT7s6ncIXk72bZ
yqANUj5IWD/YQPJMczB4khaPZRacFIWSbcn3RHR8H9kaIncGgB0F3pw+Ju1CaD5x
Lj8pX3ry1b2BNFPemhbHQy4RsrZpwmL6qSc5X/qWbJNvA83xnnE+avEzW4JFwH1l
RRABOCiNe+1RF7L+X/kqJL0oALwBWLn10sfK5AwCg3Vao4uyRUTRbC8P4Q7v+KPi
6qYEwXAe6gz1LCwD/EPyiDnMB1bNBid0g8nC8pt2Ymbz+SljAW9FDv9Xyv8iJuXT
+OXOgl8pfBA1a4zKGiRZRkN0PDF0NUh13p/0h7Wd/322eR+FTuwwggGEAgEAMGww
VTENMASGA1UEChMESUVURjERMA8GA1UECXMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQUU1QUYBSU0EgQ2VydGlnaWNhdGlvb1BbdXR0b3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAHNO6f6aUb4tfH2tb0Wz678eY
tSslVolgGLYIrJcX3Xz0ZVEg7EHJfwMMrfzuvaXtMu3VR26TZpJxJrUQy5bp1IKf
rb4ZF95XeC1KMC5E88kpOX3qb+ALpsnRbUvldPfaG17GQ11LXRML16Xvw2BdQ/p3
03EhpITTSdzFYJ0jW8J58JGe1M6sjsymI0KJZdEtvG77dNhNAXZfmbf+fBUZ+237
Kc0nbd3dWtNmriJONPKwK5qF1U01JHhGX8/UquWY7bjXYv/kH9YYZUnR3VCNFQZn
KndxvfG/jJ3HofDM6XgEZf+hogg9JVg9LN5IGmdmau7/YSt/7q8k53AL3YS7ADCC
GG4GCSqGSIb3DQEHATAdBgllghkgBZQMEAAQIEENLhBGpw6GdtyReA3vbppXaAghhA

```

yG+aQIQUVygKLkRUL7c+MZNmUhd+I7X91WOHMLTQnrHagQoCx1Kw9b3v7LCUbCL
SabxdNhhBnQwFpgec8aHPFoJjM592Zg/7AnYYDqMAttYhoabFG7wSg7+nt1JB/AX
CGFWd1ILOThR/PghR4rgOm05/FosuV0PdfBrshG2Co0WzeLtFhzUle1iVtqxq+1z
Varyg1qLwtXMAKMP052WmVhqNw9WSsvIXXYCjWdbn7g+1J5N1BfcjHXnJn8AjL9
1IzHmuHh4ZW9C8S95gdrn8ipd0oe1Ubpu7KP5C/W1H9MDU8cesFcMmUt/WLNxeb
09fV0ILaXDbnLIVTQ3xHdoQzg+TQCB4300i2Wvp6UhPn1E6Ap5mexGvObW1IIEF
RK041WVNxEoGB223n10LH6mqJxpiqUK9SYIhNCfo8uxIdZ5R49B2jbzC8e10wefm
i1QII6ZVnwPltALSvxiL97GSHG/32YmITrsZBpTitY7Q4tcDgzfFGRV23R89yorp
AuseNYbGJ5Mb1qFtbQZKycW+2RX16qt4hlcsf6wYBCzI9x0zsSCHJW4KVZc9GuIu
0Cmc3M5mFgrWwKhCvdJBofLwSqTTj6moGmqBLIZ1ouiam00zxY+VBrpLNSrnnKf
SdEUgsHujKo+A+oy0vvhYZqusnoE4o6vE5Sd/R11q6550/jI6ngCE70yZpcCxCxV5
0JgsFeUSjBLtIqGVGPwKRAreug/2rcRWDB1W4QTZ0Yuw7Zu/xVPkAevp8Hn6v0C2
rxEpaXnhzITeCsS0qLN+G+vuQAZDxz4SlpWxx6HajBToje79ZtuF/YzAZfJTWSK0
Mzx08h0CxEl/7z355AmXrKF0ubZj+/Y9UTXLSQUUXV/5b0L98xU5NoAaAhzssysb
fXLHg1iCXMNZBUL6Ukv2ovWz/9ICXHd3GdmNUW10IFRmPdY4obnMtCN0Jpkrbz81
2Uilu0BVtsvsAmhfzgo/v7MMAoeFLkc+idCOexM3v4H2tQ1J1V8MB+yz3IbM4RMA
UvnAn1fxjsR7Scsg0txauodF1tdyWA+FnpjJwT9if73HZ2/Lb8bs8ri5iv5J1+X0
FjsmhyKMUEmLUXbJ2omjDnnYmYzogYXTs5XSmrZrjvoIbQAKtmxSKywQRNFHjei
