

Workgroup: lamps
Internet-Draft: draft-ietf-lamps-samples-04
Published: 18 May 2021
Intended Status: Informational
Expires: 19 November 2021
Authors: D.K. Gillmor, Ed.
ACLU

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 Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 19 November 2021.

Copyright Notice

Copyright (c) 2021 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- [1. Introduction](#)
 - [1.1. Requirements Language](#)
 - [1.2. Terminology](#)
 - [1.3. Prior Work](#)
- [2. Background](#)
 - [2.1. Certificate Usage](#)
 - [2.2. Certificate Expiration](#)
 - [2.3. Certificate Revocation](#)
 - [2.4. Using the CA in Test Suites](#)
 - [2.5. Certificate Chains](#)
 - [2.6. Passwords](#)
 - [2.7. Secret key origins](#)
- [3. Example RSA Certification Authority](#)
 - [3.1. RSA Certification Authority Root Certificate](#)
 - [3.2. RSA Certification Authority Secret Key](#)
 - [3.3. RSA Certification Authority Cross-signed Certificate](#)
- [4. Alice's Sample Certificates](#)
 - [4.1. Alice's Signature Verification End-Entity Certificate](#)
 - [4.2. Alice's Signing Private Key Material](#)
 - [4.3. Alice's Encryption End-Entity Certificate](#)
 - [4.4. Alice's Decryption Private Key Material](#)
 - [4.5. PKCS12 Object for Alice](#)
- [5. Bob's Sample](#)
 - [5.1. Bob's Signature Verification End-Entity Certificate](#)
 - [5.2. Bob's Signing Private Key Material](#)
 - [5.3. Bob's Encryption End-Entity Certificate](#)
 - [5.4. Bob's Decryption Private Key Material](#)
 - [5.5. PKCS12 Object for Bob](#)
- [6. Example Ed25519 Certification Authority](#)
 - [6.1. Ed25519 Certification Authority Root Certificate](#)
 - [6.2. Ed25519 Certification Authority Secret Key](#)
 - [6.3. Ed25519 Certification Authority Cross-signed Certificate](#)
- [7. Carlos's Sample Certificates](#)
 - [7.1. Carlos's Signature Verification End-Entity Certificate](#)
 - [7.2. Carlos's Signing Private Key Material](#)
 - [7.3. Carlos's Encryption End-Entity Certificate](#)
 - [7.4. Carlos's Decryption Private Key Material](#)
 - [7.5. PKCS12 Object for Carlos](#)
- [8. Dana's Sample Certificates](#)
 - [8.1. Dana's Signature Verification End-Entity Certificate](#)
 - [8.2. Dana's Signing Private Key Material](#)
 - [8.3. Dana's Encryption End-Entity Certificate](#)
 - [8.4. Dana's Decryption Private Key Material](#)
 - [8.5. PKCS12 Object for Dana](#)
- [9. Security Considerations](#)
- [10. IANA Considerations](#)

[11. Document Considerations](#)

[11.1. Document History](#)

- [11.1.1. Substantive Changes from draft-ietf-*-03 to draft-ietf-*-04](#)
- [11.1.2. Substantive Changes from draft-ietf-*-02 to draft-ietf-*-03](#)
- [11.1.3. Substantive Changes from draft-ietf-*-01 to draft-ietf-*-02](#)
- [11.1.4. Substantive Changes from draft-ietf-*-00 to draft-ietf-*-01](#)
- [11.1.5. Substantive Changes from draft-dkg-*-05 to draft-ietf-*-00](#)
- [11.1.6. Substantive Changes from draft-dkg-*-04 to draft-dkg-*-05](#)
- [11.1.7. Substantive Changes from draft-dkg-*-03 to draft-dkg-*-04](#)
- [11.1.8. Substantive Changes from draft-dkg-*-02 to draft-dkg-*-03](#)
- [11.1.9. Substantive Changes from draft-dkg-*-01 to draft-dkg-*-02](#)
- [11.1.10. Substantive Changes from draft-dkg-*-00 to draft-dkg-*-01](#)

[12. Acknowledgements](#)

[13. References](#)

[13.1. Normative References](#)

[13.2. Informative References](#)

[Author's Address](#)

1. Introduction

The S/MIME ([\[RFC8551\]](#)) development community, in particular the e-mail 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. 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.

1.2. Terminology

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

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

*"Mail User Agent" (or "MUA") is a program that generates or handles [[RFC5322](#)] e-mail messages.

1.3. 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 mark 1024-bit RSA and 1024-bit DSS as weak.

This earlier document also does not use the now widely-accepted PEM encoding for the objects, and instead embeds runnable perl code to extract them from the document.

It also includes examples of messages and other structures which 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 e-mail ([[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 draft 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, there are no OCSP or CRL indicators in any of the certificates.

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 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".

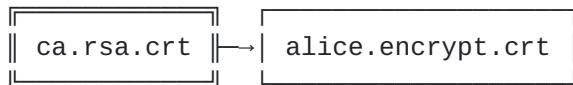
To test some tooling specifically, it may be necessary to install the root CA as a "system-level" root CA.

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 with either 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 ([Section 4.3](#), `alice.encrypt.crt`) can be validated by a peer that directly trusts the Example RSA CA's root cert ([Section 3.1](#), `ca.rsa.crt`):



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



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 draft is unprotected (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 draft.

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 [[SHA256](#)] from simple strings. 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 re-creation 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/zdaeCQlqp6yZUAGZUCDANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGx1IEExBTBVTBIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowVTENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFUMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlm
aWNhdGlvbiBBdXRob3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQc2GGPTEFVNdi0LsiQ79A0Mz2G+LRJlbX2vNo8STibAnyQ9VzFrGJHjUhrX/Omr
OP3rDCB2SYfBPVwd0CdC6z9qfJkcVxDc1hK+VS9vKncL0IPUYlkJwWuMpXa1Ielz
+zCuV+gjV83Uvn6wTn39MCmyu7nFPzihcu0nbMYOCdMmUbi1Dm8TX9P6itFR3hi
IHpSKMbkoXLM1837WafFx57kBIoIuNjKEYPIuK9wGUAeppc5QAHJg95PPEHNHlmM
yhBzC1mgkyozRSeSrKxq9XeJKU94lWGaz0zb4karCur/eiMoCk3YNV8L3styvcMG
1qUDCAaKx6FZEf7hE9RN6L3bAgMBAAGjQjBAMA8GA1UdEwEB/wQFMAMBAf8wDgYD
VR0PAAQH/BAQDAgEGMB0GA1UdDgQWBBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkq
hkiG9w0BAQ0FAAOCAQEACDXwLJGjzKadNMPcFlZInZC+Hl7RLrcBDR25jMCXg9yL
IwGVEcNp2fh4+YHTRTGLH81aPADMdUGHgpfcfqwjesavt/m00T0S0LjJ0RVm93fE
heSNUHUigVR9njTVw2EBz7e2p+v3t0sMnunvm6PIDgHxx0W6mjzMX7lg74bJfo+v
dx+jI/aXt+iih5pi7/2Yu9eTDVu+S52wsnF89BEJeV0r+EmGDxUv47D+5KuQpKM9
U/isXpwC6K/36T8Rhhd0QXDq0Mt91TZ4dJTT0m3cmo80zzcxsKMDStZH00zCBtBq
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+wIBADANBgqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC2GGPTEFVNdi0L
siQ79A0Mz2G+LRJlbX2vNo8STibAnyQ9VzFrGJHjUhRX/OmrOP3rDCB2SYfBPVwd
0CdC6z9qfJkcVxDc1hK+VS9vKncL0IPUYlkJwWuMpXa1Ielz+zCuV+gjV83Uvn6w
Tn39MCmyu7nFPZihcu0nbMY0CdMmUbi1Dm8TX9P6itFR3hiIHpSKMbkoXlM1837
WaFfx57kBIoIuNjKEyPIuK9wGUAeppc5QAHJg95PPEHNHlMMyhBzC1mgkyozRSeS
rkxq9XeJKU94lWGaz0zb4karCur/eiMoCk3YNV8L3styvcMG1qUDCAaKx6FZEf7h
E9RN6L3bAgMBAACggEAE3tFhsm7DpgDlro+1Sk1kjbHssR4s0BHb4zrPp6c18P0
6T8gwuBcj1Dz0zykNTzaMaDxAia4vuxVJB1mberkNHZTFqyb8bx3ceSE0CT3aoyq
5fiFpR0L6Ba1vgg8RTvNCAIApHNa4pVx0XD8Wq+h7mlUA0YGBie5U08/P2qWjc0z
+zcheyYXJS/uu0t2/F0ihEWGcXBmoc8D++n7mKst2jKAHD4w1PN2MgVqnmagpBz
gobFNmCZYzPDS+PPTtQZ1XvdGF5Sodc+Fz+jpWun1kxDHE4UIZZDA/HAAgORbm
aEzVs0s9ZExeq0tqu2fPB7zF/1JKdRk4UJ0UxS00QKBgQDJwonP5Rwv00sYoCiw
zuFcYTmN/hI3R3viKuxr19CH6+mvuIU85ooIHF6TiouZwhk+6+Vx7rcXds554DT4
2RbVrX/5i/M0zx8c8IIwoZJIasLz+vx8F4n6hyhV65bXN7AIBojMh2dt8tP2MZ/R
VEfsk4mNm06yKuzYAfjJziCnQKKBgQDnDH9UYUIPkq0PSvViKQFJFCB9BJPFhld2
pIgoziw/JZz3M3W3IWU0KwG7UxS0T3xmn3IX6xmWw4vX1/088yb0bZWYP0edb61GM
I9DoI5igndLgDwyOL2PFuZh5pqqc09DE+cpJW4nNoudqTNmCrjhmXNCGKgGjld8z
/OkSccvywwKBgDd0ReajRUziEjDxjF2UbzKx8lzJsX4KIs22GIdHqSRCv1cy80Qa
5WN3ULNiyB350HCP69wDFMXym5rJoQjPvh6GIuhYKv4V8ffffxkYv5kx5uWiXZVJ
7v2x+m8rMqlyv+pkYWL8KKytHmdiBzD+oTwxF7r4ueLjtaxngzx93pAoGBAKpR
rR9PnroKHubSE/drUNZFLvnZwPDv6l08T978tONL372pUT9KjR8eN31DaMpoQ0pc
BqvpSoQjBLt1nDysV2krI0RwMI0zAWc0E9C8RMvJ6+RdU50Q1BSyjuLGaKi5AAHk
PTk8cGYV01BCHGLX8p3XYfw0xQaHxtuVCV8eYgCvAoGBAIZeiVhc0YTJ0jUadz+0
vS0zA1arg5k2YCPCGF7z+ijM5rbMk7jrYixD6WMjT0kVLHDSVxMBpbA7GhL7TKy5
cepBH1PVwxEI18dQn+UoeJeBpnHo/cjJ0iCR9/aMJzI+qiUo30MDR+UH99NIddKN
i75GRVLAew0Izgt09EMEiD9joDsw0QYKKWYBBAGSCBIIATERMCKGCWCGSAFlAwQC
AgQcpcG3hHYU7WYaawUiNRQotLfwnYzMotmTAt1i6Q==
-----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 [\[SHA256\]](#) digest of the string draft-
lamps-sample-certs-keygen.ca.rsa.seed.

