
Stream: Internet Engineering Task Force (IETF)
RFC: [9216](#)
Category: Informational
Published: April 2022
ISSN: 2070-1721
Author: D. K. Gillmor, Ed.
ACLU

RFC 9216

S/MIME Example Keys and Certificates

Abstract

The S/MIME development community benefits from sharing samples of signed or encrypted data. This document facilitates such collaboration by defining a small set of X.509v3 certificates and keys for use when generating such samples.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

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). Not all documents approved by the IESG are candidates for any level of Internet Standard; see 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/rfc9216>.

Copyright Notice

Copyright (c) 2022 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	3
1.1. Terminology	4
1.2. Prior Work	4
2. Background	4
2.1. Certificate Usage	4
2.2. Certificate Expiration	5
2.3. Certificate Revocation	5
2.4. Using the CA in Test Suites	5
2.5. Certificate Chains	5
2.6. Passwords	6
2.7. Secret Key Origins	6
3. Example RSA Certification Authority	7
3.1. RSA Certification Authority Root Certificate	7
3.2. RSA Certification Authority Secret Key	7
3.3. RSA Certification Authority Cross-Signed Certificate	8
4. Alice's Sample Certificates	9
4.1. Alice's Signature Verification End-Entity Certificate	9
4.2. Alice's Signing Private Key Material	10
4.3. Alice's Encryption End-Entity Certificate	11
4.4. Alice's Decryption Private Key Material	12
4.5. PKCS #12 Object for Alice	13
5. Bob's Sample	16
5.1. Bob's Signature Verification End-Entity Certificate	16
5.2. Bob's Signing Private Key Material	16
5.3. Bob's Encryption End-Entity Certificate	17
5.4. Bob's Decryption Private Key Material	18
5.5. PKCS #12 Object for Bob	19

6. Example Ed25519 Certification Authority	22
6.1. Ed25519 Certification Authority Root Certificate	22
6.2. Ed25519 Certification Authority Secret Key	22
6.3. Ed25519 Certification Authority Cross-Signed Certificate	22
7. Carlos's Sample Certificates	23
7.1. Carlos's Signature Verification End-Entity Certificate	23
7.2. Carlos's Signing Private Key Material	23
7.3. Carlos's Encryption End-Entity Certificate	24
7.4. Carlos's Decryption Private Key Material	24
7.5. PKCS #12 Object for Carlos	24
8. Dana's Sample Certificates	26
8.1. Dana's Signature Verification End-Entity Certificate	26
8.2. Dana's Signing Private Key Material	26
8.3. Dana's Encryption End-Entity Certificate	26
8.4. Dana's Decryption Private Key Material	27
8.5. PKCS #12 Object for Dana	27
9. Security Considerations	28
10. IANA Considerations	28
11. References	29
11.1. Normative References	29
11.2. Informative References	29
Acknowledgements	30
Author's Address	31

1. Introduction

The S/MIME ([RFC8551]) development community, in particular the email development community, benefits from sharing samples of signed and/or encrypted data. Often, the exact key material used does not matter because the properties being tested pertain to implementation correctness, completeness, or interoperability of the overall system. However, without access to the relevant secret key material, a sample is useless.

This document defines a small set of X.509v3 certificates ([RFC5280]) and secret keys for use when generating or operating on such samples.

An example RSA Certification Authority is supplied, and sample RSA certificates are provided for two "personas", Alice and Bob.

Additionally, an Ed25519 ([RFC8032]) Certification Authority is supplied, along with sample Ed25519 certificates for two more "personas", Carlos and Dana.

This document focuses narrowly on functional, well-formed identity and key material. It is a starting point that other documents can use to develop sample signed or encrypted messages, test vectors, or other artifacts for improved interoperability.

1.1. Terminology

"Certification Authority" (or "CA"): a party capable of issuing X.509 certificates

"End Entity" (or "EE"): a party that is capable of using X.509 certificates (and their corresponding secret key material)

"Mail User Agent" (or "MUA"): a program that generates or handles email messages ([RFC5322])

1.2. Prior Work

[RFC4134] contains some sample certificates as well as messages of various S/MIME formats. That older work has unacceptably old algorithm choices that may introduce failures when testing modern systems: in 2019, some tools explicitly marked 1024-bit RSA and 1024-bit DSS as weak.

This earlier document also does not use the now widely accepted Privacy-Enhanced Mail (PEM) encoding (see [RFC7468]) for the objects and instead embeds runnable Perl code to extract them from the document.

It also includes examples of messages and other structures that are greater in ambition than this document intends to be.

[RFC8410] includes an example X25519 certificate that is certified with Ed25519, but it appears to be self issued, and it is not directly useful in testing an S/MIME-capable MUA.

2. Background

2.1. Certificate Usage

These X.509 certificates ([RFC5280]) are designed for use with S/MIME protections ([RFC8551]) for email ([RFC5322]).

In particular, they should be usable with signed and encrypted messages as part of test suites and interoperability frameworks.

All end-entity and intermediate CA certificates are marked with Certificate Policies from [\[TEST-POLICY\]](#) indicating that they are intended only for use in testing environments. End-entity certificates are marked with policy 2.16.840.1.101.3.2.1.48.1 and intermediate CAs are marked with policy 2.16.840.1.101.3.2.1.48.2.

2.2. Certificate Expiration

The certificates included in this document expire in 2052. This should be sufficiently far in the future that they will be useful for a few decades. However, when testing tools in the far future (or when playing with clock-skew scenarios), care should be taken to consider the certificate validity window.

Due to this lengthy expiration window, these certificates will not be particularly useful to test or evaluate the interaction between certificate expiration and protected messages.

2.3. Certificate Revocation

Because these are expected to be used in test suites or examples, and we do not expect there to be online network services in these use cases, we do not expect these certificates to produce any revocation artifacts.

As a result, none of the certificates include either an Online Certificate Status Protocol (OCSP) indicator (see `id-ad-ocsp` as defined in the Authority Information Access X.509 extension in [Section 4.2.2.1](#) of [\[RFC5280\]](#)) or a Certificate Revocation List (CRL) indicator (see the CRL Distribution Points X.509 extension as defined in [Section 4.2.1.13](#) of [\[RFC5280\]](#)).

2.4. Using the CA in Test Suites

To use these end-entity certificates in a piece of software (for example, in a test suite or an interoperability matrix), most tools will need to accept either the example RSA CA ([Section 3](#)) or the example Ed25519 CA ([Section 6](#)) as a legitimate root authority.

Note that some tooling behaves differently for certificates validated by "locally installed root CAs" than for pre-installed "system-level" root CAs). For example, many common implementations of HTTP Public Key Pinning (HPKP) ([\[RFC7469\]](#)) only applied the designed protections when dealing with a certificate issued by a pre-installed "system-level" root CA and were disabled when dealing with a certificate issued by a "locally installed root CA".

To test some tooling specifically, it may be necessary to install the root CA as a "system-level" root CA.

2.5. Certificate Chains

In most real-world examples, X.509 certificates are deployed with a chain of more than one X.509 certificate. In particular, there is typically a long-lived root CA that users' software knows about upon installation, and the end-entity certificate is issued by an intermediate CA, which is in turn issued by the root CA.

The example end-entity certificates in this document can be used either with a simple two-link certificate chain (they are directly certified by their corresponding root CA) or in a three-link chain.

For example, Alice's encryption certificate (`alice.encrypt.crt`; see [Section 4.3](#)) can be validated by a peer that directly trusts the example RSA CA's root cert (`ca.rsa.crt`; see [Section 3.1](#)):

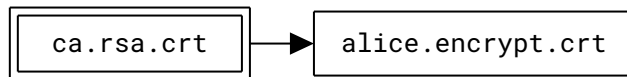


Figure 1: Validating Alice's encryption certificate directly when the issuing CA is a trust anchor

And it can also be validated by a peer that only directly trusts the example Ed25519 CA's root cert (`ca.25519.crt`; see [Section 6.1](#)) via an intermediate cross-signed CA cert (`ca.rsa.cross.crt`; see [Section 3.3](#)):

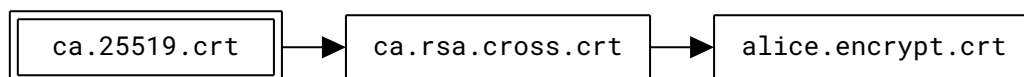


Figure 2: Validating Alice's cert from a different trust anchor via an intermediate cross-signed CA certificate

By omitting the cross-signed CA certs, it should be possible to test a "transvalid" certificate (an end-entity certificate that is supplied without its intermediate certificate) in some configurations.

2.6. Passwords

Each secret key presented in this document is represented as a PEM-encoded PKCS #8 ([\[RFC5958\]](#)) object in cleartext form (it has no password).

As such, the secret key objects are not suitable for verifying interoperable password protection schemes.

However, the PKCS #12 ([\[RFC7292\]](#)) objects do have simple textual passwords, because tooling for dealing with passwordless PKCS #12 objects is underdeveloped at the time of this document.

2.7. Secret Key Origins

The secret RSA keys in this document are all deterministically derived using provable prime generation as found in [\[FIPS186-4\]](#) based on known seeds derived via SHA-256 ([\[SHA\]](#)) from simple strings. The validation parameters for these derivations are stored in the objects themselves as specified in [\[RFC8479\]](#).

The secret Ed25519 and X25519 keys in this document are all derived by hashing a simple string. The seeds and their derivation are included in the document for informational purposes and to allow recreation of the objects from appropriate tooling.

All RSA seeds used are 224 bits long (the first 224 bits of the SHA-256 digest of the origin string) and are represented in hexadecimal.

3. Example RSA Certification Authority

The example RSA Certification Authority has the following information:

Name: Sample LAMPS RSA Certification Authority

3.1. RSA Certification Authority Root Certificate

This certificate is used to verify certificates issued by the example RSA Certification Authority.

```
-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgITCbn0xb/zdaeCQ1qp6yZUAGZUCDANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGx1IEExBTBVTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAqFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowVTENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlm
aWNhdGlvbiBBdXRob3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQc2GGPTEFVNdil0LsiQ79A0Mz2G+LRJlbX2vNo8STibAnyQ9VzFrGJHjUhrX/Omr
OP3rDCB2SYfBPVwd0CdC6z9qfJkcVxDc1hK+VS9vKncL0IPUYlkJwWuMpXa1IeIz
+zCuV+gjV83Uvn6wTn39MCmyu7nFPzihcu0nbMYOCdMmUbi1Dm8TX9P6itFR3hi
IHpSKMbkoXlM1837WafFx57kBIoIuNjKEyPIuK9wGUAeppc5QAHJg95PPEHNLmM
yhBzC1mgkyozRSeSrKxq9XeJKU94lWGaZ0zb4karCur/eiMoCk3YNV8L3styvcMG
1qUDCAaKx6FZEf7hE9RN6L3bAgMBAAgjqBAMA8GA1UdEwEB/wQFMAMBAf8wDgYD
VR0PAQH/BAQDAgEGMB0GA1UdDgQWBBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkq
hkiG9w0BAQ0FAA0CAQEACDxwLjGjzKadNMPcFlZInZC+Hl7RLrcBDR25jMCXg9yL
IwGVEcNp2fH4+YHTRTGLH81aPADMdUGHgpfcfQWjesavt/m00T0S0LjJ0RVm93fE
heSNUHUigVR9njTVw2EBz7e2p+v3t0sMnunvm6PIDgHxx0W6mjzMX7lG74bJfo+v
dx+jI/aXt+iih5pi7/2Yu9eTDVu+S52wsnF89BEJeV0r+EmGDxUv47D+5KuQpKM9
U/isXpwC6K/36T8Rhd0QXDq0Mt91TZ4dJTT0m3cmo80zzcxskMDStZH00zCBtBq
uIbwWw50a72o/Iwg9v+W0WksBCWEadf/uK+cRicxrQ==
-----END CERTIFICATE-----
```

3.2. RSA Certification Authority Secret Key

This secret key material is used by the example RSA Certification Authority to issue new certificates.

```

-----BEGIN PRIVATE KEY-----
MIIE+ wIBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQC2GGPTEFVNdi0L
siQ79A0Mz2G+LRJlBx2vNo8STibAnyQ9VzFrGJHjUhRX/OmrOP3rDCB2SYfBPVwd
0CdC6z9qfJKcVxDc1hK+VS9vKncL0IPUYlKJwWuMpXa1IeIz+zCuV+gjV83Uvn6w
Tn39MCmyu7nFPzihcu0nbMY0CdMmUbi1Dm8TX9P6itFR3hiIHpSKMbkoXLM1837
WaFfx57kBIoIuNjKEyPIuK9wGUAeppc5QAHJg95PPEHNNHlmMyhBzCImgkyozRSeS
rkxq9XeJKU94lWGaZ0zb4karCur/eiMoCk3YNV8L3styvcMG1qUDCAaKx6FZEf7h
E9RN6L3bAgMBAAECggEAE3tFhsm7DpgDlro+1Sk1kjbHssR4s0BHb4zrPp6c18P0
6T8gWuBcj1Dz0zykNTzaMaDxAia4vuxVJB1mberkNHZTFqyb8bx3ceSE0CT3aoyq
5fiFpR0L6Ba1vvgg8RTvNCAIApHNa4pVx0XD8Wq+h7m1UA0YGbie5U08/P2qWjc0z
+zcheyYXJS/iuu0t2/F0ihEWGcXBmoc8D++n7mKst2jkAHD4w1PN2MgVqnmagpBz
gobFNmCZyZpDS+PPTtQZ1XvdGF5Sodc+Fz+jpWun1kqxDHE4UIZzDA/HAAgORbm
aEZAvs0s9ZExeq0tqu2fPB7zF/1JKdRk4UJ0UxS00QKBgQDJwonP5Rwv00sYoCiw
zuFcYTmN/hI3R3viKuxr19CH6+mvuIU85ooIHF6TiouZwhk+6+Vx7rcXds554DT4
2RbVrX/5i/M0zx8c8IIwoZJIasLz+vx8F4n6hyhV65bXN7AIBojMh2dt8tP2MZ/R
VEfsk4mNm06yKuzyAfjJziCnQKBgQDnDH9UYUIPkq0PSvViKQFJFCB9BJPFhld2
pIgoziw/JZz3M3W3IWU0KKG7UxS0T3xmn3IX6xmWW4vX1/088yb0bZWYP0edb61GM
I9DoI5igndLgDwy0L2PFuZh5pqqc09DE+cpJW4nNoudqTNmCrjhmXNCGKgGjld8z
/OkSccvywwKBgDd0ReajRUziEjDxjF2UbzKx8lzJsX4KIs22GIHQSRCv1cy80Qa
5WN3ULNiyB350HCP69wDFMXym5rJoQjPvh6GIuhYKv4V8fffxkYv5kx5uWiXZVJ
7v2x+m8rMqlyv+pkyWLV8KKyTHmdiBzD+oTWx7r4ueLjtaxngzxn93pAoGBAKpR
rR9Pnr0KHubSE/drUNZFLvnZwPDv6l08T978t0NL372pUT9KjR8eN31DaMpoQ0pc
BqvpSoQjBLt1nDysV2krI0RwMIOzAwc0E9C8RMvJ6+RdU50Q1BSyjlGaKi5AAHk
PTk8cGYV01BCHG1X8p3XYfw0xQaHxtuVCV8eYgCvAoGBAIZeiVhc0YTJ0jUadz+0
vS0zA1arg5k2YPCPGf7z+ijM5rbMk7jrYixD6WMjT0kVLHDSVxMBpbA7GhL7TKy5
cepBH1PVwxEI18dqN+UoeJeBpnHo/cjJ0iCR9/aMJzI+qiUo30MDR+UH99NIddKN
i75GRVLAeW0Izgt09EMEId9joDswOQYKKwYBBAGSCBIIATERMckGCWCGSAFlAwQC
AgQcpcG3hHYU7WYaawUiNRQotLfwYzMotmTat1i6Q==
-----END PRIVATE KEY-----

```

This secret key was generated using provable prime generation found in [FIPS186-4] using the seed a5c1b7847614ed661a6b0522351428b4b7f09d8ccca2d99302dd62e9. This seed is the first 224 bits of the SHA-256 ([SHA]) digest of the string draft-lamps-sample-certs-keygen.ca.rsa.seed.