81VcyyWadLUCZn7PdoQ5qtxSHPRr7upARLAHh1jWAL08MHfJSNyN93jK1Ktxkefk
9/k7WAWsYvkyhGBBo1vydzUpK8GwS06+at+UGgUH0Ts69RrwnNWPwjjuw2sS9hX8
DHy0eGAKKAIrhMcNNJqjnQ3aEP5imIVhTlh9ZEKQzF3ywpnlpAfGdBh0Qkq4cn0p
NVpG+cLWt/ccY/ROFY3bMAuvxYOr14fJNCtRbBY6uTpgSKEoQzY77NZ0fk4I1VcU
NA1pmf9+ZysrYblQB70TggQSB5R3Ik+Xr+BzS7x+pXiBuFLU7qSnxXmLIzyK5E1U
HfHkeAIAc8ReUSSomobY1+2mmyvvWCLqIR9K3FtGtweZ9bQ3NY310u0NJAldB9Ge
cH2MdHvckaTJNx12aDKA4bm0gHEX6XXDzKARPbcbHDeu+eJ3SbGJ1C8XBqrXxgLJ
MxUxTVa3uc+Dk7ZY4jzZbGoRVLsUFvCnJk1k64GbzydMGplEPH2gR2fjecRbFknq
6DWdaM1z5J13GJbi3g2mXo2JiWuUBQCLnbdKTabXdNDBFBU1oVVqMK5PDrQ0cExW
Dnxa3r3ae2W6Pfvk6sS6LzpvMJUhGfQzhdkgBrfGrMaM7FG8hdr0ZAqJxhu+vS0c
ts3hiS77m/KQhyeEPzdNkVXAUAHAsaHQ9PgEc3E6ZHvUIdJAYBeQ3e4kXhZZN/NaV
fAlGKp1ZjWc3RYQK0h2f6ADxcdG3GHAe/vHa9QkrWHUS4QuX/h0aFYDX/bwAg036
wsYK8WUVTtpItYfV3jTmbfAuLL8En8qYgJNPQcb1S00C9Sv8qBg0PS1SRQhpG+oW
lkWTEKOn4X0hfV2uo4XMIff93SMvRss8vmmB0Kjryr92tGX3CdJWJTjFJAtnBVO
70z51D84LLJW8vyGMvZ4trxnblVlg9REopeDVq2BJeznYHz0QoawXVM4n8Z0vgp4m
xl1eVprwb8nmVUy0vxozr09V/ki9aSwZIFnHdMaVX3qwXUZ/1eu0AJJ395Ea6M4o
hM+Iqv30A19496kpHp8sfYeZsHtNNwQG4WbhpnXAdR5pJ1+CMj1iLFgpkfmWXn/J
KIF20Sew31/v7JtxUU0HBNNvs+SxLwDqFK4Rju0UBJNEA0EgCvkfpdyAbqCS15g6
fx6do36Gz4mxXNMJRqP4qunv3MVxEb+igwEP0eSxWpw9vP7XaFiit91EuoJ9/UIc
R0q0Vo3JuB9XM925T7erNHHkhd1UW2utiSjUrH0U0PIZqzbCaB/L+Sb1HhnAKFDJ
Rg2u5D5Mwv5BdpBTnPMq4Wz3kzvuIop7hUzoCVDhcM4a60IRXgyGeKH0s//ca439
zoy7aNurEjQSKjFs4dfj5z64b1GIu33X/Gpg634bowErRXGQ1Fp0y6oGnD8Llk0V
n+VODMvu5HTDcYmmNtWLRBImmdq4Er8gUN8LjZIOh/z/F+QSGWoW44pHPwvCV6/k
6RFcaQKsPx3PHPqRhM9yAmhTWobM0nJBTLccFsxYQWxe2t022B7Ecd0a9QjT70kF
+9KpNTPFP1YPMKi1F+IGf/g9KgVd6UHSQoTQ0mun0NXjuKcebamy4kRwP72q0qj+
jDMB1G+jC7I9neZ1/f50DT26av9B8HfyxVuzTBg0mDSCYvrA+yxHFXiyE09zH5fv
oq5JRT2rXTyq2RZ/EUy0a5Ye0HUI2/veje9C7y0QMyJcq0FWukw6y/BH0o6M6q//
y+S9yMevzh8oxjkjCsx/lrM8kueF2k1UxG/Xzm+uR3Peijqlus961Lx5d4qY2XQk
gIVsKphv1I47AYxtDTPx+mXRlm14NV11skrcOppwfAvXwUBiEuxBrVrrBafj416M
VsZKHsELw6Ub1/6NjEkp/C72s0bqRkDna0Q41s3s1N23wy10kWooujWI+w1r9E1Q
RT8u4kWJtgBJYGmiBRWN9jMxaOpcf4VrU0HpxNpY7hITQ4b6/KB/28UE8EB+cFp/
NmC6+vx0jKPGsLYGe0eaZoUUVXW19PmV+tbvRbRSxcLDSzSBRvCsEoeK+KBc+r3