3.3. RSA Certification Authority Cross-signed Certificate

If an e-mail 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-----

```
MIIC5zCCApmgAwIBAgITcTQnnf8DUsvAdvkX7mUemYos7DAFBgMrZXAwWTENMA5G
A1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlc3R5YXRpb24gQXV0aG9yaXR5MCAXDTIwMTIxNTIx
MzU0NFoYDzIwNTIwOTI3MDY1NDE4WjBVMQ0wCwYDVQQKEWRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTVBtIFJTQSBDZXJ0aWZpY2F0
aW9uIEF1dGhvcml0eTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALYY
Y9MQVU12LQuyJDv0DQzPYb4tEmVtfa82jxJ0JsCfJD1XMWsYkeNSFFf86as4/esM
IHZJh8E9XB3QJ0LRP2p8mRxxENZwEr5VL28qdwvQg9RiWQnBa4yldrUh6XP7MK5X
6CNXzdS+frB0ff0wKbKa7ucU/OKFy46dsxg4J0yZRuLU0bxNf0/qK0VHeGIgeIio
xuSheUzXzftZov/HnuQEigi42MoTI8i4r3AZQB6mlz1AAcmD3k88Qc0eWYzKEHMK
WaCTKjNFJ5KuTGr1d4kpT3iVYZpnTNviRqsK6v96IygKTdg1Xwvey3K9wwbWpQMI
BorHoVkr/uET1E3ovdsCAwEAAaAN8MHowDwYDVR0TAQH/BAUwAwEB/zAXBgNVHSAE
EDA0MAwGCmCGSAFlAwIBMAIwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBSRMI58
BxcMp/EJKGU2GmccaHb0WTAfBgNVHSMEGDAwBRropV9uhSb5C0E0Qek0YLkLmuM
tTAFBgMrZXADQQBnQ+0eFP/BBKz8bVELVEPw9WFXwIGnyH7rrmLQJSE5GJmm7cYX
FFJBGyc3NWz1xxyfJLsh0yYh04dxdM8R5hcD
```

-----END CERTIFICATE-----

4. Alice's Sample Certificates

Alice has the following information:

*Name: Alice Lovelace

*E-mail 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-----

MIIDzzCCARegAwIBAgITN0EFee11f0Kpolw69Phqzppp1zANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTVBtIFJTSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFNgV0cxFzAVBgNVBAMTDkFsaWNlIEExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/pd0/KLpZbJOAER0sI7Aja07B1GuMUFJeSTulamNfCwDcDkY63PQWl+DILs7GxVwXurhYdZlaV5hcUqVackPvedDBc/3rz4D/esFfs+E7QMftmd+K04s+A8TCN012DRVB DpbP4JFD9hsc8prDtpGmFk7rd0q8ggnhxBW2RZAeLqzJ0MayCQtwslq7ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR+peC rhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKk01zQ1Pq90njlsJL0wIDAQABo4Gv MIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBawDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNTaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQwDgYDVR0PAQH/BAQDAgBAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOC AQEAc4minqf0qaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJ0d64roA KHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27PmhK E1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahixRn/C9cy31wbqN sy9x0fjPQg6+DqatiQpMz9EIae6aCHHBh0iPU7IPkazgPYgkLD59fk4PGHnYxs1F hd06zZk9E8zwlclALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+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+gIBADANBgkqhkiG9w0BAQEFAASCBAKcwggSjAgEAAoIBAQC09InoWDgWPk2a
f0+StijSNOR8K/hN8D+l078ou1lsk4ASvSwjsCNo7sHUa4xQU15J06VqY18LANw0
Rjrc9BaX4MguzsbFXBe6uFh1mVpXmFSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z
34rTiz4DxMI07XYNFUE0ls/gkUP2GxzYms02kaYWTut3SryCqeHEFbZFk4urMk4
xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFFi0ucfCn+IQsaqpo1d3f9jSkbtAV5w3
vzfog8919MxKI9H6l4KuElnAtJ7BtZcs17dUy9u9C0gEyKRiVokFQgqQ7XNDU+r3
Se0Wwks7AgMBAECggEAFKD2DG9A1u77q3u3p2WDH3zueTtiqgaT8u8X0+jh0I/+
HzoX9eo8DIJ/b/G3brwHyfh17JFvLH1zbgsn5bghJTz3r+JcZZ5l3srqMV8t8zjI
JEH0KC3szH8gYVKWrIgBAQ0t1H9Ti8J2oKk2aymqBFR3ZXpBUCTWpEz2s3FMBUUI
qCEsAJqsDEch+kt43X5kvAom7LC1DHiE6RKfhMEub/LGNHswY4dmzhaG6p95FJ1h
s8HoURI2ReVpsTadaKd3KoYNc1lcffmwdZs/hFs7xmmwXKMmlonh1mzHqD1/BqeJ
Hc8MP4ueDdyVgIe/uVt1Q9NcRQbuokkDyDYMYV6hzQKBgQD75ahYGFZznRktSE3
w/2rUqTYIwxx2PQz5G58PcsTZM89Hj4aZ0oLmudHbrTQHluRNcHoXEI62rs0cVPs
D7ILZ0Lfs+SSTeNEXd57mjyyufpV650cNc1mSJAmMX2jWQ8ndnOuWPcc5J6fNvT
au0a7ZB0aeKHnA8XXL3GYilM9QKBgQC35xKi7f2JmGtsYY21tfRuDUm6EjhMW6b7
GwnI9IXF8TGj15s7oDEYvqSPTJdB6PAb/tZwdbj9mB4qj176x1kB/N7G097408UP
/PdHkU7duyf5nRq1mrI+yGFHVsgD313rc+akYdKcC207e6IRMST1ZFoznC6qNgpi
nNTuDz4ZbwKBgA5Dd9/dKKm77gvY690bjn6oBFuUs05VaaaSlcsFOL2VZMLCNqQJ
+NLfZ7k8xJJQVcEIOT2uE7X/csBKdoUUcnL5nnsqVZQPQwI5G937KQgugylMZLte
WmFXlX/w5qzKXtWr3ox9JPfzveSfs1bqZBi1QQmfp0skhBo/jyNvpYUNAOGAMNkw
GhcdQW87GY7QFXQ/ePwOmV49lgrCT/BwKPKDk18l5ZgvfL/ddEzWQgH/XraoyHT2T
uEuM18+QM73hfLt26RBCHGXK1CUMMZL+fAQc7sjH1YXlkleFASg4rrpcrKqoR+KB
YSIayNhAK4yrf+WN66C8VPknba7us0L1TEbA0AECgYEAtwRiiQwk3BlqENFypyc8
0Q1pxp3U7ciHi8mni0kNcTqe57Y/2o8nY9ISnt1GffMs79YQfRXTRdEm2St6oChI
9Cv5j74LHZXkgEVFF02Nq/uwSzTZkePk+HoPJ04WtAdokZgRAyyHl0gEae8Rl89e
yBX7dut0NALjRZFTrg18Cueg0zA5BgorBgEEAZIIEggBMSswKQYJYIZIAWUDBAIC
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 [\[SHA256\]](#) 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-----