3.3. RSA Certification Authority Cross-Signed Certificate

If an email client only trusts the Ed25519 Certification Authority Root Certificate found in [Section 6.1](#), they can use this intermediate CA certificate to verify any end-entity certificate issued by the example RSA Certification Authority.


```
-----BEGIN CERTIFICATE-----
MIIC5zCCApmgAwIBAgITcTQnnf8DUsvAdvkX7mUemYos7DAFBgMrZXAwWTENMAsg
A1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTIwMTIxNTIx
MzU0NFoYDzIwNTIwOTI3MDY1NDE4WjBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTVBtIFJTQSBDZXJ0aWZpY2F0
aW9uIEF1dGhvcml0eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALYY
Y9MQVU12LQuyJDv0DQzPYb4tEmVtfa82jxJOJsCfJD1XMWsYkeNSFFf86as4/esM
IHZJh8E9XB3QJ0LrP2p8mRxXENZWEr5VL28qdwvQg9RiWQnBa4yldrUh6XP7MK5X
6CNXzdS+frB0ff0wKbKa7ucU/OKFy46dsxg4J0yZRuLU0bxNf0/qK0VHeGIgelIo
xuSheUzXzftZoV/HnuQEigi42MoTi8i4r3AZQB6mlzlAAcmD3k88Qc0eWYzKEHMK
WaCTKjNFJ5KuTGr1d4kpT3iVYZpnTNviRqsK6v96IygKTdg1Xwvey3K9wwwBWPQMI
BorHoVkr/uET1E3ovdsCAwEAAN8MHowDwYDVR0TAQH/BAUwAwEB/zAXBgNVHSAE
EDAOMAwwCGSAFlAwIBMAIwDgYDVDR0PAQH/BAQDAgEGMB0GA1UdDgQWBBSRMI58
BxcMp/EJKGU2GmccaHb0WTAfBgNVHSMEGDAWgBRropV9uhSb5C0E0Qek0YLkLmuM
tTAFBgMrZXADQQBnQ+0eFP/BBKz8bVELVEPw9WFXwIGnyH7rrmLQJSE5GJmm7cYX
FFJBGyc3NWzlxxyfJLsh0yYh04dxdM8R5hcD
-----END CERTIFICATE-----
```

4. Alice's Sample Certificates

Alice has the following information:

Name: Alice Lovelace

Email Address: `alice@smime.example`

4.1. Alice's Signature Verification End-Entity Certificate

This certificate is used for verification of signatures made by Alice.

```
-----BEGIN CERTIFICATE-----
MIIDzzCCAreAwIBAgITN0EFee11f0Kpolw69Phqzppp1zANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGx1IEExBTvBTIFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhvcm10eTAqFw0x0TE
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMA8GA1UEChMESUVURjERMA8G
A1UECXMITEFNUFMgV0cxZzAVBgNVBAMTDkFsaWNlIEExvdmVsYW51MIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/
pd0/KLpZbJ0Aer0sI7Aja07B1GuMUFJeSTu1amNfCwDcDkY63PQW1+DILs7GxVwX
urhYdZ1aV5hcUqVackPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TCN012DRVB
DpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJ0MayCQtwS1q7ktkNBR2w
ZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR+peC
rhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKk01zQ1Pq90njlsJL0wIDAQABo4Gv
MIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBawDjAMBgpghkgBZQMCATABMB4GA1Ud
EQQXMBWBE2FsaWNlQHNtaW11LmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQw
DgYDVR0PAQH/BAQDAgBAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAf
BgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOC
AQEAc4miNqf0qaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJ0d64roA
KHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27PmhK
E1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahixRn/C9cy31wbqN
sy9x0fjPQg6+DqatiQpMz9Eiae6aCHHBh0iPU7IPkazgPYgkLD59fk4PGHnYxs1F
hd06zZk9E8zwlc1ALgZa/iSbczsqckN3qGehD2s16jMhwFXLJtBiN+uCDgNG/D0
qyTbY4fgKieUHx/tHuzUszZxJg==
-----END CERTIFICATE-----
```

4.2. Alice's Signing Private Key Material

This private key material is used by Alice to create signatures.

```
-----BEGIN PRIVATE KEY-----
MIIE+gIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQC09InoWDgWpK2a
f0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHUa4xQU15J06VqY18LANw0
Rjrc9BaX4MguzsbFXBe6uFh1mVpXmFSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z
34rTiz4DxMI07XYNFUE0ls/gkUP2Gxzys02kaYWTut3SryCqeHEfbZFkB4urMk4
xrIJC3CzWruS2Q0FhbB1fkgKN5wXVgkWFfi0ucfCn+IQsaqpo1d3f9jSkbtAV5w3
vzfog8919MxKI9H614KuElnAtJ7BtZcs17dUy9u9C0gEykrIVokFQgqQ7XNDU+r3
SeOWwks7AgMBAAECggEAFKD2DG9A1u77q3u3p2WDH3zueTtiqgaT8u8X0+jh0I/+
HzoX9eo8DIJ/b/G3brwHyfh17JFvLH1zbgsn5bghJTz3r+JcZZ513srqMV8t8zjI
JEHOKC3szH8gYVVKwRigBAq0t1H9Ti8J2oKk2aymqBFr3ZXpBUCTWpEz2s3FMBUUI
qCEsAJqsEch+kt43X5kvAom7LC1DHiE6RKfhMEub/LGNHswY4dmzhaG6p95FJ1h
s8HoURI2ReVpsTadaKd3KoYNc1lcfmwdZs/hFs7xmmwXKMlonh1mzHqD1/BqeJ
Hc8MP4ueDdyVgIe/uVt1Q9NcRQbuokkDyDYMYV6hzQKBgQD75ahYFGZznRKtSE3
w/2rUqTYIWxx2PQz5G58PcsTzM89Hj4aZ0oLmudHbrTQHluRNcHoXEI62rs0cVPs
D7I1ZOLfs+SSTeNEXxD57mjyyufpV650cNc1mSJAmMX2jWQ8ndnOuWPcc5J6fNvT
au0a7ZB0aeKHnA8XXL3GYi1M9QKBgQC35xKi7f2JmGtsYY21tfRuDUm6EjhmW6b7
GWnI9IXF8TGj15s7oDEYvqSPTJdB6PAB/tZwdbj9mB4qj176x1kB/N7G097408UP
/PdHkU7duyf5nRq1mrI+yGFHVsgD313rc+akYdKcC207e6IRMST1ZFoznC6qNgpi
nNTuDz4ZbwKBgA5Dd9/dKKm77gvY690bjn6oBFuUs05VaaaSlcsFOL2VZMLCNqQJ
+NLFZ7k8xJJQVcEIOT2uE7X/csBKdoUUCnL5nnsqVZQPQwI5G937KQgugy1MZLte
WmFX1X/w5qzKXtWr3ox9JPFzveSfs1bqZBi1QQmfp0skhBo/jyNvpYUNAOGAMNkw
GhcdQW87GY7QFXQ/ePw0mV49lgrCT/BwKPDk1815ZgvfL/ddEzWQgH/XraoyHT2T
uEuM18+QM73hfLt26RBCHGXK1CUMMZL+fAQc7sjH1YX1kleFASg4rrpcrKqoR+KB
YSiayNhAK4yrf+WN66C8VPknbA7us0L1TEbA0AECgYEAtwRiiQwk3BlqENFypyc8
0Q1pxp3U7ciHi8mni0kNcTqe57Y/2o8nY9ISnt1GffMs79YQfRXTRdEm2St6oChI
9Cv5j74LHZXkgEVFf02Nq/uwSzTZkePk+HoPJo4WtAdokZgRAyyHl0gEae8Rl89e
yBX7dutONALjRZFTrg18Cueg0zA5BgorBgEEAZIIEggBMSswKQYJYIZIAWUDBAIC
BBySyJ1DMNPY4x1P3pudD+bp/BQhQd1lpF5bQ28F
-----END PRIVATE KEY-----
```

This secret key was generated using provable prime generation found in [FIPS186-4] using the seed 92c89d4330d3d8e31d4fde9b9d0fe6e9fc142141dd65a45e5b436f05. This seed is the first 224 bits of the SHA-256 ([SHA]) digest of the string draft-lamps-sample-certs-keygen.alice.sign.seed.

4.3. Alice's Encryption End-Entity Certificate

This certificate is used to encrypt messages to Alice.

```
-----BEGIN CERTIFICATE-----
MIIDzzCCAreAwIBAgITDy0lvrE5l0rOQlSHoe49NAaKtDANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGx1IEExBTvBTIFJTQSDZXXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAqFw0x0TE
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxZzAVBgNVBAMTDkFsaWNlIEExvdmVsYWNlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmPUp+ovBouOP6AFQJ+RwpwODxxzY60n1
lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8g0UH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+
hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV
8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShp1cI3lcvvBZMswt41
/0HJvmswqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWf
NEbkN6hQury/zxnlsukgn+fHbqvDhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4Gv
MIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBawDjAMBgpghkgBZQMCATABMB4GA1Ud
EQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQw
DgYDVR0PAAQH/BAQDAgUGMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAf
BgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOC
AQEAgU14oJyxMpwWpAyl0vK6NEbM1lgD5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LD
sfx7fSIus8gWVY3WqMeu0A7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzT
jqB8+dz2AwYeMx0DWq9opwtA/1T0kRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps
98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpfb8PPwDR6chMZeegSQA
W++OIKqHrg/WEh4yiuPfqaVx2hZkPpivNJYdTPUXTS07K459CyqbqG+sN0o2kc1
nTXl85RHNRVKQK+L0YWY1Q+hWA==
-----END CERTIFICATE-----
```

4.4. Alice's Decryption Private Key Material

This private key material is used by Alice to decrypt messages.

```

-----BEGIN PRIVATE KEY-----
MIIE+gIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQCalsn6i8Gi44/o
AVAn5GnCK4PHHNjrSfWUnnelN41KImVaTC3D9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnV
z5q7M8onZm7mZjqQeb6FUH4i2Gmt4jse2Dqs165ernT905NLFf1HUjURca3ynqEB
BV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZuTtMc1zy++MxQ1qdn9WZLh0A0peNZ
KGmVwjeVy+8FkyzC3jX/Qcm+ZLCqLlqhBwDhdZ5qDTII2PVX1X3K7/cONxhvBbaU
l/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGewy6SCf58duq/A0EksCAW1b+MD8QH9Y
j7CFSmq1AgMBAAECggEADgxowEDDRE5yEZ+s7TMw+WH2o+3X00rryqnsLb0yv34I
wAAUWK7qZyjd9rSD0AtB0gFhQNXyHwZ1T+0iHs1CIIfqJMZ8wy1iFHBCIphoMSWs5
/D+idXrUef5Y23rC1BxXH0g1UnSGXnpUH4ehV6p1lvZMh40JKEoMC4cpyd1SzXrw
+VGCc1+pXv/tTW3Rb2qoW09JoWY+Epcssrw5N80FIF0Dh4QfblN6pVTt28aQ4pf/
1KhLoapjFzXSYp/jrcNjYJ9qRdSAbZsK0J2yZ0yqjLHDCDipFty+W0pkUZcJhsgu
Cg1Stt7tKgSvAV/nEjN8e/vA91/AACKBCNcLzEoLgQKBgQC4eTM6BDCz1usXJBK4
SRC/WwUthJZzf0k2Gmwr0DCTRYhWQSDjBfiQNboazH0bVPz45qP10f0t2iPEHeX+
VWAXTNrN69M91EzxygA3s761AejBR3FbLWkzLYqPB3oZwSIE7CrWHTXJipFWZv+X
FG1R418fnRCUMJ4j85qem5iyqQKBgQDWhQMJu7FC02fr83qsIdLwqhiDtTpwUN3j
qfp7JoEZ0xbm3TgM1xPAkrQTUgfr2ZhxGtUwsuKHyifxQEycrTkB0g0ggqAfG0fnv
ybyXK6/guctHJQiy641L39kPuvQkKB+Y060B/oF6zbyFvqanoKXjpsp0bn3i3yBU
X5/E0u/LLQKBgQCUVvHwWAgSg+pgBx9jG0nPK4h0CkznRJ7qyuo37Tv+E3171Ff
vYFv1YSd4CJmmiUcKZTvk3FkL7HrFo/HwSeQFQE7aDkn8jX9bPPFv8K+UoNgkGp
LA8YVfRDQSPyadfNVYvsuXhzJLZSYGjPOGHgI5JufYLDZ4UDK/T97ekQYQKBgDDM
ORCxxvXTyGiW2USVU3EkaqFDtnMmH27G6LNxuudc/dco2cFWbZ0bbGFN8yYiBCwJ1
fDGdV7wb5FIgypqtn4lpvjHUHA6hX90gShT3TTTsZ0SjJJGgZEeV/2qyq+ZdF/
Ya+ecV26BzR1Vfuzs4jBnCuS4DaHgxcuWW2N6pZRAoGAWTovk3xdTE0TZvDerxUY
18hX+vWJGy7uZjegi4cFecSk0R4iekVxrEvEGhpNdEB2GqdLgp6Q6GPdalCG2wc4
7pojP/0inc4RtRRf3nZHaTy00bnSe/0y+t00UbKRMtXhnViVhCc0t6BUcsHupbu2
Adub72KLk+gvASDduuatGjqq0zA5BgorBgEEAZIIEggBMSswKQYJYIZIAWUDBAIC
BBwc90hJ90RfRmxCciUfX5a3f6Bpiz6Ys/Hugge/
-----END PRIVATE KEY-----

```

This secret key was generated using provable prime generation found in [FIPS186-4] using the seed 1cf74849f7445f466c4272251f5f96b77fa0698b3e98b3f1ee8207bf. This seed is the first 224 bits of the SHA-256 ([SHA]) digest of the string draft-lamps-sample-certs-keygen.alice.encrypt.seed.