7/n9Z5BVH50RQx31K1AEadF1LXVVANh/ZHBrC4TBTaFMGvgJjQZJ3Eax/RKkS5oN
/APYHw3zDNFWyhtXrTL0tEG2oyppspUmfG1Zw1AlrMa9dB0kRr3iK1VlyW91t0Qu
8Q8gDHcdNahMDHdTAieb5bU5nd7Qr/2uyHIG8sswxWH0jI+137Qq6sg6wNfq6Xhu
to1/MHofcQLmiQGVucZiaQR82TjNzo99ezyu9ZAbu3J4pm2pLmHeQjg2m1+T09NA
jdctddks6cbw/bL2yFGw3juupSLTYtYGK9uWqvHSp306zLS2b2ihEPBhe5V2UgLh
Xc/CvGAwBLTJgqM64FuUPsDjXByGcGreSA3bIG4AU5hhD+SwSoaFE53Qw6FETH4K
BVcGedXnmvkdZrDxwSoRpAQhAKPdrxY+y71Fiv/dGtFQtMCYv8f1AP/bvTWNung
wZODrmw16rJj10oub+PIT31MXmm+FbM6yFq3EtfZbq2bKivzHUZpiwL7afe8s+RD

r1Zoz4y2v0Jwi/REMIDLk1q4RnFcc+FH/ZaG+gMdfkduY0iGfyqIIJeQx5HXhTDV
gxoy356pQ7QCvDAUoyP/7xp9gKqHbANfT77ZM+68KGPKuEi6byYJki1gXrB9oJL4
JmF1jQSZMYqj+FGZBbrC9G8t7vTiF+80xfxxs3G+GVdCGAEjhz4dQww1o4vIBmdy
mrsTEs205qd7Asl0du43DZrXSBt0ppfTxTEjrosTzRD8Skd9AvhFGKhtSfGPNL3
8UqnQE6jmbHHKQt7Z4DJTQ/ZyheYUawAPLLbpX4C0wUHD08YawF+vghitdt8K2+v
4dkQh9BdyFXpfqXSBDA6XcQPscLxHwjFJPczCeATuycA7/bNgs47InBGg5n+Z2/
neb0emWFi0d9Fg5uM0BruCheHCNPN9BZ66RQ7FL+jbX039Tq+QX/NnzW3WBnoTDJ
GEzULm2VjTn18gMlfl1VRjNENOC1yUH3E9jWMn8LEuTnUXTqfEfkKj9lwUXQxNeYf
uVvJ95gDas8aC/O/MmHLc6CFfq0l9MGU4FYXMFron6cfJZCpgfXQnJAqx1xMb4wI
qMUyCSzZ3umKCD+Uaf7MIMyCMEDOMLFo06LoNofFjNooK011sR4qJcM/zXiFZQa0
eCoxyIBESCv2h/LeGRW6Sx7iacntg4Se12zPlaG7ckuiz6PCY92g3WGj9E4ARWIB
VDIkJo74MDUSn1osHHojKd13lqdAH7Am2UjoIVogx8cE9cSEnmZfwZBf2Pb2TxwF
FTWG7TqheJzJxWzj14sjMPwBZRJQCdmscn8XWEEk7BBUEGbZi/3Y+PIMe9G1ZYF
3bu9GNmM4JcSdH9FX0NSUdQrgqDey+C+UCjFD1GWY1Ja18vHK1C3ssWd3wWFBFLF
e3/Vg4GZhYPSgmTVRk0l0pGR7XgMEBbGGZgloknFBet1J8F6qIXy1DNsMTQ9tNJ6
rBy0Ite6Qcvma+bz4CSR+y/FWcy93BFKVFC6y/izfdK5InHlrgBEZugR2rR0oPsJ
wXaoSHrkza1TiW/CsghAx1bjQ4Z1YtMaSfC003nKQ4z32hFcxm/de3ZUJWlaEp50
w0c7kqIzFD2w+UvtcceDo8uc7weRtiYi99K8x0ZtXTfSjWwcJch5Unpcd3d0XVko
x+ag8enG3DfmVmBvXxsyCboqXJj7FWHfYlCpKZXe+0GDj5Ms3wno8JH8aKVdrSYR
XmNzsJP9a2CMSEDhaXfaWHQqYSrV3Eg2WXeCbGHUHPCUF5f0uc9RXNN0Wtb/MBuv
dcCNyTfXyNgT21vpQ9VxLvFjw7Tt0NjLa9URR0bzZrd9I9g0MJrmw59DJm2kbBoX
3qcIq4B693ajEaJC2qpBAstTCEq0AcUzAaf4KunE5LwGY/iYzxngrIw1EljyPY+F
wYgGiy8hMkQsZfgwBnzZvr9jhg0s715VEIAMJY4cd1MhRVUf+nViVTxHqS0raX1R
I886EZmgNqMIXoJQinAaitUNIucxft+vrfXBhBnG0nvIQI807wY2CHQhcrTbLX5v