MIIDzzCCAreAwIBAgITDy0lvRE5l0rOQlShoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTBVTIFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAqFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFNgV0cxFzAVBgNVBAMTDkFsaWNlIEExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmP+ovBouOP6AFQJ+RpwODxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8g0UH/Cvt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxx5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmswqps6oQcAx3Weag0yCNj1V9V9yu/3DjcYbww2lJf5NbMHbM1LY4X5chwFNEbkN6hQury/zxnlsukgn+fHbqvDhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCAATABMB4GA1UdEQXMBWBE2FsaWNlQHNTaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQwDgYDVR0PAQH/BAQDAgUGMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOC AQEAgUl4oJyxMpwWpAYl0vK6NEbM1lgD5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LDsfx7fSIus8gWVY3WqMeu0A7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxODWq9opwtA/lT0kRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpfb8PPwDR6chMZeegSQA W++0IKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTS07K459CyqbqG+sN0o2kc1nTXl85RHNRvKQK+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+gIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCalsn6i8Gi44/o
AVAn5Gnck4PHHNjrSfWUnnelN41KImVaTC3D9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnV
z5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs165ernT905NLFf1HUjURca3ynqEB
BV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZuTtMc1zy++MxQlqdn9WZLh0A0peNZ
KGmVwjeVy+8FkyzC3jX/Qcm+ZLCq1LqhbWdHdZ5qDTII2PVX1X3K7/cONxhvBbaU
l/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy6SCf58duq/AOEksCAWlb+MD8QH9Y
j7CFSmq1AgMBAECggEADgxowEDDRE5yEZ+s7TMw+WH2o+3X00rryqnsLb0yv34I
wAAUWK7qZyjd9rSD0AtB0gFhQNXyHwZlT+0iHslCIfqJMz8wy1iFHBCIphoMSWs5
/D+idXrUef5Y23rClBxXH0g1UnSGXnpUH4ehV6p1lvZMh40JKEoMC4cpyd1SzXrw
+VGcc1+pXv/tTW3Rb2qow09JoWY+Epcssrw5N80FIF0Dh4QfbLN6pVTt28aQ4pf/
1KhLoapjFzXSyp/jrcNjYJ9qRdSAbZsK0J2yZ0yqjLHDCDipFty+w0pkUZcJhsgu
Cg1Stt7tKgSvAV/nEjN8e/vA91/AACKBCnCLzEoLgQKBgQC4eTM6BDCz1usXJBK4
SRC/WwUthJZzf0k2Gmwr0DCTRYhWQSDjBfiQNboazH0bVPz45qP10f0t2iPEHeX+
VWAXTNrN69M9lEzxygA3s76lAejBR3FbLwkzLYqPB3oZwSIE7CrWHTXJipFWZv+X
FG1R418fnRCUMJ4j85qem5iyqQKBgQDWhQMJu7FC02fr83qsIdLwqhiDtTpwUN3j
qfp7JoEZ0xbm3TgM1xPAkrQTUgfr2ZhXGtUwsuKHyifxQEycrTkB0g0ggAfG0fnv
ybyXK6/guctHJQiy64lL39kPuvQkKB+Y060B/oF6zbyFvqanoKXjpsp0bN3i3yBU
X5/E0u/LLQKBgQCUVvHwewAgSg+pgBx9jG0nPK4h0CkznRJ7qyuo37Tv+E317lFf
vYFvlySd4CJmmiUckZTvK3FkL7HrFo/HwSeQFQEt7aDkn8jX9bPPFv8K+UoNgkGp
LA8YVFRdQSPyadfNVYvsuXhzJLZSYGjPOGHgI5JufYLDZ4UDK/T97ekQYQKBgDDM
ORCxxvXTyGiW2USVu3EkaqFDtnMmH27G6LNxuudc/dco2cFwbZ0bbGFN8yYiBCwJl
fDGDv7wb5FIgypqtn4lpvjHUHA6hX90gShT3TTTsZ0SjJJGgZEev/2qqq+ZdF/
Ya+ecV26BzR1Vfuzs4jBnCuS4DaHgxcuWW2N6pZRAoGAwTovk3xdtE0TZvDerxUY
l8hX+vwJGy7uZjeg14cFecSk0R4iekVxrEvEGhpNdEB2GqdLgp6Q6GPdalCG2wc4
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 [\[SHA256\]](#) digest of the string draft-lamps-sample-certs-keygen.alice.encrypt.seed.

4.5. PKCS12 Object for Alice

This PKCS12 ([\[RFC7292\]](#)) object contains the same information as presented in [Section 4.1](#), [Section 4.2](#), [Section 4.3](#), [Section 4.4](#), and [Section 3.3](#).

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

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

MIIYKAIBAZCCF8AGCSqGSib3DQEHAaCCF7EEghetMIIIXqTCCBI8GCSqGSib3DQEH
BqCCBIAwggR8AgEAMIEdQYJKoZIhvcNAQcBMBwGCiqGSib3DQEMAQMwDgQIWQKs
PyUaB9YCAhTCgiIESCSrTOUty394FyrjkeCBSV1dw7I3o9oZN7N6Ux2KyIamsWiJ
77t7RL1/VsXsBLjVV8Sn5+/o3mFjr5NkyQbwuky33ySVy3HZUdZc2RT0oyFEdRi8
x82dzEaVmab7pW4zpoG/IVR60TizcWJ0ooGoE00Rim6y2G+iRZ3ePBUq0+8eSNYW
+jIWov9abdFqj9j1bQKj/Hrdje2TCd16a9sSlTFYvIXBWUdPlZDwvCQqwiCwmXeI
6T9EpZldksDjr5N+zFhSLorWABGRU8jXSU9AEsem9DFxoqZq8VsQcegQFY6aJcZ0
Xel7IECIAgK8nZlKCTzyNVALxeFw0ijWnW41tDaqcC6GepmuINiqqdD94YA0HxRl
1lKU4mLknSJ36W4T7vaI4fp98sK0nGpaDzQheu6BbQ+dVd44q52MDwvqvD0Y7UjF
IVEP3V9Ebf641CR0mIcVCUynxb3aaKjhgBKTGbYsKtPue974rDPIArMs2Heo8y3
cq+f7Jce0IVCglRatN6rSyJBF8JlBQW5pZGco8AwTM1pK3RrdIDziheA8DIBB+KT
4JZB06UprlcZ5wBY6ncXwa5E4feb57Cd3bB+zJuubBX9f4yG/J0cSF59w92c/6Qb
i4EFk6tAiz19PxuLLWjco71e69Jiav19Ph/WJpf/XCEurw7K+VAeZALFW41G/D30
WIBRC2shishB3j8+3fNpcvi4Fy3EkZNW4lrZFAjbBtloCcxk5rcfRS7vxucAvC5X9
4bm0xEcd0ysnuplH77u+CwWxjCk414SlKZTUbcw1a0B6yRDvojUMZKdZMqsxyYjn
JG5QhMFQrTyALwCgJsP/rAf5xPhG2p+9Qul0yiBIIzWvKNKRQKL+YLcvYvTh1bhj
rUflYzzvviyXCy9LcX2GBop9yBFJzIcmKfL0MGua6WIKWX2BIjhGTtu6VThmRHuf
OsqNg/ZrNCTYa7e1D6gWP5uFRecSZdASf+0XTe6M7e/vaN4Go4A3H8+d53SYQP6n
pTt/a0DTHzY77aNMh+mzkIHC1W3zUdlS48tUyJMIAN3Tt+RfhHZfgloJ7IdcYdM2
01I+UD/5L9ghxN8dh13Fi3rDyn6Y5xB1xFuZ0mLjoEI+3Pr1+B9Kgf+o/hxFttfx
1uP1XcHt0a4gBr6g7fWGNssfw5S6g6hS9UDTAY0pvLaatil2TzmeYzzij19ssv36
kr1VaRV9xcQCby05ucD+buymFXPn/rhVdxhgIydmv0tdzDozy0WFDtvGjUBNeRnC
eMVD6AlwdW0lmbQ0cIlJS0aY2Fwm8Kju62XZA8YIRowlLysuq3zIqDmzmjJFKwuA
mRMZmUVhophMEn86rwob3Z87gNbyy1U/dXi+s6Vybx/kiwDXjfyhWBnhn1gkhgiv
o0hgTt+yAlivUHQlEloQeQN04C5QTU0d1W0j489Ft6wpvm0tqc16NpnRYUhbCoF
XhFr4wswggR3BgkqhkiG9w0BBWagggRoMIIIEZAIADCCBF0GCSqGSib3DQEHATAc
BgoqhkiG9w0BDAEDMA4ECPoEFEHQGB9dAgIU5oCCBDA0rGHYN47xktt1J1VvWQZN
BYIMFzLN6p2/zKotGf7EMdgSdwlxkhKTWxunfoP/gfRD6boXTAA7ukJDsHXZrFXF
KjI4HI2oa/NihwqctphcLonBJXcofuHv+loP9MPLtwu3Mo1wsWTiHpf5XmxMoZQw
fbrp2ohLugJ01ZRB9RfAUpaAhtFg91pL0tXEpz7GULEyOnYh9R8iu9bSel8bpl4S
+AoxzXD4gYiEU6Yi0/47aRstd3H4u3ERDnUKSoqVstslRSKnK/WrGYUwoy7kNDwy
DBitfosMY0rpWEE5rXTBWJkBodcl3LBpDbNzdbrZw+e+y0bJ9zfrlMpl0xVfoiji
q9UbRdgN2yo0RKwF6c63V2RdF5tjQHnNIM3K3tC9zEis11jgn9Le0LB9Cd1qyE4P
WfMHn0gwqDF1eX96TmUipmYM63H6jcbnSc6p7eIZtCrqGjhsTqFwcMg04WaXWeHD
ffLXSZdzIUB+zfc8tftUUE0UX3tX411oU7K8uAuQTSK/AXwUj+MbQVhlz8te4FVr
w4ulZ184IYqhD3VdI0xXiZkfsKChRz8/7QacrXFvfKkrxS2iHMoxhoJ7WETntI
slw5R5runj61r50VT4HCFNFqfGBbTtV9AdP7yka9aQDwxPCoXFgeb1Q01F/BigzW
02JP5Lcrw7ia0y88QbTzWhi57d4he50Ip0wHUiGPh7s792m1ltvuSpRKJkOXWv6h
qAj5AsBB8JNvgXP71Ytx2vMdjw6gqzQcxASJ4UHqg0CxmiodLUP+FHAY1CPNSjBR
pHrTi1Ufi/+9hYneQci++qPvkCqMuGHVxamd40LanGJN1NxElDyMeduapX5rXuPn
g66LPey9GQuE3SBNC2dmju0y7d8fWEXEzqhqltPfsuwVzdnWb1uAcjRfQPN0+uWe4
zihYisXK3lqA557dRqdSv+6GL6/OZQOCTaYMyZIWD9jS2gU6T3q2j8uk1LNL9n8
aSpQ5xWspBXpZx039fG6CMeqzZlFCqrVqWYhdXbtxN90x/pimmW0lcqAxv+xythW
BMx+il1JEdbCj015wjmsCWNPWlM4AVSholpZhs9Mq6rvGBXi1HJgjD0DpSLCE0xh
/GNoXo0X3LrxFCIDEhT8LyZ2NE59yh3t6pm88soFzaAghdjb1Fkc79nBbc14NLKg
SmL/7GktkxEzn0iSYfnfJ905kjZC08d8RnoGfrDDUWD2ZiHbbx0Cq4E3E0Zt13aH
JOXRBOZLC9L2JNeSnIbZZGykh+Pi4TsIzXL2UPQ+dy4DDaEf8yamyY04dlhFsnhD
qr94Y9E30/rpF0yUb2gCehEgT9nppVuMeridsCkHqemmgVr/52Xv/XK9dx4+YBjL