4.5. PKCS #12 Object for Alice

This PKCS #12 ([RFC7292]) object contains the same information as presented in Sections 3.3, 4.1, 4.2, 4.3, and 4.4.

It is locked with the simple five-letter password `alice`.

```

-----BEGIN PKCS12-----
MIIX+AIbAzCCF8AGCSqGSib3DQEHAAcCF7EEghetMIIXqTCCBI8GCSqGSib3DQEH
BqCCBIAwggR8AgEAMIIEdQYJKoZIhvcNAQcBMBwGCiqGSib3DQEMAQMwDgQIWWKs
PyUaB9YCAhTCgIIESCsrTOUTY394FyrjkeCBSV1dw7I3o9oZN7N6Ux2KyIamsWiJ
77t7RL1/VSxSBLjVV8Sn5+/o3mFjr5NkyQbWuky33ySVy3HZUdZc2RTooyFEdRi8
x82dzEaVmab7pW4zpoG/IVR60TizcWJ0ooGoE00Rim6y2G+iRZ3ePBUq0+8eSNYW
+jIWov9abdFqj9j1bQKj/Hrdje2TCd16a9sS1TFYvIxBWUdPLZDwvCQqwiCWmXeI
6T9EpZldksDjr5N+zFhSLoRwABGRU8jXSU9AEsem9DFxoqZq8VsQcegQFY6aJcZO
Xe17IECIAgK8nZlKCTzyNVALxeFw0ijWnW41tDaqcC6GepmuINiqqdD94YA0HxR1
11KU4mLknSJ36W4T7vaI4fp98sK0nGpaDzQheu6BbQ+dVd44q52MDwvqvD0Y7UjF
IVEP3V9Ebf641CR0mIcVCUynxb3aaKjhgBKTGbYsKtPue974rDPIArMs2Heo8y3

```

cq+f7Jce0IVCglRatN6rSyJBF8JlBQW5pZGco8AwTM1pK3RrdIDziheA8DIBB+KT
4JZB06UprlcZ5wBY6ncXWa5E4feb57Cd3bB+zJuubBX9f4yG/J0cSF59w92c/6Qb
i4EFk6tAiz19PxuLLwjco71e69Jiav19Ph/WJpf/XCEurw7K+VAeZALFW41G/D30
WIBRC2shisHB3j8+3fNPcvi4Fy3EkZNW4lrZFAjbBtloCkx5rcfRS7vxucAvC5X9
4bm0xEcdOysnuplH77u+CWWxjCk414S1KZTUbwcl1a0B6yRDvojUMZkDzMqsxyYjn
JG5QhMFQrTyALwCgJsP/rAf5xPhG2p+9Qul0yiBIIZwvKNKRQKL+YLcvYvTh1bhj
rUflYzzvvixCY9LcX2GBop9yBFJzIcmKfL0MGua6WIkWX2BIjhGTtu6VThmRHuf
OsqNg/ZrNCTYa7e1D6gwp5uFRecSZdAsf+0XTe6M7e/vaN4Go4A3H8+d53SYQP6n
pTt/a0DTHzY77aNMh+mkzIHC1W3zUdLS48tUyJMiAN3Tt+RfhHZfgloJ7IdcYdM2
01I+UD/5L9ghxN8dh13Fi3rDyn6Y5xB1xFuZ0mLjoEI+3Pr1+B9KgF+o/hxFttfx
1uP1XcHt0a4gBr6g7fwGNssfw5S6g6hS9UDTAY0pvLaatil2T2meYZzizj19ssv36
kr1VarV9xcQCby05ucD+buymFXPn/rhVdxhgIydmv0tdzDozy0WFDTVgJUBNeRnC
eMVD6A1WdW0lMbQcILJS0aY2FWm8Kju62XZA8YIRowLlysuq3zIqDmzmJFKwua
mRMZmUVhophMEN86rwob3Z87gNbYY1U/dXi+s6VybX/kiwDXjfyhWBnhn1gkhgiv
o0hGtt+yAlcVuhQLEloQeQN04C5QTU0d1W0j489Ft6wpvm0tqc16NpnRYUhbCoF
XhFr4wsWggR3BgkqhkiG9w0BBwagggRoMIEZAIADCCBF0GCSqGSib3DQEHATAc
BgoqhkiG9w0BDAEDMA4ECPoEFEHQGB9dAgIU5oCCBDA0rGHYN47xkt1J1VvWQZN
BYIMFzLn6p2/zKotGf7EMdgSdwlxkhKTWxunfoP/gfRD6boXTAA7ukJDsHXZrfXF
KjI4HI2oa/NihwqctphcLonBJXcofuHv+loP9MPLtwu3Mo1wsWTiHpf5XmxMoZQw
fbrp2ohLugJ01ZRB9rFAUpaAhtFg91pL0tXEpz7GULEyOnYh9R8iu9bSel8bp14S
+AoxzXD4gYiEU6Yi0/47aRstd3H4u3ERDnUKSoqVsts1RSKnK/WrGYUwoy7kNDwy
DBitfosMY0rpWE5rXTBwJkBodc13LBpDbNzdbzZw+e+yObJ9zfRlMpl0xVfoiji
q9UbRdgN2yo0RKwF6c63V2RdF5tjQHnNIM3K3tC9zEis11jgn9LeOLB9Cd1qyE4P
WfmHN0gWqDF1eX96TmUipmYM63H6jcbnSc6p7eIZtCrqGjhsTqFwcMg04WaXWeHD
ffLXSZdzIUB+zfc8tftUUEOUX3tX411oU7K8uAuQTSK/AXwUj+MbQVhlz8te4FVr
w4ulZ184IYqhD3VdIOxXiZkfSKChRz8/7QacrXFvFKkrxS2iHMoxhoJ7WETNtI
slW5R5runj61r50VT4HCFNFQfGBBtV9AdP7yka9aQDWxPCoXFgeb1Q01F/BigzW
02JP5Lcrw7ia0y88QbTzWhi57d4he50Ip0wHUiGPh7s792m1ltvuSpRKJk0XWv6h
qAj5AsBB8JNvgXP71Ytx2vMdw6gqzCqCAsJ4UHqG0CxmIODLUP+FHAY1CPNSjbR
pHrTi1UFi/+9hYneQci++qPvkCqMuGHVxamd40LanGJN1Nx1DyMeduapX5rXuPn
g66LPeY9GQuE3SBNC2dmju0y7d8fWEXEzqhqltPfsuwVzdnWb1uAcjRfQPN0+uWe4
zihYisXK3lqA557dRqdSv+6GL6/OZQOCtaYMyZiWD9jS2gU6T3q2j8uk1LncL9n8
aSpQ5xWspBXpzXo39fG6CMeqzZ1FCqrVqWYhdXbtxN90x/pimmW0lcqAxv+xythW
BMx+il1JEdbcj015wjmsCWNPW1M4AVSholpZhs9Mq6rvGbx1HJgjD0DpSLCE0xh
/GNoXoOX3LrxfCIDEhT8LyZ2NE59yh3t6pm88soFzaAghdjb1Fkc79nBbc14NLKg
SmL/7GktkxEzn0iSYfnfJ905kjZC08d8RnoGfrDDUWD2ZiHbbx0Cq4E3E0Zt13aH
JOXRBOZLC9L2JNeSniBZZGykh+Pi4TsIzXL2UPQ+dy4DDaEf8yamyY04dlHfSnhD
qr94Y9E30/rpF0yUb2gCehEgT9nppVuMeridsCkHqemmgVr/52Xv/XK9dx4+YBjL
4/3Id0/yVJURqDIHH8o4ogF4rf1kz0a1rZ9nJFugP0UM8oNysal9yr7/Dli1juV0
MIIDZWYJKoZIhvcNAQcGoIIDWDCCA1QCAQAwwggnNBgkqhkiG9w0BBwEwHAYKKoZI
hvcNAQwBAzA0BAidIqBxZFwvagICFCKAggMgTzrUv4/12Jqnv3AL+P6990uX1ybZ
NcTwC+hMRV0Ho0FuAAYbzdSRBAaZch1+8GheU8yz7IYWmLn1PNHx1Z8inIYfmTfk
Pa34Rk8s/RxJIe8LMYL1qjk/FMq/Fpgc0S65S6bXvJ69Hb8gtAoGW8P1b0dd9bvG
NbAk00h5r+IWiH4U8zGpcqWDRGieGICsY00Hvx4KKMV6FIjFVCTZevORVoyzmSX
ZZGxqrbjw4CZqQ0WRHPI3aEt5xVX3BiHRgi4Eiyia6yU10V0ZTGBKQWueKm0A5Gw
SX3mH/kLiya3gwwGvdq1ncXcl7V1STN1HFyp4ebGKg4CsZ6NkWjocwq2PwM/TqoZ
5i02tqvOer8lX7LrSegxGH81Kw3nMV4dH5txoVt9hddZCKKGcJ5Z8F1zxFP4BFuF
7hOmRpUPdxiahJ/GkXDVIaw6BJKd4Q9e6sjJYxTeq4u0P6V4PMuDU7F98X/d9sEx
2X3b1cJxuA7xtOnKAPsWEyWBg98B+CKG6Kw05s8T1ZVmlk15FCUjvFoKCiWIKF4N
vGLiW0IP/jJ9N6Gqp4gNbm51zNFGZ7gZAtvsBSGQS0UPgfZcx2mRxpBmcX8tm5YJ
hmY9EDK13umUUGKrP0rG8c7/MVAQegSKqQuXSfMK6KknXGe7jwjs7xaQaRm9fFHS
0KbGU3MsLxRGjW/jzjUNAEDiSYPCVo8E/kd8LETvjAowF772y9o0X1ZzcP7HWcl
oYc0/WSSh4e+FAbgqLo/8KIkgZJ23BAcdx8XAtxzUZhRdHaItnwaJsFTr4TCwq8C
XxJG5u44/z6imqQrV0aXQfvk6sSNGdG62TkacYg2K63D9hcg+TbZPPVSStWXyj8S
N84anzT0xb1yx6aw6IL+uBLC4jISgNFijaF5pwjLSbgTs5Z7skZdCam80xYmdJVO
ES/uqFCQFUSamXXNbotviQk8jWuJFz+BXzPYJN3t+3mp6SmgTZ2zP8FUQEE4GbSH
DqYV621DcWro/mao8xzX/mvkKm4ddGBldiushZaL4gdo2A1qThSMnMBsciC+jEj
DqOr70XhHccTDW8wggWUBgkqhkiG9w0BBwGgggWFBIIFgTCCBX0wggV5Bgsqhkig