hgNnKY2Hd6EqYnWRXGL59jgACyfyj0dbdEsWtva20reWMx5fcPkVQ500H0E2hdfa
yBzIjXv0vkSLLwsLwPxcbu0S92YnFr2Fr07+G0w99fjGT/xnOhVEwkvzHjFzzzlo
fhSumEUfU6gdYi6fdjngVQxqdz/rfCWqCj9IEUrJxKUnsU322RV6vutgOjQ8ENkz
zqdY/TOS/2onRIIsaE/u11P6Cvc2XezmZI4819aARPsqrTzeH5nVE3D6EWrieDhh
LOmvIEkE64ZIKwUfG8J2hs2ALyrad1ECpQKBakW+f7RgFrZnui/4LIW6Hxwe58A8
/SQvMf/OJS7dtwX3a3Z4w2nnnp2oXV1MgWvXnuEIPYDQdaIqh1CRJwk1fu+Su7Ys
2kf0s+Czz+nBq6CRDD20YpP3rBurR+JmdBfyvR10a+pw1WqWaADYfzmvKNXcikYC
h8xCp23xL7p62XgVwVtUEkbrQJBbCSHbjZZxBx+RmAoYcThcsggLLLLL/RHKGRqQp
XI3gFKEy27HV6X4G4qMkJhzuCAvHASoSQj4g/KLwaYf+njxeRSzwPRkjCn7Z0Men
EQreLcqVHQaoR4Exo8qFJfizkMrEr1uTRtyxFcvqJcLUffPhfUWAuPwzS+CeiK4F
Y+hLYxzieVmP4lpxu1spWJfQgU105/6pj0051nMwjpfJpB3tjFFYKhKrmjHqRSHX
owguPcxkPMI/SwpRZWRR00MSzh/ph61R9E/KyeaWGTjDCDD6tdCjsLGHCuX3UzZe
+AMiDhW1AWw+HkmkLEOym4hbQnQhwuzYLUS6Cab/oN/UvBnjhrIdG8s3YF71PvY+
yPcq8AsmysxxVvL7Q205BeX8nRNhFeJc3asMBvSijuo1VMiGY/0wzzjasWZH5D5b
KTBjIqXP57aNaW/BG6eIiaSxVoLnsbgW57P0mpP5JxK4f6cvMPih09rNItSqESuK
6oDyXjXzJaYblhr0Jk0kVp4gjpHMmcsc1oruQDzWXMUNpdvPUnYnZ0yYKhmdbHo0
n+AKgwh3tmqItejAdRLthS3bwMdwgEEEx2sfnnnKwEy6Xqdu5oaB8rVRtKcMxFivA
NVefdCft4+2brFXPQv2HsQWYdVcdZMdUT8WLL7VUJ2mXiVP5422LEspTxfgBb6cV
jbfKu6btpQ0dIEux9Ykd9zH5ye54Dk/FcElFQah9MGZ0GS2P3AKFLcLLxmpRHWFv
2SE2EEKTQzp25c67nzd3/r8LNAmpkqTVHuuIvuMZgP9xIi0uYUzGrUL7k5EJTWk
OMPRQeYS8iv9v3QEarSPCJLyeUpZjXVU50u1kKgLAuA/s32/aVwGuTCUMNgGQx2q
jpozo5jYDAUv3l9EitrcM9X9WxvYP30rsVs4kNvRM08RR2wfs6sHb//t49x0L3hW
mbpAXbFz1WXIE+VvVo09ZCsXx3JBRkWyxoUpDibijBQirYkwWx+TdDm4DP27KdM
w70bRhM5jVqsYUGIfA756WFIpoaXrRpCHja1ZXyaFs8pyoSr7XZIZ380A8kexEB7
XskfB3vBf0gcJsYVn3ebojEPFSjC4ayUxJxiNZVtluyIcz0gGdo5AWGo/0BstfLI
nFbx+4D7xH2SwPC2XQIXrYJnsawqEb0H4+hPVg0C5fnqK7QrjVWLKx2b64z+VowI
xHyiHfWrcAfMygh5YBAQp/XoLzDL65VWKYbCV0UzFy2iwfoTs1RbqcAPRhjjdMJS
U/ep/EBPa8bF5KNKdqG80hcT0Y3iFEW45k06E6kXs2w3NgHKhrU1wY3FLDD/w1u
f7SjMtPVN1HEhrQoEUGP14fztUBRuC6I2vy0jiJ0RaJG+TU2Z1Ks2sE5ey1EUKnk
dvETYA8Qjso3JYb7WWMRKTtiaXj/tPMVGvqfD50QxNLGcvS1qjds5eNMuXHuof1C
fyubt0U6FmS2oThM6r6/K17GXjg7Usui1XtL8ATuMKMn7nQG0zQJpFeDawJER6KB
8vTrjgYlZQkni25eIi0LH1XpaJXUIDWIyOeDxYCr19BQHukf0a1o5f7WQ56cp2M7