4/3Id0/yVJURqDIHH8o4ogF4rf1kz0a1rZ9nJFugP0UM8oNysaL9yr7/Dli1juV0
MIIDZwYJKoZIhvcNAQcGoIIDWCCA1QCAQAwggNNBgkqhkiG9w0BBwEwHAYKKoZI
hvcNAQwBAZA0BAidIqBxZFwvagiCFCKAggMgTzrUv4/12Jqnv3AL+P6990uX1ybZ
NcTwC+hMRV0Ho0FuAAYbzdSRBAaZch1+8GheU8yz7IYwLn1PNHx1Z8inIYfmTfk
Pa34Rk8s/RxJIe8LMYL1qjk/FMq/Fpgc0S65S6bXvJ69Hb8gtAoGW8P1b0dd9bvG
NbAk00h5r+IWiH4U8zGpcqWDWRgieGICsY00Hvx4KKMV6FIjFVCTZev0RVoyzmSX
ZZgxqrbjw4CZqOWReHPI3aEt5xVX3BihRGi4EIyia6yU10VOZTGBKqWUeKm0A5Gw
SX3mH/kLiya3gwwGvdq1ncXc17V1STN1HFyp4ebGKg4CsZ6Nkwjocwq2PwM/TqoZ
5i02tqv0eR8lX7LrSegxGH81Kw3nMV4dH5txoVt9hddZCKKGcJ5Z8FlzxFP4BFuF
7hOmRpUPdxiahJ/GkXDVIAw6BJKd4Q9e6sjJYxTeq4u0P6V4PMuDU7F98X/d9sEx
2X3b1cJxuA7xtOnKAPsWEyWBg98B+CKG6Kw05s8T1ZVmlk15FCUjvFoKCiWIKF4N
vGLiW0IP/jJ9N6Gqp4gNbm51zNFGZ7gZAtvsBSGQSOUpgfZcx2mRxpBmcX8tm5YJ
hmY9EDK13umUUGKRpOrG8c7/MVAQegSKqQuXSfMK6KknXGe7jwjs7xaQaRm9fFHS
0KbGU3MsLxRGjw/jzjUNAEWDiSYPCVo8E/kd8LETvjAowF772y9o0X1ZzcP7HWc1
oYc0/WSSh4e+FAbgqLo/8KIKGzJ23BACdx8XAtxzUZhRdHaItwnaJsfr4TCwq8C
XxJG5u44/z6imqQrV0aXQfvk6sSNGdG62TkacYg2K63D9hcg+TbZPPVSStWxyj8S
N84anzT0xb1yx6aw6IL+uBLC4jISgNFijaF5pwjLSbgTs5Z7skZdCam80xYmdJV0
ES/uqFCQFUSamXXNbotviQk8jWuJFz+BXzPYJN3t+3mp6SmgTZ2zP8FUQEE4GbSH
DqYV621DcWRo/mao8xzX/mvKkm4ddGBldiushZaL4gdo2A1qThSMnMBsciC+jEj
DqOr70XhHccTDW8wggWUBGkqhkiG9w0BBwGgggWFBIIFgTCCBX0wggV5BgsqhkiG
9w0BDAoBAqCCBSYwggUiMBwGCiqGSib3DQEMAQMwDgQIehcRLmVUApMCAhQ0BIIF
AHb5dXZKzCeRUo2ZSj0oyuFS3zQ5HhKyfapsyCqbYCKv/lSzNYwvuda7xfa+uOM7
/wCB9sWdz0MTpaBMHwX9hvibZIY65oM+ry4tTuKKQ0Jl370snjB0dSNTKszsI3fa
PUjslxqIH3aC1shD70qhIRGZzRjK44PJyWv626oQrgVtTYR9NYTdee+SbBZbkEt/
EpWipwftWXGR6tSYJQn99e09Vih8HyQvwIpidUh3pCF0low4VZyAQIW0Hcw9TAjB
XNv+qfdh7fiX9wM5/GvnQReIsqjXCUoc6pSQIAqD/f+I/d1F2ZmqM7KwX0LGRER9
OWZGyF734pN9GLBNetWm6rKxmLSI/5m6+2Jxxfann16P+vBSEgWJ/I8GnJAdzIbB
Tyfjog4Gi2+lmrPzK7+C79ntM9nfsr4xvZy/BknwZiaJksd4Vv0Gks9nfm6shtBJ
B9uR+GJfthtsvIVUHN0kz2r/lVzMSRb0g9yR53hv1H/nXCmUjWz/BvobmoaVBcCm
mOnnYZTHMNarIVYdLQFif5ZLH7WV/XVEVioRntNRiKsK96VAHm5XboWQGCqL0heh
IX3Nily1genGm1aFlSQNMvLDko1ILDTrKINvPmjG/WFoLntpJFPtYZsooT1jjXLw
3VTSodtgKQNdpYOEidSJqWIS87fzrCB2Wmwys0iGfdsuNhSaqNqa0dM06FiW2fku
x7H+w7SX1/n9YeZUNLOcewLcC7E8IA1IarjglZE1L6Yb2ldXxv9q3PPowKuGnah0
TKnD6mLn5BIGOGTZf1VspXRrJhFrcLe+xsJR1r6niI3bcMwXy7gbm1X/CRE902I
ynxE1oDR+xZ6rjPwDJP7kvf4GvA8trCGrot4pbJbmwlBeMIy1ScdQoHEnyqrenOn
RMmXZakz13njtq7Wk78qoJq0a6Vh/sde0KcOPFkyTZdMB1Tztm0K2VJU3jUVzPlM
0WY2fyGD0A89o1+/MiNsgiaEghGybXBYip0ex+p7j1GIRN/CKmpwsqjZnB78kyXm
Z6AE1vC6neD/7zANInDkzXiun6ic72LoBX3JGiCSuM6hIPJ0AcDwlzTDu0H2rCQN
w+tivJ2v4KbgeKoc6beQb5fZHS7VsWHikIcpwqB5ngwt34wHgFG0nTS4lZmvzSJ7
FMRVGmsDYkDTPzZgN0axiUBQMCEvxNIE3nAmA+dvB7w6XRQVSUsL+vBFhHiWGZ7h
k5sCeHElewXK0SyJADgfflYq3EfEgZ13h4wtoSfbBVtzbbbyg2LNegUCLfIJkc7fm
T7X7JSxbjOgndMHEeMdVb+NFxbgsXYrYD8rC2A8l5cQzZrsxb1bvgybEJz+NU/52
UgGrPmdjJKuGBK/V2zor6qPvKyId1Gb4QQuIoyClwhZ+qk9nE4Eft84y7ISgMywH
+lw87HrSHKfpqzQhCxlrLu53IYK/4PhE7BYC9Q4tvIsZXSgZ+nju4tyzERSlaNe5
njUeIENr4B/+kXULwVDCvMFHqUFJMkFai8FUga7gyipZ+654clGgJjnNB01va8Jc
dtdPRRW4gwdrVn8u8J78KBzt6ChkrpKRV8VewKBk9lhct0ZNPJnNqhDrkFzHBqP0
Uo133I7P7C+h9sNDI153W6IOIodyQE0Av1WxHo4y/1d1VeGDaB7h0SDq9ZMpm9n1
En7F6/1/s4IUZHja/qRrK9hD4M0Xq0LhFXuUzuipo490MUAWGQYJKoZIhvcNAQKU
MQweCgBhAGwAAQBJAGUwIwYJKoZIhvcNAQkVMRYEFKJTQdVEPIApFXwBI/Dnjq/N

83cPMIIFlAYJKoZIhvcNAQcBoIIFhQSCBYEwgV9MIIFeQYLKoZIhvcNAQwKAQKg
ggUmMIIFiJAcBgoqhkiG9w0BDAEDMA4ECKq4DtyiaY0yAgIUUpQSCBQAKQtKPOS4s
LE60s7nP4RaJBuYXl27V/o6TusBRBgQoPzP+aC+099wgisEKedyB47bAzc04sba
4q8UKERAsYHcEhdD2hGRCL7ou9jTtrr4RgZpa5V9CJcB00t4bqy2lUef0pm6no+R
X840uyM4q5Q+cfH1rTQ1a/a+gLglbptoEkH/4dFR3ELYiXcM5UrBYTJ0HcyME8c+
TXbpf7kiplTtIsrlZyU5zrWcxngrBxwFA+085W/uVR3QZSW+EGx/VCYwGruZlNyt
BvBYjsYsnC+yKYXbqL81Dg0ePy+eh6VX64SwBLXcWcY+NK2EZrhZrUFjl+PXFkY3
IVVPJhTE9o7gJA0hzvAan0luWxozD3/WPQaXhyIJDwM2MjznjL2MBydpy9K8Cio7
XaV6PX8DsZIZkfI4DAZ5f7G7WbwUq3IjPPPWiUv+JsR+dnqzWDJ22Sxc+AdQP2sK
qMvP8g0Ph0sVlXXE76c5rUcZCZD+gGv1av07YttWqbDqLj6oQEIJ8LX0Qvwd0YEh
etE0bJ5uv2njhQDhLkH/JIbmFSgJZEm8dtKHb8f5wZc2B+nXGB+TFboGzSuP7gaW
u1vKsJNqT/J/FYEcamI2F+td7z1sGfBR9ckAcxXeb2uPVbCJ1a50gRlZ9qVm5Hb
5f53X7aoQqP3F3LDGQmJ+GFQ/oXXwabqn4TvN09KDhxpGcMMU9RnugUfNU9GBec0
vfrzmVKZdmJ36H0mMnLvGRakRhCV3kGABXY83hwUv17E1qASLKcAWIachkCCGpBG
yGtP2IOZTn7PsLJR1BzKnePa7MgFcgoCToIpdQnCTtAsalmbm1s480LN3GB5ojeG
bQvNf9TAVia0tg5VuT4/048V6uYSJsIZsawm3tGA/LjxyfV1aLddQT5ZF5ZX9BX+
K/PB4oYAFxtUpMK/aL5G1MvppUJ9CjqAtnoKE+EkdQmyZ1VoD09ih44zuRx6XV4A
EYafNB8ygjRHGsVPW0/M0Es0w16wzJHTuf/15fD/nH7Xh5MzhCF0CtvLn8v+S1Po
i2/4006pS2byjUFRbeCpzEpRxdv90LCb9ALdy0yG9u41W3yInKNFnaWBulf0PFce
ZT92M1BgwJA8ZcydtiunRNAH5iWLSPlOUp0D1v6En+rat+PoyRXIy2fLHBL25aw
LhABoZPgRsCiLsiNiohfYngksrQKeRg0laBMT92J8r1E4sUKirQlc0diWBE6vmBS
XzyN/twvfgPNIXgR0rw6c7VhHS+hNTrsttg/xcfvJ/bftDbKm+RZL+yQoOkkAf9R
5tizyMdBlaMrpfrBxvNtMiykbZ88SYoA70Trwab2aHqluVhs80jXGBE0qmSudcS
dV1EhBpo9HBsDZZi0Iw0p5/B9fCHdnThCTiUm80eQ6mX2/DB9LlNh7gH0yLL3azT
m12D0ZpZNaXyxLzdiRiAdwpWZmmeg00G70yi0D5eIxh6cbnBU6Ygdp+pFFVYHfA
vc5CzPne20PhXX2k00kbwawr9AfrFjIfAEmBFx5GBGr/lSiUQSkbUC/s209Yga0g
WTYt3KXPzrThJJGZnnXZRTGfIi6vp8RsnPX35+Dxe/Lp3gXDdIJewG6XVA8t3fsp
coTqPkm/XGNMmOZ81KX/ReVdP+dC93sov2DuDZbYGPmHlD47b00iA68GD64DEuNt
Q8MhWk8VRR1FqcuwB0T0bc+SIKEINKvYmDFAMBkGCSqGSib3DQEJFDEMhgoAYQBs
AGkAYwBlMCMGCSqGSib3DQEJFTEWBBS79syyLR0GEhyXrilqkBDTIGZmczBfME8w
CwYJYIZIAWUDBAIDBEC6rujtKFi2F7NJGihlMt4ptDGckray1zjr1/Hql/5Qw7iL
BSuc4wEGnDSBEZuE9oFnyTbrzzEtebTsXluPRoV5BAj10QCGvaJQwQICKAA=
-----END PKCS12-----