9w0BDAoBAqCCBSYwggUiMBwGciqGSiB3DQEMAQMwDgQIehcRLmVUApmCAhQ0BIIF
AHb5dXZKzCeRUo2ZSj0oyuFS3zQ5HhKyfapsyCqbYCKv/lSzNYWvuda7xfu+u0M7
/wCB9sWdz0MTpaBMHWx9hvibZiY650m+ry4tTuKkQ0Jl370snjB0dSNTKszsI3fa
PUjslxqIH3aC1shD70qhIRGZzRjK44PJyWv626oQrgVtTYR9NYTdee+SbBZbkEt/
EpWipwftWXGR6tSYJQn99e09Vih8HyQvwIpidUh3pCF0low4VZYAqIWOHcw9TAjB
XNv+qfdH7fiX9wM5/GvnQReIsqjXCUoc6pSQIAqD/f+I/d1F2ZmqM7KwX0LGRER9
OWZGyF734pN9GLbNetWm6rKxmLSI/5m6+2Jxxfann16P+vBSEgWJ/I8GnJAdzIbB
Tyfjog4Gi2+lmrPzK7+C79ntM9nfsr4xVzy/BknwZiAJksd4VvOGkS9nfm6shtBJ
B9uR+GJfthtsvIVUHN0kz2r/lVzMSRbOg9yR53hv1H/nXCmUjWz/BvobmoaVBcCm
mOnnYZTHMNarIVYdLQFif5ZLH7WV/XVEVioRntNRiKsK96VAHm5XboWQGCqL0heh
IX3Nily1genGm1aFlSQNMvLDko1ILDtKrINvPmjG/WFoLntpJFPtYZsooT1jjXLw
3VTSodtgKQNdPYOEidSJqwIS87fzrCB2Wmwys0iGfdsuNhSaqNqa0dM06FiW2fku
x7H+w7SX1/n9YeZUNL0cewLcC7E8IA1IarjglZE1L6Yb2ldXxV9q3PP0wKuGnah0
TKnD6mLn5BIGOGTzF1VspXRrJhFrcLe+xsJR1r6niI3bcMWXy7gbm1X/CRE902I
ynxE1oDR+xZ6rjPwDJP7kVf4GvA8trCGrot4pbJbmwlBeMIylScdQoHEnyqren0n
RMmXZakZl3njtq7Wk78qoJq0a6Vh/sde0KcOPFkyTZdMB1Tztm0K2VJU3jUVzP1M
0WY2fyGDoA89ol+/MinsgiaEghGybXBYip0ex+p7j1GIRN/CKmpWsqjZnB78kyXm
Z6AE1vC6neD/7zANInDkzXiun6ic72LoBX3JGiCSuM6hIPJ0AcDwlzTDu0H2rCQN
w+tivJ2v4KbgeKoc6beQb5fZHs7VSWHikIcpwqB5ngwt34wHgFG0nTS4LZmvzSJ7
FMRVGmsDYkDTPzZgN0axiUBQMcEvxNIE3nAmA+dvB7w6XRQVSUsL+vBFhHiWGZ7h
k5sCeHElewXK0SyJADgfflYq3EfEgZ13h4wtoSfbBVtzbbyg2LNegUCLfIJkC7fm
T7X7JSxbjOgndMHEeMdVb+NFxbgsXYrYD8rC2A8l5cQzZrsxb1bvgybEJz+NU/52
UgGrPmdjJKuGBK/V2zor6qPvKyId1Gb4QQuIoyClwhZ+qk9nE4Eft84y7ISgMywH
+lw87HrSHKfpqzQhCxlrLu53IYK/4PhE7BYC9Q4tvIsZXSGZ+nju4tyzERSlaNe5
njUeIENr4B/+kXULwVDcvMFHqUFJmKFai8FUGa7gyipZ+654clGgJjnNB01va8Jc
dtdPRRW4gwdRvN8u8J78KBzt6ChkrpKRV8VeWKBk9lhCt0ZNPJnNqhDrkfzHBqP0
Uo133I7P7C+h9sNDI153W6IOIodyQE0Av1WxHo4y/1d1VeGDaB7hOSDq9ZMpm9n1
En7F6/1/s4IUZHja/qRrK9hD4M0Xq0LhFXuUzuipo490MUawGQYJKoZIhvcNAQkU
MQweCgBhAGwAAQBjAGUwIwYJKoZIhvcNAQkVMRYEFKJtQdVEPIApFXwBI/Dnjq/N
83cPMIIFlAYJKoZIhvcNAQcBoIIFhQSCBYEwggV9MIIFeQYLKoZIhvcNAQwKAQKq
ggUmMIIFiJAcBgoqhkiG9w0BDAEDMA4ECKq4DtyiaY0yAgIUUpQSCBQAKQtKPOS4s
LE60s7nP4RaJWBuyXl27V/o6TusBRBgQoPzP+aC+099wgisEKedyB47bAzc04sba
4q8UKERAsYHcEhdD2hGRCL7ou9jTtrr4RgZpa5V9CJcB00t4bqy2lUef0pm6no+R
X840uyM4q5Q+cfH1rTQ1a/a+gLglbptoEkH/4dfR3ELYiXcM5UrBYTJOHcyME8c+
TXbpf7kip1Tt1sr1ZyU5zrWcxngrBxwFA+085W/uVR3QZSW+EGx/VCYwGruZlNyt
BvBYjsYsnC+yKYxbqL81DgOePy+eh6VX64SwBLXcWcY+NK2EZrhzrUFjl+PXFKY3
IVVPJhTE9o7gJA0hzvAan0luWXozD3/WPQaXhyIJDwM2MjznjL2MBydpy9K8Cio7
XaV6PX8DszIZkfI4DAz5f7G7WbwUq3IjPPPWiUv+JsR+dnqzWDJ22SXc+AdQP2sK
qMvP8gOpH0sVlXXE76c5rUcZCZD+gGv1av07YttWqbDqLj6oQEIJ8LX0Qvwd0YEh
etE0bJ5uv2njhQDhLkH/JIbmFSgJZeM8dtKHb8f5wZc2B+nXGB+TFboGzSuP7gaW
u1vKsJNqT/J/FYEeqamI2F+td7z1sGfbr9cKAcXeb2uPVbCJ1a50gRlZ9qVm5Hb
5f53X7aoQQp3F3LDGQMj+GFQ/oXXwabqn4TvN09KDhxpGcMMU9RnugUfNU9GBec0
vfrzmVKZdmJ36H0mMnLvgRakRhCV3kGABXY83hwUv17E1qASLKcAWIachkCCGpBG
yGtP2IOZTn7PsLJR1BzKnePa7MgFcgOCToIpdQnCTtAsalmbm1s480LN3GB5ojeG
bQvNf9TAviA0tg5VuT4/048V6uYSJsIZsawm3tGA/LjxyfV1aLddQT5Zf5ZX9BX+
K/PB4oYAFxtUpMK/aL5G1MvppUJ9CjqAtnoKE+EkDQmyZ1VoD09ih44zuRx6XV4A
EYafNB8ygjRHGsvPW0/M0Es0w16wzJHTuf/15fD/nH7Xh5MzhCF0CtvLn8v+S1Po
i2/4006pS2byjUFRbeCpzEPxrdv90LCb9ALdy0yG9u41W3yInKNFnaWBulf0PFCe
ZT92M1BgwJA8ZcydtiunRNAH5iWLSPlOUp0D1v6En+rat+PoyRXIy2fLHBL25aw
LhABoZPgRsCiLSiNiohfnygksrQKeRg0laBMT92J8r1E4sUKirQlc0diWBE6vmBS
XzyN/twvfgPNIXgr0rw6c7Vhhs+hNTrsttg/xcfvJ/bftDbKm+RZL+yQo0kkAf9R
5tizzyMdBlaMrpfrBxvNtMiykbZ88SYoA70Trwab2aHqluVhs80jXGBE0qmSudcS
dV1EhBpo9HBsDZZi0IwOp5/B9fCHdnThCTiUm80eQ6mX2/DB9L1Nh7gH0yLL3azT
m12D0ZpZNaXyxLzdiRiAdwpWZmmeg00G70yi0D5eIxb6cbnbuU6Ygdp+pFFVYHfA
vc5Czpne20PhXX2k00kbwawr9AfrFjIaEmBFx5GBGr/lSiUQSkbUC/s209Yga0g
WTYt3KXPzrThJJGZnnXZRTGfIi6vp8RsnPX35+Dxe/Lp3gXDdIJeWG6XVA8t3fsp
coTqPkm/XGNMM0Z81KX/ReVdP+dC93sov2DuDZbYGPmHlD47b00iA68GD64DEuNt
Q8MhWk8VRR1FqcuwB0T0bc+SIKEINKvYmDFAMBkGCSqGSiB3DQEFDEMhgoAYQBs

```
AGkAYwB1MCMGCSqGSIB3DQEJFTEWBBS79syyLR0GEhyXrilqkBDTIGZmczAvMB8w
BwYFKw4DAh0EF0/nnMx9hi1oZ0S+JkJAu+H3/jPzBAj10QCGvaJQwQICKAA=
-----END PKCS12-----
```

5. Bob's Sample

Bob has the following information:

Name: Bob Babbage

Email Address: bob@smime.example

5.1. Bob's Signature Verification End-Entity Certificate

This certificate is used for verification of signatures made by Bob.

```
-----BEGIN CERTIFICATE-----
MIIDYjCCArKgAwIBAgITaQ0kD33fBy/kGaVsmPv8LghbwzANBgkqhkiG9w0BAQ0F
ADBVMMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGx1IEExBTBVTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowODENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFUMgV0cxFDASBgNVBAMTC0JvYiBCYWJiYWdlMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnAF0glRof9NjBKke6g+7RLrOgRfwQjch+2z
m0Af67FJRNRewTu0utlWamUA3p9+wb7XqizVH0QhVesjwgp8PJpo8Adm8ar84d2t
tey10VdxaCJuNe7SjJfwrShB6NvAm7S8CDG3+EapK09fzn2pWwaREQ6twWtHi1QT
51PduRtiQ1oqsuJk8LBDgUMZlKUsaXfF8GKzJlGuaLR15/3Kfr9+b6VkdDuxTZYL
Zxt6+a3/QkaC3I9m2yGPubtHFJB5P5+s8boR0SKm10B1gsLow8eF9S70tcGGeooZ
JiJUQCR14NaU5bIyfkEZV2YStXwdztoEJJ2fRURIK+8Ynw1B3QIDAQABo4GtMIGq
MAwGA1UdEwEB/wQCMAAwFwYDVR0gBBBwDjAMBgpghkgBZQMCATABMBwGA1UdEQQV
MBOBEWJvYkZzbWltZS5leGFtcGx1MBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1Ud
DwEB/wQEAwIGwDAdBgNVHQ4EFgQUF8WEe9Cn73aQ0Lizbwi8krWeK5QwHwYDVR0j
BBgwFoAUKTC0fAcXDKfxCSHlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAG7e
QY6Px7WZC5vCbF5hj0itxoz3oyM+LRcSTGWOYXdmLwsNUzy31pE3dtADvevRtsP8
uN7xyfK6XZBzhShA/BtkkqYGiFvXDplu0xWmqC0WPmc1PNK2mHil+pGMfvnUwnxd
6gKched5p+bUhDyIH2fy9hGye0Us8nvi+7/HwBipN+nA/PfsPn+aU4l1K6qDoG/i
kwyuiWcFFlc5yE5rkAe2J0/a4+HtzNmTK4jB/4GbyI6xlUzP1EqKE+Es10Xut/y
UWL5nKKaqpRRd07Pq371MpFQs2+zXt4fGheKzZU3XXrIPcAPyJjWiyU1DzpqgSJM
OIp/HtXdFscHb9+Qic8=
-----END CERTIFICATE-----
```

5.2. Bob's Signing Private Key Material

This private key material is used by Bob to create signatures.


```
-----BEGIN PRIVATE KEY-----
MIIE+wIBADANBgkqhkiG9w0BAQEFAASCBAKggwggSkAgEAAoIBAQMCAAXSCVGH/02M
EqR7qD7tEus6BF/BCNwf7b0bQB/rsU1E2sTB04662VZqZQDen37BvteqLNUc5CFV
6yPCCnw8mmjwB2bxqvzh3a217LU5V3FoIm417tImN+vBKEHo28CbtLwIMbf4RqmQ
71/Ofa1bBpERDq3Ba0eLVBPNu925G2JDWiQy4mTwsE0BQxmUpSxpd8XwYrMmUa5o
tGXn/cp+v35vpWQIO7FNlgtG3r5rf9CRoLcj2bbKA+5u0cUkHk/n6zxuhE5IqbU
4HWCWujDx4X1Ls61wYZ6ihkmILRAJHXg1pTlsjJ8oR1XZhK1fB302gQknZ9FREgr
7xifCUHdAgMBAAECggEABcQg1fTtieZ+O/aNdU149NK0qx97GLTBjIguQEDDBVFK
2lu4PhBg9AdgAUqLH1PE+eq65JaGZwvFH8X1Ms2AKiRzYsPOQIoJ4n1hc69uiEN9
Ykcv4QH0vvqtCtWYjJyb5By9WPeLH6QynJ6F1BoSqxhURSwYyftUwqt10HEhsUuH
d3N5BmbFiRBNj4aIA9zz+i5xL0m33kMKai/Aj3sI0AJsZ5ZVAhYbC8sCt1Xevb6
i41p9S6GSwGC19by+1y9WC1QGtb5GDotvChMvmZS/03NeDc6xC/LZoQcHNvgiZd7
f1g6iEkJlCYK+D7xsd7Y630w75Haj0vnlhiJ0bSA+wKBgQDxv8jp2D6IVRGgYfaC
nUU3Mg70wagX1fGPH09Sk6e9c8CgORh2uwWjpTawu88xBGFyZ+XnWqr7GCNs1tas
3m94ri4A4R94+5uL8+o0LC26gMDfzATd1Q3k/h919YLk89tonQEUBCFZJdphThEb
vg2W+nNsEVcQGuClzhX0AyGMswKBgQD0BYk3sdGQbBA/hYD1EYsZfYebUiYv21Tt
VGRgTohKfclRAW0tGP9YRbKyEVkBLhjgkXzS9xGqKywP71z9Iny+zDGbzk8ElB/g
lS7FGGX50TG0ISfaFWTYdxt4mN9pduZE2b1T/26uyU8DXCEBhF/OqhwQjJqKTYTT
Rl3Ara5fLwKBgQDQyVtjIyD2q8naY2D8c4mo3vHtzyc21tQzcUD8Z4vSYps1hbos
KN/48qJmRv3tjqP+o+SXasYKsFE/4pIroLxTVNNkbQm6ektfttwp01yPG8340wLk
97HVW0ig/tX6m0Wg1yBsm+q9TKTrrm1pRGlmE6BQgSYy4r504u3VlnYwKBgQC1
B4FvWyDhTVQHwaAfHUg3av/k+T++KSg6gVKJF1Nw1x8ZW5kvnBJC3pAlgTnyZFyK
s5n5iwI1VZEtdbKTt1kqKCp8tqAV9p9AYWQKrgzxUJs0uUWcZc+X3aWEf87IIPNE
iQKfXiZaquZ23T2tKvsoZz8nqg9x7U8hG3uYLV26HQBgc0J/C21yW25NwZ5FUdh
PsQmVH7+YydJaLzHS/c7PrOgQFRMdejvAku/eYJbKbUv7qsJFIG4i/IG0CfVmu/B
ax5fbfYZtoB/0zxWaLkIESTVWaKrSKRdTrNzTA0reeJKsY4RNp6rvmpgojbmIGA1
Tg8Mup0xQ8F4d28rtUeynHxzoDswOQYKKwYBBAGSCBIIATERmCkGCWCGSAFlAwQC
AgQc9K+qy7VHPzY0Bqwy4AGI/kFzrhXJm88E0ouPbg==
-----END PRIVATE KEY-----
```

This secret key was generated using provable prime generation found in [FIPS186-4] using the seed f4afaacbb5473f360e06ac32e00188fe4173ae15c99bcf043a8b8f6e. This seed is the first 224 bits of the SHA-256 ([SHA]) digest of the string draft-lamps-sample-certs-keygen.bob.sign.seed.