if3rUpGk+50tx2RWB1WvzVJtF5HEB+1xbaaEaMCqS80exHWQUcZApzhnQC9NeniN
8oelZkojmOPHUNZti4lZBwqJvVj4Ag455hWXMzy8lqlz0ivvfYzIquQYaxozXS

PHR0Pi0tIDxici8+QWxpY2U8YnIvPmFsaWNlQHNTaW1lLmV4YW1wbGU8L3R0Pjwv
cD48L2JvZHk+PC9odG1sPg0tLTU3OS0tCgotLTE0NAPDb250ZW50LVR5cGU6IGlt
YWdlL3BuZwpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nO0BiYXNlNjQKQ29udGVu
dC1EaXNwb3NpdGlvbjogaW5saW5lCgppVkJPUncwS0dnb0FBQUFOU1VoRVVnQUFB
Q1FBQUFBVUNBWUFBUQNOaVIwTkFBQUFjRWxUVVZSNDJ1VlRPeGJBCK1BZ1M3Mzlu
TzNUcFJ3MjBkcXBkZkFSUUVqT3l3aXdZbkN0a0RLbmJjTGs2NnNxbFQrenQ5Y2lk
a0UrNkt3a1oKc2dyemZjcVZNcEwyam8wNDQ3Z1lEcGVBCmsrT25KSgtJaEFmVFBS
aWNpaEFmNVlKcnc3dmp2MFpXUldNL3VsaQp2ZFBmMVFaMmtERDl4cHBkOHdBQUFB
QkpSVTVFcmTKZ2dnPT0KCi0tMTQ0LS0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0R
OZdKzkJU6HuPTQGirQwDQYJKoZIhvcNAQENBQAuVTENMAsgA1UEChMESUVURjER
MA8GA1UECXMITEFNUFmgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQUU1QUYBSU0EgQ2Vy
dGlmawNhdGlvbiBBdXRob3JpdHkwIBcNMtKxMTIwMDY1NDE4WhgPMjA1MjA5Mjcw
NjU0MThaMDsxDTALBgNVBAoTBELFVEYxETAPBgNVBAsTCExBTvBTIFdHMRcwFQYD
VQDEw5BbG1jZSBMb3Z1bGFjZTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAJqVkfLwLjJ+gBUCfkacKTg8cc20tJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg
9r1mAfIDlB/wlbdmadXPmrszyidmbuZmOpB5voVQfiLYYy3i0x7Y0qzXrl6udP07
k0sV+UdSNRFXrfKeoQEFXg0aGdmnx40G/e3p1fIKM0dPzZLo0AJF5m500xzXPL74
zFCWp2f1ZkuE4A6l41koaZXCN5XL7wWTLMLenF9Byb5ksKqUuqEHAMd1nmoNMgjY
9VfVfcv9w43GG8FtpSX+TWzB2zNS20F+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r
8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAA0BrzCBrdAMBgnVHRMBAf8EAjAAMBCG
A1UdIAQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbG1jZUBzbWltZS5l
eGftcGx1MBMGA1UdJQMMMAoGCCsGAQUFBwMEMA4UdDWEB/wQEAWIFIDABGNV
HQ4EFgQUo1NB1UQ8gCkVfAEj80e0r83zdw8wHwYDVR0jBBgwFoAUKTC0fAcXDKfx
CShlNhpHGH29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCCsTKcFqQMPTryujRG
zJdYA+R9eBAuDLsatbtKt14FzkRyOg31/+Cw7H8e30iLrPIF1WN1qjHrjg0yIs5
AQ/hgxLvLir3hEUVZ2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5U
zpEYPLr0r2X4P5uXxaP0LIZRzWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGn
UZROsVSyKgiWdp1JhqXwfDz8A0enITGXnoEkAFvVjiCqh64P1hIeMorj36pgL19o