5. Bob's Sample

Bob has the following information:

*Name: Bob Babbage

*E-mail 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
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGx1IEExBTVBTIFJTQSBdZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFow0DENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxFDASBgNVBAMTC0JvYiBCYWJiYWdlMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5nAF0glRof9NjBKke6g+7RLrOgRfwQjch+2z
m0Af67FJRNrEwTuOutlWamUA3p9+wb7XqizVH0QhVesjwgp8PJpo8Adm8ar84d2t
tey10VdxaCJuNe7SjJfrwShB6NvAm7S8CDG3+Eapk09fzn2pwwaREQ6twWtHi1QT
51PduRtiQ1oqsuJk8LBDgUMZlKUsaXff8GKzJlGuaLR15/3Kfr9+b6VkcDuxTZYL
Zxt6+a3/QkaC3I9m2ygPubtHFJB5P5+s8boR0SKm10B1gsLow8eF9S70tcGGeooZ
JiJUQCR14NaU5bIyfKEZV2YStXwdztoEJJ2fRURIK+8Ynw1B3QIDAQABo4GtMIGq
MAwGA1UdEwEB/wQCMAAwFwYDVR0gBBawDjAMBgpghkgBZQMCAATABMBwGA1UdEQQV
MBOBEWJvYkZzbWltZS5leGFtcGx1MBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1Ud
DwEB/wQEAwIGwDAdBgNVHQ4EFgQUF8WEe9Cn73aQ0Lizbwi8krWeK5QwHwYDVR0j
BBgwFoAUKTC0fAcXDKfxCSHlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAG7e
QY6Px7WZC5vCbF5hj0itxoz3oyM+LRcSTGwoYXdm1wsNUzy31pE3dtADvevRtsP8
uN7xyfK6XZBzhSHA/BtkkqYGifvXDplu0xWmqC0WPmc1PNK2mHil+pGMfvnUwnxd
6gKcHED5p+bUhDyIH2fy9hGye0Us8nvi+7/HwBipN+nA/PfsPn+aU4l1K6qDoG/i
kwyuiWcFFlc5yE5rkAe2J0/a4+HtzNmTK4jB/4GbyI6x1UuszPlEqKE+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+wIBADANBgqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDmcAXSCVGh/02M
EqR7qD7tEus6BF/BCNwf7b0bQB/rsU1E2sTB04662VZqZQDen37BvteqLNUc5CFV
6yPCCnw8mmjwB2bxqvzh3a217LU5V3FoIm417tImN+vBKEHo28CbtLwIMbf4RqmQ
71/OfalbBpERDq3Ba0eLVBPnU925G2JDWiQy4mTwsE0BQxmUpSxpd8XwYrMmUa5o
tGXn/cp+v35vpWQIO7FNlgtG3r5rf9CRoLcj2bbKA+5u0cUkHk/n6zxuhE5IqbU
4HWCwujDx4X1Ls61wYZ6ihkmIlRAJHXg1pTlsjJ8oRlXZhK1fB302gQknZ9FREgr
7xifCUHdAgMBAECggEABcQg1fTtieZ+0/aNdU149NK0qx97GLTBjIguQEDDBVFK
2lu4PhBg9AdgAUqLH1PE+eq65JaGZwvFH8X1Ms2AKiRzYsPOQIoJ4n1hc69uiEN9
Ykcv4QH0vvqtCtWyjJyb5By9WPeLH6QynJ6FlBoSqxhURSwyYfTuwqt10HEhsUuH
d3N5BmbFiRBNj4aIA9zz+i5xL0m33kMKai/Ajj3sI0AJsZ5ZVAhYbC8sCt1Xevb6
i41p9S6GSwGC19by+1y9WC1QGtb5GDotvChMvmZS/03NeDc6xC/LZoQcHNvgiZd7
f1g6iEkJlCYK+D7xsd7Y630w75Haj0vnlhiJ0bSA+wKBgQDxv8jp2D6IVRGgYfaC
nUU3Mg70wagX1fgPH09Sk6e9c8Cg0Rh2uWwjpTawu88xBGFyZ+xnWqr7GCNsItas
3m94ri4A4R94+5uL8+o0LC26gMDfzATd1Q3k/h919YLk89tonQEUBCFZJdphThEb
vg2W+nNsEVCQGuClzhX0AyGMswKBgQD0BYk3sdGQbBA/hYD1EYsZfYebUiYv2lTt
VGRgTohKFc1RAW0tGP9YRbKyEVkBLhjgkXzS9xGqKywP71z9Iny+zDGbzk8ElB/g
lS7GFGX50TG0ISfaFWTYdxt4mN9pduZE2b1T/26uyU8DXCEBhF/OqhwQjJqKTYTT
Rl3Ara5fLwKBgQDQyVtjIyD2q8naY2D8c4mo3vHtzyc21tQzcUD8Z4vSYps1hbos
KN/48qJmRv3tjqP+o+SXasYKsFE/4pIroLxTVNNkbQm6ektfttwP01yPG8340wLk
97HVW0ig/tX6mOWg1yBsm+q9TKTrrrvm1pRGlmE6BQgSYyY4r504u3VlnYwKBgQC1
B4FvWyDhTVQHwaAfHUG3av/k+T++KSg6gVKJF1Nw1x8ZW5kvnbcJC3pAlgTnyZFyK
s5n5iwI1VZEtdbKt1kqKCp8tqAV9p9AYWQKrgzxUJs0uUwCzc+X3aWEf87IIPNE
iQKfXiZaQuZ23T2tKvsoZz8nqg9x7U8hG3uYLV26HQBgc0J/C21yW25NwZ5FUDh
PsQmVH7+YydJaLzHS/c7Pr0gQFRMdejvAku/eYJbKbUv7qsJFIG4i/IG0CfVmu/B
ax5fbfYZtoB/0zxWaLkIEStVwaKrSKRdTrNzTA0reeJKsY4RNp6rvmpgojbmIGA1
Tg8Mup0xQ8F4d28rtUeynHxzoDsw0YQKKwYBBAGSCBIIATERMCKGCWCGSAAFlAwQC
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 [\[SHA256\]](#) 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+WwNeG1DANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGx1IEExBTVBTIFJTQSBZDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAqFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowODENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFmgV0cxFDASBgNVBAMTC0JvYiBCYWJiYWdlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtHAlBNMiBIk8iJqWHk/yDoFwwj8P9Z1uYdq1aqIuofvjoAyjdA8TbsBRGdmvaIOSQ0epsNjW1ko7lE8HlDs9JHn1E+tzH3mKfn+G2erY+alkMJTXPvMAudCA8+e10J7k91gYXDpzIWrP3Kc0xTlsJ8tGJ6mhydJX3wP0/HuyHpfKQqfDusPH8S5yidPciWuB7Wj0X4xY1pUAz2rSSAlngvhEzKFbW43BPjYXPUnRWMtXFya1djQ6Eb9M/klbhdZheDLLsjLUSXYU70r9VXGM/qcjd/NhWYphCeBcqswaM5mXLYdm0mFmqoecF62mUE0DiNdhwKTtnefd0cll+D3FQIDAQABo4GtMIGqMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBawDjAMBgpghkgBZQMCATABMBwGA1UdEQQVMB0BEWJvYkZzbWltZS5leGFtcGx1MBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQU5R0sMVMCSZxN42554CVhlT6IYiUwHwYDVR0jBBgwFoAUKTC0fAcXDKfxCSHlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAC2cY8FgaxGB+Dx9gAFj35ae1vgzYiWI3Ax3FSxogo/GzpK//LB4215oeBuKXbm0ixBn4nojd7Pm1M0i+ilAvVNJNaHY9TtgIgq8V/C0C7vL8SdBN01e5ZRI764ohu9ivYvIxvvt7gzvSTpe+NUT1i09xNgsC8v19WB/BwkqMAgDqMxqCxt4fyrVvWpxNBke75jE6Q3xCjfdOWYcfMLK7EsTSgimYuonZjN7v/yqTdjn/iVH+agL/2MlSfiU36w/Yf17EM09uKGH/Javh+2Vjd0j8rE/q2Iaac5VI91M6xz5oDZUknycBKKinR+nJWmt5AKUAaL2Mjl3YtrUGBpxxY=