5.3. Bob's Encryption End-Entity Certificate

This certificate is used to encrypt messages to Bob.

```
-----BEGIN CERTIFICATE-----
MIIDyjCCArKgAwIBAgITMHxHQA+GJjocYtLrgy+WwNeG1DANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGx1IEExBTBVTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAqFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowODENMA5GA1UEChMESUVURjERMA8G
A1UECzMITEFNUFmGv0cxFDASBgNVBAMTC0JvYiBCYWJiYWdlMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAgHAlBNMiBIk8iJqWHk/yDoFWwj8P9Z1uYdq
1aqIuofvjoAyjdA8TbsBRGdmvaIOSQOepsNjW1ko71E8H1Ds9JHn1E+tzH3mKfn+
G2erY+a1kMJTXPvMAUdCA8+e10J7k91gYXDpzIWrP3Kc0xTlsJ8tGJ6mhydJX3wP
0/HuyHpfKQqfDusPH8S5yidPciWuB7Wj0X4xY1pUAz2rSSAlnGvhEzKFbW43BPjY
XPUnRWMtXFya1dj6Eb9M/klbhdZheDLLsJLUSXYU70r9VXGM/qcjd/NhWYphCeB
cqsWam5mXLYdm0mFmqoecF62mUE0DiNdhwKTtnefd0c1l+D3FQIDAQABo4GtMIGq
MAwGA1UdEwEB/wQCMAAFwYDVR0gBBawDjAMBgpghkgBZQMCATABMBwGA1UdEQQV
MBOBEWJvYkZzbWltZS5leGFtcGx1MBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1Ud
DwEB/wQEAwIFIDAdBgNVHQ4EFgQUSrOsMVMCSZxN42554CVh1T6IYiUwHwYDVR0j
BBgwFoAUKTCOfAcXDKfxCSHlnhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAC2c
Y8FgaxgB+Dx9gAFj35ae1vgzYiWI3Ax3FSxogo/GzpK//LB4215oeBuKXbm0ixBn
4nojxD7PMLM0i+i1AvVNJNaHY9TtgIgg8V/C0C7vL8SdBN01e5ZRI764ohu9ivYv
Ixxvt7gzvSTpe+NUT1i09xNgsC8v19WB/BwkqMAGDqMxqCxt4fyrVvWpxNBke75j
E6Q3xCjfdOWYcfMLK7EsTSgimYuonZjN7v/yqTdjn/iVH+agL/2MlSfiU36w/Yf1
7EM09uKGH/Javh+2Vjd0j8rE/q2Iaac5VI91M6xz5oDZUknycBKKinR+nJWMt5AK
UAaL2Mjl3YtrUGBpxxY=
-----END CERTIFICATE-----
```

5.4. Bob's Decryption Private Key Material

This private key material is used by Bob to decrypt messages.

```

-----BEGIN PRIVATE KEY-----
MIIE/AIBADANBgqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQCq0cCUE0yIEiT
ImrAet/IOgVbCPw/1nW5h2rVqoi6h++OgDKN0DxNuWFEZ2a9og5JA56mw2NbWS
jUUTweU0z0kefUT63MfeYp+f4bZ6tj5gWQw1Nc+8wBR0IDz57U4nuT3WBhcOnM
has/cpzTFOWwny0YnqaHJ0lffa/T8e7Ie18pBB806w8fxLnKJ09yJa4HtaPRfjF
jW1QDPatJICWca+ETMoVtbjce+Nhc9SdFYy1cXJrV20roRv0z+SVuF1mF4Msuy
MtRjdhTvSv1VcYz+pyN382FZimEJ4FyqzBozmZcth2bSYWaqh5wXraZQTQ0I12
HAp02d593RyWX4PcVAgMBAAECggEAEvPt6aAQJEJzHfiKnqt1U7p4UKb5Ef4yFr
E7PdTLkeK2RjncIhb6MeevVs8g06co7Zn8tuUT95U3c0XLhV0WTvaHYeurTXakn
ICz3Ie0oS18skiVZko70uJ8pR6asWU1r/z0j1EwZ7RnEUWet97oM0YeA07LDFDk
F7eUq//6bfzTewr/QfDDsv+erwJBh+9CRH0JyTuDH1WeGxYV8VK3M6VhdTjFxx
FhrQ4pBe5J/UA17Bd2Gm8Urg6VYzVo6x4ajnc1H/ezYLdc459poTffv6Fg2trq
FVAj2IrQ1Aeqjda1emsa6Np801mUGknq3fjKS13RYGBv/48rCH0T8eRgQKBgQDM
5TuS4ANQj0Yo0gtFxoVjbVlnd0o+SmdFkZihzQHxcblY9HXe5H1bLf1IMXz/nERx
l+SmYuuJk0EdiM9rHOCcHRLfBmC7t0GdVvLDHSAX8Ec47LbtKZqyM1U9dn7Z+5q
4iywqpaP8pP3+oY57cgtQax1jle3xhRAj65c11RBmQQKBgQDVbLqK6wKDFsdZu
MZGUtOY0rtambDCgEU6rEqBAyCPy5NpF1pomUFcYKWT/wbReFqtuyq20yiATB0yH
HMko46BUtN7qX/m/sktDHWXVWs1+G4IgEMVokM9jjrkgdY5grrJ68sagKC+bgv
35BizHPiQgQu06qnPSrM9bevwbQej1QKBgQCiPE/zeBSnzyjeaTdLxGkR1R+ZX2
WqdNdYqnQkiWMkf1aSmt5J4raEj+GhLC5BZsZ6+z480M6XXFWOWSkbMv5WH1824
KHvgKcfoh00iR1EVyjn1gDxwK0QvjycMhs3FpXn0arjCczS2wSGpGGEpUR4JJhcf
faF6kphZsWDWzV1AQKBgQC2ivbK1tNhj4w2q1m7EGC3F5bz15j0I1QTkQXYbsp
M8zwz6KuFR3+1+Wvlt30ncJ9udOXFU7gCdBeMotTBA7uBVUxZ0tKQy19bTorNU1w
Nn1zNnJbETDLi1WH9zCdKrTICPtFK67WQ6yMFdWzC1gEy5YjzRjbTe/rukBP5w
eH1uQKBgQC+WfachEmQ3NcxSjBRkUxCcida8REewWh4AlDU8U0gFcFxF6YwQI8I
7ujtnCK2RKTECG9HCyaDXgMwfArVzf17a9xDJL2LQKRj9ATeSo34o9zIkpBJL0N
CHHoc0qYdHU+V02ZE4Gu8DKk3siVHXAAj/RJSEqAIM0gwfGuH0hhto6A7MDkGC
isGAQQBkggSCAExKzApBg1ghkgBZQMEAgIEHjImYZS1Ykp6InjQZ87/Q7f4KyhX
aMGDe34oeg=
-----END PRIVATE KEY-----

```

This secret key was generated using provable prime generation found in [FIPS186-4] using the seed 98c8998652958929e889e3419f3bfd0edfe0aca15da3060dedf8a1e8. This seed is the first 224 bits of the SHA-256 ([SHA]) digest of the string draft-lamps-sample-certs-keygen.bob.encrypt.seed.

5.5. PKCS #12 Object for Bob

This PKCS #12 ([RFC7292]) object contains the same information as presented in Sections 3.3, 5.1, 5.2, 5.3, and 5.4.

It is locked with the simple three-letter password bob.

```

-----BEGIN PKCS12-----
MIIX6AIBAzCCF7AGCSqGSIB3DQEHAaCCF6EEghedMIIXmTCCBIcGCSqGSIB3DQEH
BqCCBHgwggR0AgEAMIEbQYJKoZIhvcNAQcBMwGCiqGSIB3DQEMAQMwDgQIE/d6
qDQ/28QCAhQGgIIEQJKA5kzRVm9d6rEwC/0RyBSgpPuSR0UQTjspt6EhBZlgHc3u
FTCPa05P/vpeWacnBRarGFn3DmqA3JT+59bmRpGdiP3Zr1k2EbHi0yrd2P3UFDnX
qRkKI+7pf6e0HWJRntJA+KJS8v3tZ/hpiEKAeav/Mq0IFNFyEiZpCkbKCX5auDb1
p5c3J2MNg/WNBfpGJUHKVizuIF3H+8LfFgayRsDsppoUMffR+GmdL8nxLiqhraHD
+Iqr3LpEroNi/iZQWUTFTUlaePf/2KMqaH0uy41IVvcH1jIcLXHGNaa66S8AP/Hj2
TJPPg/lve76DvaGdEnx4QJd4pBFQac90zmhxU1HZrvzubK9t4e51r80wpd2djvZK
wSLzUgtQZxq8pSs1r85vrb3KItdYGF6SZpX029FS7rY3uYth5SYVUQWdUYYY3S0/
nsaLg4MCWU04Sh7nYJZ15Ijkk9LS7JhmvKvizHRRTXbLyRDH06e+jCRgLcU2WSUq

```

1bEr9Jy0ucK8zNPTf8HWBTS0ubvy4Jf03mVp4REX/8ozXlLztWGb1FGbyaJ9Y4ga
LM3JpKxMtb1UTxoAyj3iFwGlZFGKBlWp1r+0dkKkC4dl0FE22IINfLdRNLV9mP0
aGZhsDheB8iV0tN01u91B1U68Q7AL1ryXWUSjouKGRSU6uMDLZ7rw0w1ZC1m4oLG
BF8Cm04ELmb0ci78fBs/qDXlF3BJazcNtciamEsQPYRGkHASBRYtoDfVvy6mTT40o
obdrZigcvCwttDBu7RtynAQVZ8DvKzxFGhe2p2Yc9H5A5ML7IwqNtYzheduBAQTE
jAU2jMqwnZN5wULEnH2TF6KAQNRKdtBYMbqkToKgxf5Zf+cJZbyQq7WM6nVf0M7g
kcFdeHdn/CWoSNHI1+JA3wSDM06zkU5HMD2MpT1RLTSaemImUKCAGYieJmwNQxR9
aYHBBw5BNBw1XRB7WRka2Uah0Xq/wAgaI/o9L+mShDRFJjFi+t8AV3KR0WWWHg020
9qchX7P5H3Sy/tq8yUQIo1+hRiRjkfi9qy6AxIRttrK4WbW4scUtBZSk9uFkTVU
ybnV6WvBpn2SrnwF/E1ueKARVmouWJ/7fiLJXk6wVvVtuBZW2gE5QGfuCwq0PQsC
xPx8MhN1KZYDVCgsyUr/LMHeKNc31S2HLGQK7kh/o+QQazafiJocQ+kRbS1VX1D
nQlIhz4zvKsBgZHpoe3wQcfAY5sp2ubepsZ5T/YHkmroBmvA4g1vi7n1CetgxXrh
2V60XvaZ+BnfsYxJeUZGnNMNEDFlzS7xB18ojtT5JN0o+9tLsdikdikl69IsVv+2
eCv9Go+wh19cSAL24rkzdKVuiIAXS7tze13eWGjdKq3Ke+tfJtobSGrB39xgLVr
3ho63hd+qTUyjcAhVL3hAJinv+/KT0jR8fq+CDsXMnCEWugHhwB+66N0r876MIIE
bwYJKoZIhvcNAQcGoIIEYDCCBFwCAQAwggRVBgkqhkiG9w0BBwEwHAYKKoZIhvcN
AQwBAzA0BAjiGuDSkfG4UwICFLWAggOgyL08hPtU152dk0+BVimcGXW3FmDrT0D
gU3Drd0P76KzYzd21LuGb9dx84wx0XnFIXeBM4F3QSDbCK4t0uJ6JRaEeUoCAyZd
XyHtLjVeuozt2xHBDUGQVE01dZhtk1VUgzLSCha1rXjcwpa4+8xqqoVM3C15uBh6
QLUNey8Z3Y1K1k018Tdge600Urg72BPKppNfJ1N4Tn0FwMVMA/qHAJl4pL1YDpmc
5BZm4tMg0HvPiz96uwjEhw1GZFG0gZIoqeVJuqCNiZPDjCFEDgnCw6sciS5Bi+dX
Km0VUdamSr93e2eEPLbzxZr0E0A3Ic0j66iHuZpU9YhKzsAIhLMxT8kf81I0ZZzj
8N+P1hmkjdVWuJLg77pkXxQJyvuT0e2oc9r/DCHjckneen3+E66IKsYbib7sX4g6
2oFBJs+7xQopy69pC8jCn3fx61t7AFx2RiVvVHY/eU4sXoWkJNqQ3Vxj2SPWKjzJ
4IIvWVxIFiQjJ0tDFdGYPGukJXn62Lbb8CFgam9s4jDKnr0LHIngVeUIgi4wkvva
QzZTzXfUApezQgQy4x+ogdiYF1U0a00aqvrGRiiJlMdRi0/MDy+jzkX5cULhxf
vdBNCirv+3zBaiJ5Eu6q0zP5Cxi2qXhSbehZqvTPB4dD/vu9yxHpZmUCvzm7H213
Tdrb9WxH0c92ZpBzsfICA1smVwTDFVGa/kqN6noPw0qWZANIk27/+apsTkBYaVpa
jpf9eydi5eV2+pEQV08fh40JfIKbHS012E3Gp/rPm91VgmCmjBWh+Di1k4qgF/f
lsxWgzXN0xPntpohnM6AZDxW9Sk+BE1DLYS4WFwUg679BsJG6hQqAZKvG/8agSH2
k+TKKYUbXbFVCB0+iuNZIwgf4qxGzvI5+Iok+OcxuGCqw0u30QbfECEG01QbKETn
ic3kMiZ5Cxt7NQsuyEYaq/AmvM4qo0x7Tw1r7tR8BcAEF6fGxd2VXIv8Tr/pXG02
HL+0iIHs+0b67z1ThR7wUB4tCp9LC3IIWdsr7KcSRNEMxpUIFI0etCjNgCU3it+R
9152150fWNGxQfaXTEyMVNaT1HpwiHIsSb9QHbagaRLbYmqJ+ILSECADYQPEWf+
LT01tcOhkIb6BiwVWUu00qNj6ILJM2XvmknATyUj9MYcd77x0JzMrJE5VtaM5BVT
oRpcOLfhY0mihceGSEqXX5go1kqfLUze7zls1NWMYTTLw6tC6I+c/IUIWJnZT4m2
RbTQ0krfPn94zbTjrg42HS5+Ke3ySV6Fv8MZ+s93yY1v9iB6cVPEuteLRc+C7e7t
lw0bQ2+MyAkjenS5Td+3tC71R4202CSfy2Sa0sRv+EaYjTGzf9F3TM706o5+VZrM
gtIKtw2okRcjRhaKDFhui6jo46YYzWbrgOS3vzc60VcwggnNbgkqhkiG9w0BBwag
ggNYMIIDVAIBADCCAA00GCSIGSIB3DQEHATAcBgoqhkiG9w0BDAEDMA4ECEyHXPVs
ncxTAgIUQ4CCAYDSB1YeFnsa4vtKApbLnd9FENDYeYqkKmj0lkDagMqHC22/nQ9v
gz210o5FQJoaJx/WSorQt0Jny1QP9vZd2t+bkfoaXOR0MtmFY5S0tYEudJp1rCz+
ZEw8JlePJR0Q3lnwEiSk5NnXLRWNzurIeuyZEd1VbTvi/rF22sRWlmU335L67zj
P1sPeXkBPiYCPHw8E4rkaC8G1ko5wyrnhuqL4Itzhv00RvgRaDflpP9WTj9LVUv
FD5D59zgB0ptaW0jIw4Jp1IGXIEZiYnW4KfkWy2YJvsXiuLHvN3Z8qL6VtxNGk1s
g340uKkUULzmtDJqGT9RVkoYBXn7KYesbStt0NhPwDv/MxHrEo8TGHZAvbmwgt
hOUrc/WVtUopPES4QgrsA8d0MrSd51VtPW0XPSBPEnLuh7dqAlmgztY1P4Yztk2/
JJ+E4MosmhRjbKzM2N5WuGLDC5m9KF/5JjNVwQ7e8gMeUv/3gizgCG/4Mgng0VGG
IxGzzBoQXPWCKdT3sLQVyt4/pqPBpZYnPO9bmkkY/UIa1unNB+WWpL0kKSzD5wRv
/2xmN02D37DnHwTFYC51Zb1Kz7FGjOgCwG95VPc8NQ8aG5rqpQ+muq/Jil5mXgNw
IDeM4bawa01UKEzqTGQuB3gsJMGiV0hgtOrBi09Kx/2PJolUuwZGcho4oGSVR7KH
lLgIuC8aIQDyFURVYRCNw0w5U7JN5arkvZ4ty0/qk5UbjxQuDkF8o6ZdVi03l0Do
C+6zvncDx4HvUd6uQ+u/kZfr8qfwM5o6D2qXhS/ZHskq2xwIzb47uUUqaeg3y0ZJ
++na7gc+ibtHXXnNsHUvPbpCn9qViFhzi1cQZYq0tZxDKa0E/pzEP/IA4IG24wEL
GnyuUIHXBS9T0MchTx17Bglyc0PRDnFKzMQfUXY1rAErK76cs3y4VQDbfYDi0zsa
1qqMApIX4i/qKfDrVduLxtZQbVA/rNumm40LPUQ50vEngIESA74G+//YQbvjbMjP
y+hm7/15q5LRO9YxCS49KGlz4NG1QMWjnfkP0CNVZVpaQ7TPGOIYZBL6kTCCBZgG
CSqGSib3DQEHAAcCBYkEggWFMiIFgTCCBX0GCyqGSib3DQEMCGECoiIFLjCCBSow