WZD6YrzSWHuZ1F00juyu0fQsqm6hvrDTqNpHNZ015f0URza1SkCvi9GFmNUPoVgw
ggPPMIICt6ADAgECAhM3QV57XV/QqmiXDr0+Gr0mqnXMA0GCSqGSIb3DQEBDQUA
MFUxDTALBgNVBAoTBELFVEYxETAPBgNVBAsTCExBTvBTIFdHMTewLwYDVQQDEyhT
YW1wbGUgTEFNUFmgU1NBIEENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEy
MDA2NTQxOfoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYD
VQLEwhMQU1QUYBXRzEXMBUGA1UEAxMQQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgWPK2af0+StijSNOR8K/hN8D+1
078ou1lSk4ASvSwjsCNo7sHUa4xQU15J06VqY18LANw0Rjrc9BaX4MguzsbFXBe6
uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEO
ls/gkUP2Gxzyms02kaYWTut3SryCqeHEFbZfKb4urMk4xrIJC3CzWruS2Q0FHbB1
fkgKN5wXVgkWFfi0ucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H614Ku
ElNAtJ7BtZcs17dUy9u9C0gEyKriVokFQgQ7XNDU+r3Se0Wwks7AgMBAAGjga8w
gawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOA0AwGCMGSAF1AwIBMAEwHgYDVR0R
BBcwFYETWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDA0
BgNVHQ8BAf8EBAMCBsAwHQYDVR0OBBYEFLv2zLiThQYSHJeuKWqQENMgZmZzMB8G
A1UdIwQYMBaAFJewjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IB
AQBziaI2p86poGkjD/4Kkk0HG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAo
cCn5zbzhW/JVdYn30UxfyrZlRAZef7GHqgB/Nyj0ad3pdpVYeDh4ciNKjbs+aEoT
WgAkoqENT1sRxlcvb7HVX524bKZa1oPTUNl6QpivtqDIdqGJdGf8L1zLFXBuo2z
L3HR+M9CDr40pq2JCKzP0Qhp7poIccGE6I9Tsg+Rr0A9iCQsPn1+Tg8YedjGzUWF
07rNmT0TzPCVzUAuB1r+JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSr
JNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCAFwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRG
MREwDwYDVQLEwhMQU1QUYBXRzEXMCGA1UEAxMoU2FtcGx1IEExBTvBTIFJTSBD
ZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69Phqzppp1zALBg1g
hkgBZQMEAgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJ
BTEPFw0yMTAyMjA5MjA5MDY1MDY1MDY1MDY1MDY1MDY1MDY1MDY1MDY1MDY1MDY1
4jEbYj1qU5Tgru11NftjsHf5ojANBgkqhkiG9w0BAQEFAASCAQCPddNT02dMep9S
Ux9R61FJylyqjA4n22MbI3haUrxV0gk1+FAacmva+eo8weKDd+FR3fYuy4C+PkIj
woc1AH4Hb7QkNHQgv5DSuvqN1/QoIHGvF0atF0NXK0irYFGIZmeytKJJ9WR67A1
Myuh/Yi8aaUDheliEIPsD+59pFRHDZicM1MkNuSJGw6LHMCHSA9p7WggrLrD8trC