-----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/AIBADANBgqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQCq0cCUE0yIEiTy
ImrAeT/IOgVbCPw/1nW5h2rVqoi6h++OgDKN0DxNuWFEZ2a9og5JA56mw2NbWSju
UTweU0z0kefUT63MfeYp+f4bZ6tj5qWQw1Nc+8wBR0IDz57U4nuT3WBhcOnMhas/
cpzTF0Wwny0YnqaHJ0lffa/T8e7Ie18pBB806w8fxLnKJ09yJa4HtaPRfjFjw1QD
PatJICwca+ETMoVtbjce+Nhc9SdFYy1cXJrV20roRv0z+SVuF1mF4MsuyMtRjdHT
vSv1VcYz+pyN382FZimEJ4FyqzBozmZcth2bSYWaqh5wXraZQTQ0I12HAp02d593
RyWX4PcVAgMBAECggEAEvPt6aAQjEJzHfiKnqt1U7p4UKb5Ef4yFrE7PdTLkeK2
RjncIhb6MeevVs8g06co7Zn8tuUT95U3c0XLhV0WTvaHYeurTXaknICz3Ie0oS18
skiVZko70uJ8pR6asWUlr/z0j1EwZ7RnEUwet97oM0YeA07LDFDKF7eUq//6bfzT
ewr/QfDDsv+erwJBh+9CRH0JyTuDH1WeGxYV8VK3M6VhdTjFxxFhrQ4pBe5J/UA
17Bd2GM8Urg6VYzVo6x4ajnc1H/ezYldc459poTffv6Fg2trqFVAj2IrQlAeqjda
lemsa6Np801mUGknq3fjKS13RYGBv/48rCHOT8eRgQKBgQDM5TuS4ANQj0Yo0gtF
xoVjbVlnd0o+SmdFkZihzQHxcblY9HXe5H1bLf1IMXz/nERx1+SmYuuJk0EdiM9r
HOCcHRLfBmC7t0GdVvLDHSAX8Ec47LbtKZqyM1U9dn7Z+5q4iywqpaP8pP3+oY57
cgtQax1jle3xhRAj65c11RBmQQKBgQDVBqK6wKDFsdZuMZGUtOY0rtamBDCgEU6
rEqBAyCPY5NpF1pomUFcYKWT/wbReFqtuyq20yiATB0yHHMko46BUTN7qX/m/skt
DHWXVws1+G4IgEMVokM9jjrkgdY5grrJ68sagKC+bgv35BizHPIqqQu06qnPSrM9
bevwbQEj1QKBgQCiPE/zeBSnzyjeaTdLxGkR1R+ZX2WqdNdYqnQkiWMkf1aSmt5J
4raEj+GhLC5BZsZ6+z480M6XXFW0wSkbMv5WH1824KHvgKcfoh00iR1EVyjN1gDx
wk0QvjycMhs3FpXn0arjCczS2wGSgPGEpUR4JJhcfaf6kphZsWDWzV1AQKBgQC2
ivbKltNhj4w2q1m7EGC3F5bz15j0I1QTKQXYbspM8zwz6KuFR3+1+Wvlt30ncJ9u
d0XFU7gCdBeMotTBA7uBVUxZ0tKQyl9bTorNU1wNn1zNnJbETDLi1WH9zCdkrTIC
PtFK67WQ6yMFdWzC1gEy5YjzRjbTe/rukbp5weH1uQKBgQC+WfachEmQ3NcxSjBR
kUxCcida8REewWh4AlDU8U0gFcFxF6YwQI8I7ujtnCK2RKTECG9HCyaDXgMwfArV
zf17a9xDJL2LQKrJ9ATeSo34o9zIkpbJL0NCHHoc0qYdHU+V02ZE4Gu8DKk3siVH
XAaJ/RJSEqAIM0gwfGuH0hhto6A7MDkGCisGAQQBkggSCAExKzApBg1ghkgBZQME
AgIEHJjImYzS1Ykp6InjQZ87/Q7f4KyhXaMGDe34oeg=
-----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 [\[SHA256\]](#) digest of the string draft-lamps-sample-certs-keygen.bob.encrypt.seed.

5.5. PKCS12 Object for Bob

This PKCS12 ([\[RFC7292\]](#)) object contains the same information as presented in [Section 5.1](#), [Section 5.2](#), [Section 5.3](#), [Section 5.4](#), and [Section 3.3](#).

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

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

MIIYGAIBAZCCF7AGCSqGSib3DQEHAaCCF6EEghedMIIxmTCCBIcGCSqGSib3DQEH
BqCCBHgwggR0AgEAMIEbQYJKoZIhvcNAQcBMBwGCiqGSib3DQEMAQMwDgQIe/d6
qDQ/28QCAhQGgIEQJKA5kzRVm9d6rEwC/0RyBSgpPuSROUQTjspt6EhBZlgHc3u
FTCPa05P/vpeWaCnBRarGFn3DmqA3JT+59bmRpGdiP3ZrIk2EbHi0yrd2P3UFDnX
qRkKI+7pf6e0HWJRntJA+KJS8v3tZ/hpiEKAeav/Mq0IFNFyEiZpCkbKCX5auDb1
p5c3J2MNg/WNBfpGJUHKVIZuIF3H+8LfFgayRsDspPoUMffR+GmdL8nxLiqhraHD
+Iqr3LpEroNi/iZQWUTFTUlaePf/2KMqaH0uy41IVvcH1jIcLXHGNaa66S8AP/Hj2
TJPPg/lve76DvaGdEnx4QJd4pBFQac90zmhxU1HZrvzubK9t4e5lr80wpd2djvZK
wSLzUgtQZXq8pSs1r85vrb3KItDYGF6SZpX029FS7rY3uYth5SYVUQWdUYYY3S0/
nsaLg4MCWU04Sh7nYJZL5Ijkk9LS7JhmwKvizHRRTXbLyRDH06e+jCRgLCu2WSUq
1bEr9Jy0ucK8zNPTf8HwBTS0ubvy4Jf03mVp4REX/8ozXlLztwGblFGbyaJ9Y4ga
LM3JpKxMtb1UTxoAyj3iFwG1GZFGKBlwPlr+0dkKkC4dloFE22IINfLdRNLV9mPO
aGZhsDheB8iV0tN01u91BLU68Q7AL1ryXWUSjouKGRSU6uMDLZ7rw0wLZC1m4oLG
BF8cm04ELmb0ci78fBs/qDXlf3BJazcNtciamEsQPYRGkHASBRYtoDfVvy6mTT40o
obdrZigcvCwttdBu7RtynAQVZ8DvKzxFGhe2p2Yc9H5A5ML7IwqNtYzheduBAQTE
jAU2jMqwnZN5wULEnH2TF6KAQNrKdtBYMbqkToKgx5Zf+cJZbyQq7WM6nVfOM7g
kcFdeHDn/CwoSNH1+JA3wSDM06zkU5HMD2MpT1RLTSaemImUKCAGYieJmwNQxR9
aYHBBw5BNBw1XRB7WRka2Uah0Xq/wAgAI/o9L+mShDRFJjFi+t8AV3KR0WWHg020
9qchX7P5H3Sy/tq8yUQIo1+hRiRjkfi9qy6AxIRttrK4WbW4scUtBZSk9uFkTVU
ybnV6WvBpn2SrnwF/E1ueKARVmouWJ/7fiLJXk6wVvVtuBZW2gE5QGfuCwq0PQsC
xPx8MhN11KZYDVCgsyUr/LMHeKNC31S2HLGQK7kh/o+QQazafiJocQ+kRbS1VX1D
nQlIhz4zvKsBgzhpoe3wQcfAY5sp2ubepsZ5T/YHkmroBmvA4g1vi7nlCetgxXrh
2V60XvaZ+BnfsYxJeUZGnNMNEDFlzS7xB18ojtT5JN0o+9tLsdikdikl69IsVv+2
eCv9Go+wh19cSAL24rkzdKVuiIAXS7tzel3eWgjdKoq3Ke+tfJtobSGrB39xgLVr
3ho63hd+qTUyjcAhVL3hAJinv+/KT0jR8fq+CDsXMnCEWugHhwB+66N0r876MIIe
bwYJKoZIhvcNAQcGoIIeYDCCBFwCAQAawggRVBqkqhkiG9w0BBwEwHAYKKoZIhvcN
AQwBAZA0BAjiGuDSkfg4UwICFLWAggQogyL08hPtU152dk0+BVimcGXW3FmDrT0D
gU3Drd0P76KzYzd2lLuGb9dx84wx0XnFIXeBM4F3QSDbCK4tOuJ6JRaEeUoCAyZd
XyHtLjVeuozt2xHBDUGQVE01dZHtk1VUgzLSCha1rXjcwpa4+8xqqoVM3C15uBh6
QLUNey8Z3YlKlk018Tdge600Urg72BPKppNfJlN4Tn0FwMVMA/qHAJl4pL1YDpmc
5BZm4tMg0HvPiz96uwjEhw1GZFG0gZIogeVJuqCniZPDjCFEDgnCw6sciS5Bi+dX
Km0VUdamSr93e2eEPLbzxZR0E0A3Ic0j66iHuZpU9YhKzsAIhLMxT8kF81I0ZZzj
8N+P1hmkjdVWuJLg77pKXxQJyvuT0e2oc9r/DCHjckneen3+E66IKsYbib7sX4g6
2oFBJs+7xQopy69pC8jCn3fx61t7AFx2RivuVHY/eU4sXowkJNqQ3Vxj2SPWkjzJ
4IivWvXiFiQjj0tDFdGYPGukJXn62Lbb8CFgam9s4jDKnr0LHIngVeUIgi4wkvva
QzZTzXfUApezQgQy4x+ogdiYF1U0a00aqvrGRiiJlMdRi0/MDy+jzkX5cULhxkF
vdBNCirv+3zBaiJ5Eu6q0zP5Cxi2qXhSbehZqvTPB4dD/vu9yxHpZmUCvzm7H213
Tdrb9WxH0c92ZpBzsfICA1smVwTDFVGa/kqN6noPw0qWZANIk27/+apsTkBYaVpa
jpfn9eydi5eV2+pEQV08fh40JfIKbHS0l2E3Gp/rPm9lVgmCmjBWh+Di1k4qgF/f
lsxwGzXN0xPntpohnM6AZDxw9Sk+BE1DLYS4WFWUg679BsJG6hQqAZKvG/8agSH2
k+TKKYUbXbFVCB0+iuNZIwgf4qxGzvI5+Iok+0cxuGCqw0u30QbfECEG01QbKETn
ic3kMiZ5Cxt7NQsuyEYAQ/AmvM4qo0x7Tw1r7tR8BcAEF6fGxd2VXIV8Tr/pXG02
HL+0iIHs+0b67z1LThr7wUB4tCp9LC3IIWdsr7KcSRNEMXpUIFI0etCjNgCU3iT+R
9152150fWNGxQfaXTEyMVNaT1HpwiHiisSb9QHbagaRLbYmqJ+ILSECADYQPEWf+
LT01tc0hkIb6BiwVWUu00qNj6ILJM2XvmknATyUj9MYcd77x0JzMrJE5VtaM5BVT
oRpcOLfhY0mihceGSEqXX5golKqfLUze7zls1NWMYTTLw6tC6I+c/IUIWJnZT4m2
RbTQ0krfPn94zbTjrG42HS5+Ke3ySV6Fv8MZ+s93yY1v9iB6cVPEuteLRc+C7e7t
lw0bQ2+MyAkjenS5Td+3tC7lR4202CSfy2Sa0sRv+EaYjTGzf9F3TM706o5+VZrM