HAYKKoZIhvcNAQwBAzA0BAi0/0ICbTbZLQICF0wEggUIFWt/JI8UjJQPfYTFonJE
o8zEbpYWXKboqw6/zZsMGMAnUPgQNQDxyuLVprs5jUc437kVB2M3F0x8DjmEppeb
tHfIoyjoXF7jdnA4EF38tsso0K1nMPmSgl02iYzt0qs0vBpfe05Hj40vhi26J9Pz
TwPcgl3QQPqfWv7CwgGVn4/hntBARIpSE4gAlfAcqkxtJBm01QwDoAds0K0MsYnt
gWajpr1J3Hm+34NPL04Usf10pcesPUJ4CBxNyLXxjjs0zD78WVvKY+N+j89xTsy
z5Y0fEkFqrc18pgBQxH72jBwSCm5YwHz3BhWQgr2bpWJ1f2LWcVsnrN9tx6RhQtA
AkcyNgX/ksp5EW4JTo+o6oXLRhXIYauRrUrisMY++b8ZJTp6C1t0RW2QdqqMZghS
ZgaW6FSC6Dy2Dd/ezdkYUCgiEtq8eSxF/8WDw6Va2iGVSNt4/p/OJ97yN5y0J0K1
g0hAtEbU+I3E74PQ9RK84FfJvyHDBC6fvYZW/ouMcgp3YmAF+dTm74Hq88X4daV+
/UPYf/cVpyiwcBTg6H3jrkrs0yKoWLIfrIvMNBeeKZ+f12Enw1MFzkLI4VGD/UeR
wrbbN0SHkh51IGtu0yRTfq6msYQpkw+jr7QwJIdQyrAaaaVaRotVvygTOLlHw8r6
o7v36yoNov3kDPW7DfbSVTWX51IyQn8NqMwa4N1c1WT8ukfZXSAyYkFSqF3w5za1
a4iIhu03GjDcfiWLMULYVAUcvSmcIULE1oW7FKiJc80adeIu0JBYSRSEvf7B3w81
eYUs+u/h1ptrZZKhe1JdAtlszvHJ0DD0kMqA6Ig4yomscGSol/sRUqpecIQwVZTC
RRq9dJOFJkKhKD5E09E0Z2snp01fpUF5q1MeBjpYgkX7jhyFyvq+qDqBAY8izvkc
ruE69WooBVyorqKHURjWtY+rhzcB4+HL72wZKzLnY3iUjJ1UANxM8mC9fpD1NJt/
7epqzPyZ2Kd4GJVYi8sQpFKf4tRHDr0tI5iUB78qj1EBp1w4qvRn/jC4ii7+Bas8
mz/AJ25QeviC44Vj+eT2YYXafDivrmoeBuVMIBbD066YnuBC2CeKydNWdiARzc3I
fhcuHvWq7riotYfyDqd4e0Jy7Y57pbwv4Qwz1yCXRjSwiFQ7/fRa2Cx8xtxKcC/A
4LGnXAKISy+uNbDWA7AYaP6RmGgMCaNiXy3F1zvxnE3bv68tXRF9vjuEChUq56N6
992qhoBuHP0J/mRItw+JoI4m/OFnEUGT3bNyxpEFyA7aXBE91aQdSX14a97nC0/R
SFH/fRwPFYgxr3XdcIF3Cw5PDs25YnsXWCsDCVeJWMFfw0zmDwa8sBkY270+rGv7
6qXvb/ugD3M2C+DySVy55Zd42wjghSezgY6taT0tqKfLOS6V14ELU78Q6va2o8M1
cUdi343t0i60MZgCDUwPP8TjKZINH8u1KNhZgpwNLz1gE0dd200l3bbzdZ6uio3R
52WQWRCK17Z91UesCJavytcAi0mMefMxBPM0dnUi608TPDRA0mcohbE5rybwDXAo
B/VUbwgM0/qCpZ7VcSKN1lUuo9+Kho0NK/gyMEvntMxGNNI8arV8UkeFollPhrt
umvdwqbVCeN8TBj5vXo6Hu+eKB7AVwjBk/rRHpZxnnVGXbm8HzM+kjib2cY1dius
VRJ/1+Q9GXuo135tQbobgcMzAmqAqZp9KDE8MBUGCSqGSIB3DQEFDEIHgYAYgBv
AGIwIwYJKoZIhvcNAQkVMRYEFEqzrDFTAKmcTeNueeAlYzU+igIIMIIIFkAYJKoZI
hvcNAQcBoIIFGQSCBX0wggV5MIIFFdQYLKoZIhvcNAQwKAQKgggUmMIIIFjAcBgoq
hkiG9w0BDAEDMA4ECCNi2K1bMEiBAGIUdGSCBQDLIXo4ExcyE8+4aiZIJ/Wnh/SV
VVR0n7s4PGCbXt+Vr0Hd9YzTuUicAQIcHH62dv7NSy+fgqZG7SmVR1IodadFe+5u
sAzXoyyhhEe2c+ToeVbr5rs+vBvQUyh6X5XTV5QV0AkWsyKGjyfdy86x1Q8cL2D2
BM+Rpkm1cFtjgWcB46U6S6w50sG7XOKSCMI4a6rnHPVgPPdXMrj3VSPJY8bhBqED
PVTnfSHf/wKZrIi5403F33B5jt6Cm9+9m9Fed8n+81w59rRom72CY9Xii/ULER9T
HwjxOZQO+dIm123Kauwexu0Gjii0UR8MeM/A0n7UNys+bZTulgdpWW/mDhJ+eLAT
nhJw5ro/AWA6YVVG+t5k9LjdJ1ZmqS4bJxvBwilPEGoh0MM6Yp0dr1XM4mT/E0JM
WD458Ngs05CuCpwAUXGdQmgrVsFrrV0HTyHeVLDhe43J3GI6HCWJV0eDQzzma03A
M+IooRDkTHnJMaxUXphKTag5+f/smNYEhzVjZeIc8GFZ36eSI4BNGHsXFACwLu2T
hkzpXMMg50JAUhBYxqE/fVevLUH4JPLgz869wk8gr1UBo6ihQGrnsx7Z05IsYahE
Yjz0N05PVPJYMLSyMovG9i+LpzQ49gIBzPu2fdLR41u5n505mG1Y4aJ70CJxMORY
hWHuctHdGdpJsgiq8+1iiUwmfyCfb0ZL3ePMU+W0zkAsyn22aK8jDBLLVZlv0ZIV
qR3Gx4QFPsk6qCMQ0E58VkMUMxYvClzTwSeEMu66eND/AKTE+XXV/d9bmSmWgk7Y
8XrDKLKfmrdr1leondVJv5mk12YKxBPQGeUqK5XJUa2dzH9zvEX8iYzdt4281QC
iXJ3qwmBT+8Ro0LBt4Ky0s2e2ZSZnrL9004oUsHI0yEfjwnWoLhKbkmun8GJxoB
2yCzTawVQf9/qIUXaSzcp23AV6Lflk90f79HYPW3cQJAtjf6XBVE1xVZPkftu3y
VLuf1js2ed/ctPhg9nuId/xHFH7t4HbmU3/Zufe1GHnsRQ3kbnqA5WXerd9UzeoD
aVDjFXGrITp8env08GXyvwWGXL150l0DuJSv1E+1yww86SNjBYUTx0r0CJjjTk2
7vIUhAYUEA+J71IeifqPDKYXnrCdUEajbFEdek30WiLR+ChEvEp48M1a6UVTLm/
mjziwbsxm5Q1Gccmz13e32RiyrfsB+RyllmzeJtydP2IHkWK7pww9y01PK0QtZs
66IGZKqeXrWBk9QFYDX42gAy/xTfglco4K07akhp3UzTIQyTXnt+Os0Scc+ArVm/
dwClm+Zxybt0cVyadjpKWydyfAr3aTkGxX6RmHrEW1R9BnMGPyEsDs+yeVNs1Qd
Dhff/bQLwCLXldGLWwLe6kitUiyi8F3bdfPjR7R611EUvJrBm7YLmgdxRCJ02LFLG
n09iSMNe5vmiNaKiuzfb4Dp9dqEMhmJfdsTURagfJIyqULoe08EIIozahivbzoWV
A6oPAkk2D8DnTiMegX4IZ/Zb3LPxJKAeX03Ys1YQrNSNZ3B2ZISBapzGzhFZFRVz
P0mXhN53pDhlxkw0btKb1YA9CvP+kzgewkzCy/M1q/Hb038CV1NKzay3yg4nteh
J+v9/k7gaqKmo3ZWMGk0WGBv/GFxYhmeNd14Y65D9T1ypM/zrXSYGo0qZgSA6H1A
gogzwwSaGwx9n/o6czE8MBUGCSqGSIB3DQEFDEIHgYAYgBvAGIwIwYJKoZIhvcN

```
AQkVMRYEFBfFhHvQp+92kDi4s28IvJK1niuUMC8wHzAHBgUrDgMCGgQUgwafFeGU
n9Q1rAOUCgw+KWxk+8EECJ1vqXe6ro0FAgIoAA==
-----END PKCS12-----
```

6. Example Ed25519 Certification Authority

The example Ed25519 Certification Authority has the following information:

Name: Sample LAMPS Ed25519 Certification Authority

6.1. Ed25519 Certification Authority Root Certificate

This certificate is used to verify certificates issued by the example Ed25519 Certification Authority.

```
-----BEGIN CERTIFICATE-----
MIIBtzCCAWmgAwIBAgITH59R65FuWGNFHoyc0N3iWesrXzAFBgMrZXAwWTENMA5G
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTEwMTIxNTIx
MzU0NFoYDzIwNTIxMjE1MjEzNTQ0WjBZMQ0wCwYDVQQKEWRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzE1MDMGA1UEAxMsU2FtcGx1IExBTVBTIEVkmjU1MTkgQ2VydGlm
aWNhdGlvbiBBdXRob3JpdHkwKjAFBgMrZXADIQCEgUZ9yI/rkX/82DihqzVIZQZ+
RKE3URyp+eN2TxJDBKNCMEAwDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8EBAMC
AQYwHQYDVR00BBYEFGuilX26FJvklQTRB6TRguQua4y1MAUGAyt1cANBAFAJr1Wo
QjzwT0ph7rXe023x3GaLPMXMwQI20f+apkdG2mH9ID6PE1bu3gRRqIH5w2tyS+xF
Jw0ouxkJyAyXEQ4=
-----END CERTIFICATE-----
```

6.2. Ed25519 Certification Authority Secret Key

This secret key material is used by the example Ed25519 Certification Authority to issue new certificates.

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VwBCIEIA889xRDvxNT8ak53T7tzKuSn6CQDe8fIdjrCiSFRcp
-----END PRIVATE KEY-----
```

This secret key is the SHA-256 ([[SHA](#)]) digest of the ASCII string `draft-lamps-sample-certs-keygen.ca.25519.seed`.

6.3. Ed25519 Certification Authority Cross-Signed Certificate

If an email client only trusts the RSA Certification Authority Root Certificate found in [Section 3.1](#), they can use this intermediate CA certificate to verify any end-entity certificate issued by the example Ed25519 Certification Authority.

```
-----BEGIN CERTIFICATE-----
MIICvzCCAaegAwIBAgITR49T5oAgYhF5+eBYQ3ZBZIMuujANBgkqhkiG9w0BAQsF
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGx1IEExBTVBtIFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAqFw0yMDEy
MTUyMTM1NDRaGA8yMDUyMDkyNzA2NTQxOFowWTENMA8GA1UEChMhSUUVURjERMA8G
A1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBMQU1QUyBFZDI1NTE5IENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAwBQYDK2VwAyEAhIFGfcip65F//Ng4oas1
SGUGfkShN1Ecqfnjdk8SQwSj fDB6MA8GA1UdEwEB/wQFMAMBAf8wFwYDVR0gBBaw
DjAMBgpghkgBZQMCATACMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUa6KVfboU
m+QtBNEHpNGC5C5rjLUwHwYDVR0jBBgwFoAUkTC0fAcXDKfxCSHlNhpnHGh29Fkw
DQYJKoZIhvcNAQELBQADggEBAGV0x00EzgYlRKixMcztiikxxJDmRat1pcipD15
1n8kiBoGhsT4fNZJVoL00QBa/WTMntL+qcAk2itqZCNIEZeGklUljXBaz5tkDRAF
f/v99LEcsZTcuIbnJqz35danQkp4/upG4hPkfx+nbc1bsVylrITwIGOpnGhz7z3m
VCK03DFE3Qt4w9m1v9yuMse33nmsBGXog/XZvM2JRY0iKt0xksQqQD9uYm7MoMeH
qQs30t7EaoPj54xyWvy42run6TLUye64D94SNjB/q/wjL96bsVIKGrRn10T1ybCh
4F5HD00hQZgP15D1b1rg+vskN8MSk5nuD+6z1VsugioW0+k=
-----END CERTIFICATE-----
```

7. Carlos's Sample Certificates

Carlos has the following information:

Name: Carlos Turing

Email Address: carlos@smime.example

7.1. Carlos's Signature Verification End-Entity Certificate

This certificate is used for verification of signatures made by Carlos.

```
-----BEGIN CERTIFICATE-----
MIICBzCCAAbmgAwIBAgITP14fVCTrtAFDeA9zwYoXhR521jAFBgMrZXAwWTENMA8G
A1UEChMhSUUVURjERMA8GA1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAwBQYDK2VwAyEA
hIFGfcip65F//Ng4oas1SGUGfkShN1Ecqfnjdk8SQwSj fDB6MA8GA1UdEwEB/wQC
MAAwFwYDVR0gBBawDjAMBgpghkgBZQMCATACMA4GA1UdDwEB/wQEAwIGwDAdBgNV
HQ4EFgQUZIXj05wdWs3mC7oafwi+xJzMhD8wHwYDVR0jBBgwFoAUa6KVfboUm+Qt
BNEHpNGC5C5rjLUwBQYDK2VwA0EAwVGQWbdy6FQIPtFsaWvG2/US2fnS6B+BzgCrk
GQKWX1WgkTj4ME0qL+0cFXLr7ZQ2DQUo2iXyTAu58BR6btcCQ==
-----END CERTIFICATE-----
```

7.2. Carlos's Signing Private Key Material

This private key material is used by Carlos to create signatures.

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VwBCIEILvvxL741LfX+Ep3Iyye3Cjr4JmONIVYhZPM4M9N1IHY
-----END PRIVATE KEY-----
```

This secret key is the SHA-256 ([SHA]) digest of the ASCII string `draft-lamps-sample-certs-keygen.carlos.sign.25519.seed`.