```
rR/xL2ZWbswb5sr3Y6NucbZS51e0UAY2fKzxK/CUFG/M4VhFQF1UgUZU/6hwXHMg
ffr7xEDPeco1Tq7/fCLCVYz5Ixf+RfC0id7Gps07qsQlMIV/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

iVBORw0KGgoAAAANSUUEUgAAABQAAAAUCAYAAACNiR0NAAAAcE1EQVR42uVT0xbA
MAgS739n03TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+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:

Composing New Message

To:

Alice <alice@example.net>

Subject:

Handling the Jones contract

Send

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

Thanks.
Bob

--
Bob Gonzalez
ACME, Inc.

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:

Replying to Bob ("Handling the Jones Contract")

To: Bob <bob@example.net>

Subject: Re: Handling the Jones contract

Send

On Wed, 11 Jan 2023 16:08:43 -0500, Bob wrote:

> Please review and approve or decline by Thursday.
> it's critical!
>
> Thanks.
> Bob
>
> --
> Bob Gonzalez
> ACME, Inc.

--
Alice Jenkins
ACME, Inc.

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:

Replying to Bob ("Handling the Jones Contract")

To: Bob <bob@example.net>

Subject: Re: Handling the Jones contract

Send

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.

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 `hpc_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

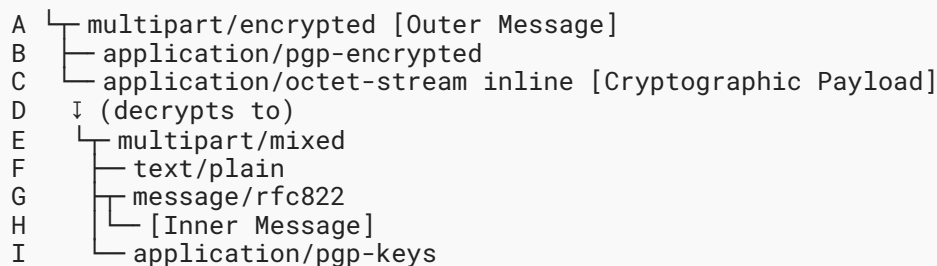
S/MIME [RFC8551] (as well as its predecessors [RFC5751] and [RFC3851]) defined a form of cryptographic Header Protection that has never reached wide adoption and has significant drawbacks compared to the mechanism in this document. See [Section 1.1.1](#) for more discussion of the differences and [Section 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:



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