gtIKtw2okRcjRhaKDFhui6jo46YYZwbrg0S3vzc60VcwggNnBgkqhkiG9w0BBwag
ggNYMIIDVAIBADCCA00GCSqGSib3DQEHAAtCBgoqhkiG9w0BDAEDMA4ECEyHXPVs
ncxTAgIUQ4CCAYDSB1YeFnsa4vtKApbLnd9FENDYeYqKmj0lkDagMqHC22/nQ9v
gz2l0o5FQJoaJx/WSorQt0Jny1QP9vZd2t+bkfoaXOR0MtmFY5S0tYEudJp1rCz+
ZEw8JlePJRP0Q3lnwEiSk5NnXLRWNzurIeuyZEd1VbTvi/rF22sRWlmU335L67zj
P1sPeXkBpIYCPLHw8E4rkaC8G1ko5wyrnhuqL4Itzhv00RvgRaDflpP9WTj9LVUv
FD5D59zgb0ptaW0jIw4JplIGXIEZIynW4KfkWy2YJvsXiuLHVn3Z8qL6VtxNGk1s
g340uKkUULzmtDJqGT9RVkoYBXnN7KYesbStt0NhPwDv/MxHrEo8TGHZAvbmwgft
h0Urc/WvtUopPEs4QgrsA8d0MrSd5lVtPW0XPSBPEnLuh7dqAlmgztYlP4YztK2/
JJ+E4MosmhRjbKzM2N5WuG1DC5m9KF/5JjNVwQ7e8gMeUv/3gizgCG/4Mng0VGG
IxGzzBoQXPWCKdT3sLQVyt4/pqPBpZYnPO9bmkkY/UIa1unNB+WWpLokKSzD5wRv
/2xmN02D37DnHwTFYC51ZblKz7FGj0gCwG95VPc8NQ8aG5rqpQ+muq/Jil5mXgNw
IDeM4bawa01UKEzqTGQub3gsJMGiV0hgtOrBi09Kx/2PJo1UuwZGcho4oGSVR7KH
lLgIuC8aIQdyFURVYRCNw0w5U7JN5arkvZ4ty0/qk5UbjxQuDkF8o6ZdVi03l0Do
C+6zvncDx4HvUd6u+u/kZfr8qfW5o6D2qXhS/ZHskq2xwIzb47uUUqaeg3y0ZJ
++na7gC+ibtHXNnSHUvPbpCn9qViFhzilcQZYq0tZxDKa0E/pzEP/IA4IG24wEL
GnyuUIHXS9T0MchTx17BglycOPRDNfKzMQfUXY1rAErK76cs3y4VQDbfYDi0zsa
1qqMApIX4i/qKfDrVduLxtZQbVA/rNumm40LPUQ50vEngIESA74G+/YQbvjbMjP
y+hm7/15q5LR09YxCS49KG1z4NG1QMwjnfkpOCNVZVpaQ7TPG0IYZBL6kTCCBZgG
CSqGSib3DQEHAaCCBYkEggWFMIIIfgTCCBX0GCYqGSib3DQEMCGECOIIFLjCCBSow
HAYKKoZIhvcNAQwBAZA0BAi0/0ICbTbZLQICF0wEggUIFwT/JI8UjJQPfYTFonJE
o8zEbpYWXkboqw6/zZsMGmAnUPgQNQDxyuLVprs5jUc437kVB2M3F0x8DjmEppeb
tHfIoyjoXF7jdnA4EF38tsso0K1nMPmSgl02iYZt0qs0vBpfe05Hj40vhi26J9Pz
TwPcgl3QQPqfWv7CwgGVn4/hntBArIPSE4gAlfAcqkxtJBm01QwDoAds0K0MsYnt
gWajpr1J3Hm+34NPL04Usf10pcesPUJ4CBxNyLXxjjs0zD78WVvKY+N+j89xTsyt
z5Y0fEkFqrc18pgBQxH72jBwSCm5YwHz3BhwQgr2bpWJ1f2LWcVsnrN9tx6RhQtA
AkcyNgX/ksp5EW4JTo+o6oXLRhXIYauRrUrisMY++b8ZJTp6C1t0RW2QdggMZghS
ZgaW6FSC6Dy2Dd/ezdkYUCgiEtq8eSxF/8WDw6Va2iGVSnt4/p/0J97yN5y0J0K1
g0hATebU+I3E74PQ9RK84FfJvyHDBC6fvYZW/ouMcgp3YmAF+dTm74Hq88X4daV+
/UPYf/cVpyiwcBTg6H3jrkrsoyKowLIfrIvMNBeeKZ+fl2Enw1MFzKLI4VGD/UeR
wrhbN0SHkh5lIGtu0yRTfq6msYQpkw+jr7QwJIdQyrAaaaVaRotVyvgTOLlHw8r6
o7v36yoNov3kDPW7DfbSVTWX5lIyQn8NqMwa4N1clWT8ukfZXSAyYkFSqF3w5za1
a4iIhu03GjDcfiWLMU1YVAUcvSmcIULE1ow7FKiJc80adeIu0JBYSRSEvf7B3w8l
eYUs+u/h1ptrZZKhe1JdAtlszvHJ0DD0kMqA6Ig4yomscGSol/sRUqpecIQwVZTC
RRq9dJ0fJkKhKD5Eo9E0Z2snp01fpuF5qlMeBjpYgkX7jhyFyvq+qDqBAY8izvkc
ruE69WooBVyorqKHURjWtY+rhzcB4+HL72wZKzLnY3iUjJ1UANxM8mC9fpD1NJt/
7epqzPyZ2Kd4GJVYi8sQpFKf4tRHDROT5iUB78qj1EBp1w4qvRn/jc4ii7+Bas8
mz/AJ25Qevic44Vj+eT2YXafDivrmoeBuVMIBbD066YnuBC2CeKydNWdiARzc3I
fhcuHvWq7riotYfyDqd4e0Jy7Y57pbwv4Qwz1yCxRjSwiFQ7/fRa2Cx8xtxKcC/A
4LGnXAKISy+uNbDWA7AYaP6RmGgMCaNiXy3F1zvxnE3bv68tXRF9vjuEChUq56N6
992qhoBuHP0J/mRitw+JoI4m/0FnEUGT3bNyxpEFyA7aXBE91aQdSX14a97nc0/R
SFH/fRWPFYgxR3XdcIf3Cw5PDs25YnsXWcsDCVeJWMFrw0zmDwa8sBKY270+rGv7
6qXvb/uGD3M2C+DySVy55Zd42wjghSezgY6taT0tqKfLOS6V14ELU78Q6va2o8M1
cUdi343t0i60MZgCDUwPP8TjKZINh8u1KNhZgpwNLz1gE0dd200l3bbzdZ6uio3R
52WQWRck17Z9lUesCJavytcAi0mMefMxBPM0dnUi608TPDRA0mcohBE5rybwDXAo
B/VUBwgM0/qCpZ7VcSKN1lUuoE9+Kho0NK/gyMEvntMxGNNI8arV8UkeFollPhrt
umvdwqbVCeN8TBJ5vXo6Hu+eKB7AVwjBk/rRHpZxnnVGXbm8HzM+kjib2cY1dius
VRJ/1+Q9GXuo135tQbobgcMzAmqAqZp9kDE8MBUGCSqGSib3DQEJFDEIHgYAYgBv
AGIwIwYJKoZIhvcNAQkVMRYEFEqzrDFTAKmcTeNueeAlYZU+iGI1MIIFKAYJKoZI