7.3. Carlos's Encryption End-Entity Certificate

This certificate is used to encrypt messages to Carlos. It contains an SMIMECapabilities extension to indicate that Carlos's MUA expects Elliptic Curve Diffie-Hellman (ECDH) with the HMAC-based Key Derivation Function (HKDF) using SHA-256, and that it uses the AES-128 key wrap algorithm, as indicated in [RFC8418].

```
-----BEGIN CERTIFICATE-----
MIICNDCCAeagAwIBAgITfz0Bv+b10MAT79aCh3arViNvhDAFBgMrZXAwWTENMA5G
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcjZm1jYXRpb24gQXV0aG9yaXR5MCAXDTEwMTIxNTIx
MzU0NFoYDzIwNTIxMjE1MjEzNTQwWjA6MQ0wCwYDVQQKEwJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzEWMBQGA1UEAxMNQ2FybG9zIFR1cm1uZzAqMAUGAyt1bgMhAC5o
MczTIMiddTUyTc/WymEqXw8hZm1QbIz2xX2gFDx0o4HdMIHaMCsGCSqGSIb3DQEJ
DwQeMBwwGgYLKoZIHvCNAQkQAxMwCwYJYIZIAWUDBAEFMAwGA1UdEwEB/wQCAAw
FwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB8GA1UdEQQYMBaBFGNhcmxvc0BzbWlt
ZS5leGFtcGx1MBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIDCDAd
BgNVHQ4EFgQUgSmg+i0gSyCMDXgA3u3aFss0JbkWwYDVR0jBBgwFoAUa6KVfboU
m+QtBNEHpNGC5C5rjLUwBQYDK2VwA0EAzss75UzFuADPfd4hQdo5jyAQ3GvkyvI
BdBGnWtJ1eT1WuMaIMhi1rH4vPGPd9scwW+sqd9fG+pv3MShl+zKAQ==
-----END CERTIFICATE-----
```

7.4. Carlos's Decryption Private Key Material

This private key material is used by Carlos to decrypt messages.

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VuBCIEIIH5782H/otrLy9Dtvzt79ffsvpcVXgdUczTdUvSQsK
-----END PRIVATE KEY-----
```

This secret key is the SHA-256 ([SHA]) digest of the ASCII string `draft-lamps-sample-certs-keygen.carlos.encrypt.25519.seed`.

7.5. PKCS #12 Object for Carlos

This PKCS #12 ([RFC7292]) object contains the same information as presented in Sections 6.3, 7.1, 7.2, 7.3, and 7.4.

It is locked with the simple five-letter password `carlos`.

-----BEGIN PKCS12-----

MIIKZgIBAzCCCpYGCsQGSiB3DQEHAaCCcCocEggqDMIIFzCCAvcGCSqGSiB3DQEH
BqCCAuwgggLLkAgEAMIIC3QYJKoZIHvcNAQcBMBwGCiqGSiB3DQEMAQMwDgQIwS3R
pT1mkyMCAhS7gIICsGKkBM0nci9VHfqx0TWy/lkKyQeF5bwsF/9gZrQuym1KtHZF
a4rSJIPUctmzqVnhGmfW9m+LEi7Em9rRmUIQbDZt4kQDG5eDk7AdhyDnB3uZDG1W
4cAeUVXJmZGfnwtzy5TzBZZe05nnVX74A1+PDW9wdpbv2TiriL0m29fBT+7HVS9F
Z/95XokSwbb6mmCYeGiPpNEaoeUeuU4zrh/k+JJqDuqNsU66I30wH0CFmk3aarBV
3LkEeCjKfKngzM0ZqiKZu8D2hEUjsGQ9ALsRn7P+hIWNFIg jvqgcCMTF8fLK1C/8
vYGD+H0pnn23nLele4b/qpFYx5kJ0b0K1Zo1SpGUQ7Bu6gectUceyOgi7CjRScuV
ew7918ZY0ugyYoIWAT0kecPM0TFtxAn19JPXo4jBYA1wUtx7GYA1DkgZCb/0dbkv
4L+PAeJK4kVDREDQ6ch/6/hlqU8xHeNzdagEwYL6FxWDiHebASxIvZzqkLd7RV9m
dL1FXst9R9G74j0s0WMMFMd9toyOhD0q6G19cat0rolCVS/CKaC0CucsJfiKr1J/
duQkt/JwcELveu0g60u2uaGKUqHmFhd3+6omk+wNBoY+0D5MmBZ/xnrVELGmzp94
q0f/HfZPT6sxkYBGUP2eUA/qR/zimNG3TuGVch/MdnduuVhvAYLyh1gbA8yRm+I/
zGCVuAqhsHITTx7Fqc3tyVp/mL YU00QuwmgAw6NhzwKZf5N+tR0DZGcgw8rZpeJA
yTxVfcjzXvoShxog7RroR9Nc4FwJhWI4B02410HFEiQZeRk8vzi8WIFXnn6t42/q
j1mV7Ba42zxPEGoy3m0bKwjR6rDp6KwmmfkghpwMPU3qP2/ASV8WT1+9GIYHc5Am
9CmSOT1QMLuW70Ra2k5ZMLwnbKNyMRbjUB/yHwwwggKvBgkqhkiG9w0BBwagggKg
MIICnAIBADCCApUGCSqGSiB3DQEHAATAcBgoqhkiG9w0BDAEDMA4ECOMzXMste/8a
AgIULICCAmgXa+q2JhTLvWsj5SKLdMninTk5uB6Hh0sDKYR9GDg/cABqUFxycR0G
JeJuewIRKJhsfdXJi+TSRtnQ0qpyVM9oRudxcBGuCI98fEbLmVyr7KF8GudTgC+b
ealJjn6HYkWpv71WdvsFG8BEy6Jqi3/tP9PgNvpCYgVVM7yx6SX8QArcLSQkxbTsv
Ae0iN18H89W9x0HEz4Z2qHYyb7f0pPHrmpTGC6qmtvo1gNRsKTF0wYeQ5Sy/9U3f
oM6bIcrOvHDKsaco4+5n0zeySDETY8W4m01K0uC/t0oT0ScYGBerhVr0DQapZGT/
Ej5LpgjX0uosAoT3IKnMwK3C00Z8oBzcvgSpeAa/V/OTKDPZb22yq6sEaHAPoUqb
cKRJmB6HC5mdLs3n0uP1v1ZuYsHu7EvT0Uhs9pbk1JDiCgM+4SFGKTRbd6Xt8bf
GHkWNmpv4pQL7jjzA3epP2DHyc8MJaDvleWY7Z3t/IEtkzVxf1Lo8kT21edz12cm
uFVK9i1MW3eJuyiRyFXFPgVsuNi/HFniJXfgxzAncP7fFP5MCs0o6daiEjJjemKf
J3D+HdD60gFih/eX9V+tg14y7/jtxCRA/54mit4sCy3LC0++1Ep9AtFwGYrDw825
uGj27a7mE26qgGdGXdzT9UJ8FfUsIoRPrG38Q4mhS10pTarNucWOGjkftZiKJLay
rMRf3HYx0I/7iupfxYLK/4/FODijaHzAfSdqf2Bo7csPaz2HqkK/0ny0+tt68S9
pUCjEfV6Liy22tang/jXxPFbBDK/P68Mnmgr8C3PcYhPJCo/K0JR2/8F8pVVEqd5
MIIDPwYJKoZIHvcNAQcGoIIDMDCCAYwCAQAwggM1BgkqhkiG9w0BBwEwHAYKKoZI
hvcNAQwBAZA0BAho9g0tQyYTvwICFIGAgg143SpNCoshZX3ikmK1m0IJP2Ah8Xv
94S/5NA8kwHtaNXpLrjYr3CyRL93USm55uvGAtECR/Eb1ON9zeo2p0gK2JPSbDr6
/1oovo7UoZNRoRBZ8pUegVWJswNWjqvzVu5JIRmpD05XjVDKHBfQixAqtj9/w3q0
Qq/p/M9UrLWD93hyLNdIppWr2KR2it9mASTKEHX9dqXcTOG0Kp2GmrfGNteGL02j
qVKZaZyYI8gkSxhVLS9zzgf10ynAkzYQsoo+GKhdAW1fJECemAyPc3L+eeARw/SY
q1d5QVwxKfYpIJ2wiiavdeRVNbWiwV7Ti+P9PtPx/hV22NNLwMhvnJcHaSS1Pa0i
SjoxFJ1EJWGES0QwcdwM8iN3oVuqT5HU/edMgx9TLNTiE1g2GEq59I/RwBtCL8Dh
0zKnUb4PU1Z81+HimV3KPI8g3cduhYaBR4HfqAhMnc+w5HXI6J3C1NtAE/izZ1Y2
Od71+GTJfjPgZiy0hjQfbMt8uU9D9aPr2XjN0WoKRSojae16v8bLx+dFn6RMxFUS
g3nLEZ6EDpyrJfpGPm6mPgZKSXtnvHuFcbS+utkRuVatqu07r2XpkGBIJLNVIRHU
5gLACbtj9TPcAce6RLoaYSDgOuFK0YZMdwzhsAI0YMPyHsUEZpQ5tjWSBY6ENbvF
7+QhmDnf6N3Bj+vxUtGS40pVsYCGbmOD7UM5QpUxIgVkpPrfRok0Zs/fi9sW+Xy6
eQ2Brbn3t9C2TAs0RYzFbuBwuTCqFW/rXHS6iffJpx2eAg3DCqaUAJjptSV/yzj4
vxiX1DB3fMRcpNd5Je7DoHS4axuj7SLHdpNoUHs+qQsG6yDM5BEuXWGxo/L9sGhe
XQRUnkZ4m4g01sfGTOfDNurXx/oP0ym+B50q6nLUWv0tYZpmCVi1358dIEGPPSMY
AMXh05tIPfYdYSJ3WLS0cxy5X4sXZ15w16Pzeb9SF5topqRUB5PDTfVr2bQUMwTbp
99Fc0Qf6cg8HXyT+8b4qKp9WyjCBxAYJKoZIHvcNAQcBoIG2BIGzMIGwMIGtBgsq
hkiG9w0BDAoBAQBaMFgwHAYKKoZIHvcNAQwBAZA0BAgNhF0EdzSrQICFF0EOCEq
Fie1peiCS90SXNqjLwbN3k081YM2HqeSZoEKJ4JSF1V1kWW3xwfu5aZKrGEYBfGM
d8renRijMUIwGwYJKoZIHvcNAQKUMQ4eDABjAGEAcgBsAG8AczAjBgkqhkiG9w0B
CRUXFgQUgSmg+i0gSyCMDXgA3u3aFss0JbkwgcQGCSqGSiB3DQEHAaCBtgSBszCB
sDCBrQYLKoZIHvcNAQwKAQKgWjBYMBwGCiqGSiB3DQEMAQMwDgQINFCqIEMfd9UC
AhS1BDgZruEsSaBY+Cm9WKR8HhH3JXh+AoMSrwdCKytWt+MNIXB0jY2QZHDn3u
Fn7qHw06MDthnKniazFCMBsGCSqGSiB3DQEFJDEOHgwAYwBhAHIAbABvAHMwIwYJ

```
KoZIhvcNAQkVMRYEFGSF4zuchVrN5gu6Gn8IvsSczIQ/MC8wHzAHBgUrDgMCGgQU
8n0YIWrnJVXEur957K5cCV3jx5cECJDjaZkfy4FnAgIoAA==
-----END PKCS12-----
```

8. Dana's Sample Certificates

Dana has the following information:

Name: Dana Hopper

Email Address: dna@smime.example

8.1. Dana's Signature Verification End-Entity Certificate

This certificate is used for verification of signatures made by Dana.

```
-----BEGIN CERTIFICATE-----
MIICAzCCAbWgAwIBAgITaWZI+hVtn8pQZviAmPmBXzWfnjAFBgMrZXAwWTENMAcG
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnRpZm1jYXRpb24gQXV0aG9yaXR5MCAXDTIwMTIxNTIx
MzU0NFoYDzIwNTIxMjE1MjEzNTQ0WjA4MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQL
EwhMQ01QUyBXRzEUMBIGA1UEAxMLRGFuYSBib3BwZXIwKjAFBgMrZXADIQCy2h3h
hkaKDY67PuCuNLnnrQiHdSWYpPlgFsOif85vrrq0BrjCBqzAMBGNVHRMBAf8EAjAA
MBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAdBgNVHREEFjAUGRjKjYw5hQHNTaW11
LmV4YW1wbGUwEwYDVVR0lBAwwCgYIKwYBBQUHAWQwDgYDVVR0PAQH/BAQDAgBAMB0G
A1UdDgQWBBRIA4bBabh4ba7e88wGsDOsVzLdljAFBgNVHSMEGDAWgBRropV9uhSb
5C0E0Qek0YLkLmuMtTAFBgMrZXADQDpORBZitzXGYUjxnoKVLicWL5xner97it5
VKxEf8E7AeAp96POPEu//2jXnh4qAT40ymW0wrqxU1NT8WW/dSgC
-----END CERTIFICATE-----
```

8.2. Dana's Signing Private Key Material

This private key material is used by Dana to create signatures.

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VwBCIEINZ8GPfmQh2Amp+uNI5ZMbzyvT0ltwvEt13usjnUaW4N
-----END PRIVATE KEY-----
```

This secret key is the SHA-256 ([[SHA](#)]) digest of the ASCII string `draft-lamps-sample-certs-keygen.dana.sign.25519.seed`.

8.3. Dana's Encryption End-Entity Certificate

This certificate is used to encrypt messages to Dana. It contains an `SMIMECapabilities` extension to indicate that Dana's MUA expects ECDH with HKDF using SHA-256, and that it uses the AES-128 key wrap algorithm, as indicated in [[RFC8418](#)].

```

-----BEGIN CERTIFICATE-----
MIICMDCCAeKgAwIBAgITDksKNqnvupya02gkj1IdwN7zpzAFBgMrZXAwWTENMAsG
A1UEChMESUVURjERMA8GA1UECzMITEFNUFNgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTEwMTIxNTIx
MzU0N0FoYDZlIwNTIxMjE1MjEzNTQ0WjA4MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzEUMBIGA1UEAxMLRGFuYSBib3BwZXIwKjAFBgMrZW4DIQDgMaI2
AWkuU9LG8CvaRHgDSEY9d72Y8ENZemwibPugKVK0B2zCB2DARBgkqhkiG9w0BCQ8E
HjAcMBoGCyqGSIb3DQEJEAMTMAsGCWCGSAFlAwQBBTAMBgNVHRMBAf8EAjAAMBcG
A1UdIAQMA4wDAYKYIZIAWUDAgEwATAdBgNVHREEFjAUGRjkYW5hQHNtaW11LmV4
YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQwDgYDVDR0PAQH/BAQDAgMIMB0GA1Ud
DgQWBBSd303UBe+a7GCGvCdtB0nOWtyPpDAfBgNVHSMEGDAWgBRropV9uhSb5C0E
0Qek0YLkLmuMtTAFBgMrZXADQD6f7DCCxXzpnY3BwmrIuf/SNQSf//Otri7USkd
9GF+VthGS+9KJ4HTBCh0ZGuHIU9EgnfgdSL1UR3WUKL7tv8A
-----END CERTIFICATE-----

```

8.4. Dana's Decryption Private Key Material

This private key material is used by Dana to decrypt messages.

```

-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VuBCIEIGxZt8L71Y480Eq4gs/smQ4weDhRNM1YHG21StivPzf3
-----END PRIVATE KEY-----

```

This seed is the SHA-256 ([[SHA](#)]) digest of the ASCII string `draft-lamps-sample-certs-keygen.dana.encrypt.25519.seed`.

8.5. PKCS #12 Object for Dana

This PKCS #12 ([[RFC7292](#)]) object contains the same information as presented in Sections [6.3](#), [8.1](#), [8.2](#), [8.3](#), and [8.4](#).

It is locked with the simple four-letter password `dana`.

```

-----BEGIN PKCS12-----
MIIKtgIBAzCCCN4GCSqGSIb3DQEHAAcCCm8EggprMIIKZzCCAU8GCSqGSIb3DQEH
BqCCAUAwggLcAgEAMIIC1QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIZNqH
TA2APx0CAhQXgIICqK+HFHF6dF5qwlWM6MRCXw11VKrcYBff65iLABPyGvWENnVM
TTPpDLqbGm6Yd2eLntPZvJoVe5Sf2+DW4q3BZ9aKuEdneBBk8mDJ6/Lq1+wFxY5k
WaBHTA6Lnm1/NkM3za/fr4abKFQnu6DZgZDGBZh2BsgCMm09TeHgZyepsh3WP4Z0
aYdVSD0LiEzerDP10BgjYahcNLjv/Dn/dFxt003or010TTUoQCqHJ0oq3hJtSI+
8n0iXk6gtf1/R0j6Jrt/3Aqz/mLMIhuxIg/5K1wxY9AwFT4oyflapNJoZGg9qwGi
PWVtEy3QDNvAs3bDfINQqAfJOEHv2z3Ran7sYuz3vE0FnPfA81oWbazlydjB0P/B
0Q+s6VLbsAosnZq9jv2ZVrCDaDA1/g7oD7fY8qmaC602q5/Z3KusfMt+r9En2v81
H2vjgrpxnDIXjYuLZdrnNE/slRtqad0GR/WQ358RG+yUmRUbHYHGnkjn9f0GLasI
ZUV0aowivcWyF/kR7QV3VVexgqJMX6k1vzSXR0J/tnA+1/WPWy1mCJe1jG0gYqSV
txtVB61Qmc2XP48F7wyaQZvdAU9zfe11/tHAaKKJWBpE11IuAEKgtIP6ozYJBFjH
I11tBA8fijTnug+S40vSgjtSRV/+kSEiW4F+pwE8RuTYfUu7q+Ew0LYdLgkH50yE
sn0b62UFpR/E1D9exWzohrFbIdUCbjtssXucruAqPNhW/abT0zicWu5nvf+Pniow
2VxvhwoGt5jZ+1kaR5Z+1/GpbMgq47EUyGCgKv+5GAcJxUxINZqLbACJ/MhLfYPB
eJrXz8f5Cigm1wZLisYCqnuc8cGCXjNqNkUlqtzodM8xv4gcgT/zILxmJTZP2q4n
YA4yBQx5/n2G2dZC+pf3kAfbXcp0MIICpwYJKoZIhvcNAQcGoIICmDCCApQCAQAw

```

```

ggKNBgkqhkiG9w0BBwEwHAYKKoZIhvcNAQwBAzA0BAjxuoiaSZDbnwICFH+AggJg
k2hcNYt00+15uLqXdiNhr5Q0JkYcrHdo0wR6G5AgLmwI+TYi+P8EZUjDIJ4TJ3b4
6xv7+3pT8cbEFf6PXcfS8/sCFm7FaV3SpLACLZbBJV520KE0CAgALZOLuIz5mGVU
tWI2h1x587KeIv5GRPIxumDebT3Gmkkp9Qoi55hjTgn68o1SgDaJF8o5wnf0Dhks
o110a3x90wkJSN1AXfmBfj33KnT8Dc4bTfAZy1S5o1zCtaEqnct2Urb4Pe03LfHB
ErBsvY8HE4D7qh6P5ftXHQAAX/b3hbU8jQP1tR0N90h0SiLi//ebCeGXWQRdVjL5
+VQrh1QF5d4Kz9Zx79oC36g7C2BxCQomur/F9TT12NPzPpaEGGo6ljB6myAHnYw9
rCxbSxBvbtEt1gJnxxb1Y5Q4ukgyjzK6431Bwq2+iNL0vGc9o2c5ELUPU9zGeLBZ
tXWvdX27aOHjusPfDZ170C5zHiYs1FU6Tkn9Aotc424Q3d2IRTtCynnjs1VS1sSr
4bRyB8zBAQmdQrniBW++7eJm3m/E0U0Yy0noUT169m8KNJrmSspMvKS6pyiYHR4I
BvAIkRijvdtQvJdQJ+Uyr+HH5daE6go1W1917b2bXj/41mvXYkJY6W8x0km1RYhH
QJZphW1vNcrHKO46Unk48Qc/5J5tI+6UDTXFr//V34vcpQ2ktp0MAK11rBH549ef
CsGQTGoq8XHPksehEEMRm0JDeKTVKkx8xNhbwb395yFCIxfF2NHeDLXP+JyW+nH
Iy2fnBDlyTiPF7YXyGiPjPAgK8LS8GUE+Zq2rWqrGNkwwgM/BgkqhkiG9w0BBwag
ggMwMIIDLAIBADCCAYUGCSqGSIB3DQEHATAcBgoqhkiG9w0BDAEDMA4ECOFJ/s3Y
f5bgAgIUnYCCAvi4NaYP4lpAtuXtE02Zqg19aLFwsj9B/rikBo601ZR/lSryJ4PJ
VGyY6NyBPjG67glJVMYiI3Hge+j66FXKXD/AaiMVD21ZmfrH935S14ZUKS9tpTJL
QDw3ejpDEDqJUFJZJ/ybgpRAKoNjhcE3B7F7+WMI8Pr70M1Fbw7ytUCAj0f18sIW
prUA8f809dLiGgiWyjE5HMzSXEib5IMRpq5x4Q28pBrT8rVYgoQSSyVkfHtU7LDi
Bm68RfBgEl7jIqLdrt2kKxHC3/lC4xXQgFNXeQ056aRp8Yu4VpoRwraVLU03tJk+
pf1zFfmUei/JtiFlC6uf0Pvc2B5h6kAZocE11LxGIDFH7ftD6dzP7qTDbUQ+uEk3
qsgktT2pcoVnxTanvQmTCEZM9ZKCX5/z7Gkm+z831GLDDU9oNyRSrxHrRBIvgH4w
3aGH1v6kfY0WwwwagHQIZFyzGVRKXsP7As1L+n4ti831TxqSUZX2qy9LpI4Tjp
5A/NLMKo3uqmHF1TLnnYUqoppe88FNY8T/LXnHp0KTkuXFmdKJtp1/ydqh18jBk7
nflCqFdf1R/5okysblRtaMujlhelymT7MoM8u5C8ceI07uWX8NI5B/IB+Yn2BvzZ
9LXoSia/wHjTu7UK610o7W0q9qTYe1i1x+HsmJa0C6hpaQh6b33VWDrHJb17c/4Z
tvQ9qAzqkqIhFWMRXNK+32jFVAgXrD8U1QHw2ip5s7W/Xtm1AegrhG1nSQgJezY1
OnE/t2PDWuPeW94kr0uv1fNsh6p1LyZYf/BaqhoGCHsa/ipD86viVSZDgJ8ASVLF
eLUK3HYFMhJ+MLEzZJffYZA0nbYoyNPNc0vc7dpbk+ZMnlb5bDFcMCpm7+fW0jsC
nsNNL9nqQ1NHHCJRKGuX05rujftbPM7R3GLT9d/u5e9YY5cX0RiDLxomFffl1j2Yh
uRoyX+8WzEst98I/KmAraWKXnxOP1FEWajtNcrnGCezDK03xEHTQhECpg+z704mj
MjN6MIHABgkqhkiG9w0BBwGggbIEga8wgawwgakGCyqGSIB3DQEMCGECofowWDac
BgoqhkiG9w0BDAEDMA4ECL2Bz1vW+YZkAgIUugQ4Y0yEjke53NDvCFR0ciUH7re
f9/wPx5TgV3qzGhfR4bP2rdpi0t9hAHVK5cmUAR7+wjAJiYdLUQxPjAXBgkqhkiG
9w0BCRQxCh4IAGQAYQBAGewIwYJKoZIhvcNAQkVMRYEFJ3ftdQF75rsYIa8J20E
6c5a3I+kMIHABgkqhkiG9w0BBwGggbIEga8wgawwgakGCyqGSIB3DQEMCGECofow
WDacBgoqhkiG9w0BDAEDMA4ECFw78Uk8K64uAgIU+gQ4id0jRb3JyEM5fdpaeQR+
YEeMn+Y5Kavp1VD5HtgQQY9hhppbQqG4af7KY+MT6xus6oNEQeJAE5wxPjAXBgkq
hkiG9w0BCRQxCh4IAGQAYQBAGewIwYJKoZIhvcNAQkVMRYEFEGDhsFpuHhtrt7z
zAawM6xXmt2WMC8wHzAHBgUrDgMCGGQUzSoHpcIerV21CvC0jAe5ZVhs2M8ECC5D
kkz12M1tAgIoAA==
-----END PKCS12-----

```

9. Security Considerations

The keys presented in this document should be considered compromised and insecure, because the secret key material is published and therefore not secret.

Any application that maintains a deny list of invalid key material should include these keys in its list.

10. IANA Considerations

This document has no IANA actions.

11. References

11.1. Normative References

- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, DOI 10.17487/RFC5958, August 2010, <<https://www.rfc-editor.org/info/rfc5958>>.
- [RFC7292] Moriarty, K., Ed., Nystrom, M., Parkinson, S., Rusch, A., and M. Scott, "PKCS #12: Personal Information Exchange Syntax v1.1", RFC 7292, DOI 10.17487/RFC7292, July 2014, <<https://www.rfc-editor.org/info/rfc7292>>.
- [RFC7468] Josefsson, S. and S. Leonard, "Textual Encodings of PKIX, PKCS, and CMS Structures", RFC 7468, DOI 10.17487/RFC7468, April 2015, <<https://www.rfc-editor.org/info/rfc7468>>.
- [RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <<https://www.rfc-editor.org/info/rfc8032>>.
- [RFC8479] Mavrogiannopoulos, N., "Storing Validation Parameters in PKCS#8", RFC 8479, DOI 10.17487/RFC8479, September 2018, <<https://www.rfc-editor.org/info/rfc8479>>.
- [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>>.

11.2. Informative References

- [FIPS186-4] National Institute of Standards and Technology (NIST), "Digital Signature Standard (DSS)", FIPS PUB 186-4, DOI 10.6028/NIST.FIPS.186-4, July 2013, <<https://doi.org/10.6028/NIST.FIPS.186-4>>.
- [OPENPGP-SAMPLES] Einarsson, B. R., juga, and D. K. Gillmor, "OpenPGP Example Keys and Certificates", Work in Progress, Internet-Draft, draft-bre-openpgp-samples-01, 20 December 2019, <<https://datatracker.ietf.org/doc/html/draft-bre-openpgp-samples-01>>.
- [RFC4134] Hoffman, P., Ed., "Examples of S/MIME Messages", RFC 4134, DOI 10.17487/RFC4134, July 2005, <<https://www.rfc-editor.org/info/rfc4134>>.
- [RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <<https://www.rfc-editor.org/info/rfc5322>>.

- [RFC7469]** Evans, C., Palmer, C., and R. Sleevi, "Public Key Pinning Extension for HTTP", RFC 7469, DOI 10.17487/RFC7469, April 2015, <<https://www.rfc-editor.org/info/rfc7469>>.
- [RFC8410]** Josefsson, S. and J. Schaad, "Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure", RFC 8410, DOI 10.17487/RFC8410, August 2018, <<https://www.rfc-editor.org/info/rfc8410>>.
- [RFC8418]** Housley, R., "Use of the Elliptic Curve Diffie-Hellman Key Agreement Algorithm with X25519 and X448 in the Cryptographic Message Syntax (CMS)", RFC 8418, DOI 10.17487/RFC8418, August 2018, <<https://www.rfc-editor.org/info/rfc8418>>.
- [SHA]** National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHS)", FIPS PUB 180-4, DOI 10.6028/NIST.FIPS.180-4, August 2015, <<https://doi.org/10.6028/NIST.FIPS.180-4>>.
- [TEST-POLICY]** National Institute of Standards and Technology (NIST), "Test Certificate Policy to Support PKI Pilots and Testing", Computer Security Resource Center, May 2012, <https://csrc.nist.gov/CSRC/media/Projects/Computer-Security-Objects-Register/documents/test_policy.pdf>.

Acknowledgements

This document was inspired by similar work in the OpenPGP space by Bjarni Rúnar Einarsson and juga; see [\[OPENPGP-SAMPLES\]](#).

Eric Rescorla helped spot issues with certificate formats.

Sean Turner pointed to [\[RFC4134\]](#) as prior work.

Deb Cooley suggested that Alice and Bob should have separate certificates for signing and encryption.

Wolfgang Hommel helped to build reproducible encrypted PKCS #12 objects.

Carsten Bormann got the XML sourcecode markup working for this document.

David A. Cooper identified problems with the certificates and suggested corrections.

Lijun Liao helped get the terminology right.

Stewart Bryant and Roman Danyliw provided editorial suggestions.

Author's Address

Daniel Kahn Gillmor (EDITOR)

American Civil Liberties Union

125 Broad St.

New York, NY 10004

United States of America

Email: dkg@fifthhorseman.net