hvcNAQcBoIIFgQSCBX0wggV5MIIFdQYLKoZIHvcNAQwKAQKgggUmMIIFIjAcBgoq
hkiG9w0BDAEDMA4ECCNi2K1bMEiBAgiUdgSCBQDLIXo4ExcyE8+4aiZIJ/Wnh/SV
VVR0n7s4PGCbXt+VrOHd9YzTuUicAqIcHH62dv7NSy+fgqZG7SmVR1IodadFe+5u
sAzXoyyhhEe2c+ToeVbr5rs+vBvQUyh6X5XTV5QV0AkWsyKGjyfdy86x1Q8cL2D2
BM+Rpkm1cFtjgWcB46U6S6w50sG7X0KSCMI4a6rnHPVgPPdXMrj3VSPJY8bhBqED
PVTnfSHf/wKZrIi5403F33B5jt6Cm9+9m9Fed8n+81w59rRom72CY9Xii/ULER9T
Hwjx0ZOQ+dIm123Kauwexu0Gjii0UR8MeM/A0n7UNys+bZTulgdpWW/mDhJ+eLAT
nhJw5ro/Awa6YVYG+t5k9LjdJ1ZmqS4bJxvBwilpEGoh0MM6Yp0dr1XM4mT/E0JM
WD458Ngs05CuCpwAUXGdQmqrVsFrrV0HTyHeVLDhe43J3GI6HCWJV0eDQzzma03A
M+IooRDkTHnJMaxUXphKTag5+f/smNYEhzVjZeIc8GFZ36eSI4BNGHSXFACwLu2T
hkzpXMmg50JAUhBYxqE/fVevLUH4JPLgz869wk8gRlUBo6ihQGrnsx7Z05IsYahE
Yjz0N05PVPJYMLSyMovG9i+LpzQ49gIBzPu2fdLR41u5n505mG1Y4aJ70CJxMORY
hWHuctHdGdpJsgiq8+1iiUwmfyCfb0ZL3ePMU+W0zkAsyn22aK8jDBLLVZlv0ZIV
qR3Gx4QFPsk6qCMQ0E58VkmUMxYvClzTwSeEMu66eND/AKTE+XXV/d9bmSmWGk7Y
8XrDKLkfmRdr1IeondVJv5mk12YKxBPQGeUqK5XJUa2dzH9zvEX8iYzdt4281QC
iXJ3qwmBt+8RoOLBt4Ky0s2e2ZSZnjrL9004oUsHIOyEfjwnWoLhKbkmun8GJxoB
2yCzTawVQf9/qIUXaSzcp23AV6Lf1k90f79HYPW3cQJAtjf6XBVE1xVZPkfTuC3y
VLufljs2ed/ctpHg9nuId/xHFH7t4HbmU3/Zufe1GHnsRQ3kbnqA5WXerd9UzeoD
aVDjFXGrITp8env08GXyvwGXLL150l0DuJSv1E+1yww86SNjBYUTx0r0CJjjTk2
7vIUhAYUEA+J71IeifqqPDKYXnrCdUEajbfEdek30WiLR+ChEvEp48Mla6UVTLm/
mjziwbsxm5QlGccmz13e32RiyrseB+RyllmzeJtydP2IHkWK7pww9y0lPK0QtZs
66IGZKqeXrWBk9QFYDX42gAy/xTfglco4K07akhp3UzTIQyTXnt+0s0Scc+ArVm/
dwC1m+Zxybt0cVyadjpKWydyfAr3aTkGxX6RmHrEwr1R9BnMGPyEsDs+yeVNs1Qd
Dhff/bQLwCLXdGLWwLe6kitUiYi8F3bdfPjR7R61lEUvJrBm7YlmgdxRCJ02LFLG
n09iSMNe5vmiNaKiuzfb4Dp9dqEMhmJfdsTURagfJIYqULoe08EIIozahivbzoWV
A6oPAkk2D8DnTiMegX4IZ/Zb3LPxJKAeX03Ys1YQrNSNZ3B2ZISBapzGzhFZfRVz
P0mXhN53pDhlxkw0btkKblYA9CvP+kzgwckzCy/Mlq/Hb038CV1NKzay3yg4nteh
J+v9/k7gaqKmo3ZWMGk0WGBv/GFxYhmeNd14Y65D9TlypM/zrXSYGo0qZgSA6Hla
gogzwwSaGwx9n/o6czE8MBUGCSqGSIB3DQEJFDEIHgYAYgBvAGIwIwYJKoZIHvcN
AQKVMRYEFBfFhHvQp+92kDi4s28IvJK1niuUMF8wTzALBg1ghkgBZQMEAgMEQEA7
SD/WvuMDyvP1ipdXA2WUre12gbn4LB27Hc9hSCYJoGBNjjnqCgLnkr0GYn3c0JQa
BlUu13AJnVU2Ep4R+DwECJ1vqXe6ro0FAGIoAA==
-----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-----

```
MIIBtzCCAwmgAwIBAgITH59R65FuWGNFHoyc0N3iWesrXzAFBgMrZXAwWTENMAsg
A1UEChMESUVURjERMA8GA1UECzMITEFNuFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcjYXRpb24gQXV0aG9yaXR5MCAXDTIwMTIxNTIx
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-----

```
MC4CAQAwBQYDK2VwBCIEIAt889xRDvxNT8ak53T7tzKuSn6CQDe8fIdjrCiSFRcp
```

-----END PRIVATE KEY-----

This secret key is the [[SHA256](#)] digest of the ASCII string draft-lamps-sample-certs-keygen.ca.25519.seed.

6.3. Ed25519 Certification Authority Cross-signed Certificate

If an e-mail 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
U2FtcGx1IExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0yMDEy
MTUyMTM1NDRaGA8yMDUyMDkyNzA2NTQxOFowWTENMASGA1UEChMESUVURjERMA8G
A1UECxMITEFNuFmGv0cxNTAzBgNVBAMTLFNhbXBsZSBMQU1QUyBFZDI1NTE5IENl
cnRpZm1jYXRpb24gQXV0aG9yaXR5MCoBQYDK2VwAyEAhIFGfciP65F//Ng4oas1
SGUGfkShN1Ecqfnjdk8SQwSjFDB6MA8GA1UdEwEB/wQFMAMBAf8wFwYDVR0gBBaw
DjAMBGpghkgBZQMCATACMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUa6KVfboU
m+QtBNEHpNGC5C5rjLUwHwYDVR0jBBgwFoAUKTCOfAcXDKfxCSHlNhpnHGh29Fkw
DQYJKoZIhvcNAQELBQADggEBAGV0x00EzgyLRKixMcztiiKxxJDbmRat1pcipD15
1n8kiBoGhst4fNZJVoL00QBa/WTMntL+qcAk2itqZCNIEZeGklUlJXBAz5tkDRAF
f/v99LEcsZTcuIbnJqz35danQkp4/upG4hPkfx+nbc1bsVylrITwIGOpnGhz7z3m
VCK03DFE3Qt4w9mlv9yuMse33nmsBGXog/XZvM2JRY0iKt0xksQQD9uYm7MoMeH
qQs30t7EaoPj54xyWvy42run6TLUye64D94SNjB/q/wjL96bsVIKGrRn10T1ybCh
4F5HD00hQZgP15Dlb1rg+vskN8MSk5nuD+6z1VsugioW0+k=

-----END CERTIFICATE-----

7. Carlos's Sample Certificates

Carlos has the following information:

*Name: Carlos Turing

*E-mail 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-----

MIICBzCCAAbmgAwIBAgITP14fVCTRtAFDeA9zwYoXhR521jAFBgMrZXAwWTENMASG
A1UEChMESUVURjERMA8GA1UECxMITEFNuFmGv0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnRpZm1jYXRpb24gQXV0aG9yaXR5MCoBQYDK2VwAyEAhIFGfciP65F//Ng4oas1
SGUGfkShN1Ecqfnjdk8SQwSjFDB6MA8GA1UdEwEB/wQFMAMBAf8wFwYDVR0gBBaw
DjAMBGpghkgBZQMCATABMB8GA1UdEQQYMBaBFGNhcmxvc0Bz
bWltZS5leGFtcGx1MBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIG
wDAdBgNVHQ4EFgQUZIXj05wdWs3mC7oafwi+xJzMhD8wHwYDVR0jBBgwFoAUa6KV
fboUm+QtBNEHpNGC5C5rjLUwBQYDK2VwA0EAwVGQWbdy6FQIPtFsaWVG2/US2fnS
6B+BzgCrkGQKWX1WgKtj4ME0qL+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 [[SHA256](#)] 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 ECDH with HKDF using SHA-256; uses AES-128 key wrap, as indicated in [[RFC8418](#)].

```
-----BEGIN CERTIFICATE-----
MIICNDCCAeagAwIBAgITfz0Bv+b10MAT79aCh3arViNvhDAFBgMrZXAwWTENMA5G
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnpZmljYXRpb24gQXV0aG9yaXR5MCAXDTEwMTIxNTIx
MzU0NFoYDzIwNTIxMjE1MjEzNTQ0WjA6MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzEwMBQGA1UEAxMNQ2FybG93IFR1cm1uZzAqMAUGAyt1bgMhAC5o
MczTIMiddTUYTc/WymEqXw8hZm1QbIz2xX2gFDx0o4HdMIHaMCsGCSqGSIb3DQeJ
DwQeMBwwGgYLKoZIhvcNAQkQAQMwCwYJYIZIAWUDBAEFMAwGA1UdEwEB/wQCMAAw
FwYDVROgBBAwDjAMBgpghkgBZQMCATABMB8GA1UdEQQYMBaBFGNhcmxvc0BzbWlt
ZS5leGFtcGx1BMGA1UdJQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIDCDAd
BgNVHQ4EFgQUgSmg+i0gSyCMDXgA3u3aFss0JbkWwYDVROjBBgwFoAUa6KVfboU
m+QtBNEHpNGC5C5rjLUwBQYDK2VwA0EAzss75UzFuADPfd4hQdo5jyAQ3GvkyyvI
BdBGNWtJ1eT1WuMaIMhi1rH4vPGPd9scwW+sqd9fG+pv3MSh1+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 [[SHA256](#)] digest of the ASCII string draft-lamps-sample-certs-keygen.carlos.decrypt.25519.seed.

7.5. PKCS12 Object for Carlos

This PKCS12 ([\[RFC7292\]](#)) object contains the same information as presented in [Section 7.1](#), [Section 7.2](#), [Section 7.3](#), [Section 7.4](#), and [Section 6.3](#).

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

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

MIIK/gIBAZCCCPYGCsSqGSib3DQEHAAcCCcCocEggqDMIIfzCCAvCGCSqGSib3DQEH
BqCCAUGwggLkAgEAMIIC3QYJKoZIHvCNAQcBMBWGCiqGSib3DQEMAQMwDgQIwS3R
pT1mkyMCAhS7gIICsGKkBM0nci9VHfQx0TWy/lkKyQeF5bwsF/9gZrqUym1KtHZF
a4rSJIPUctmzqVnhGmfW9m+LEi7Em9rRmUIQbDZt4kQDG5eDk7AdhyDnB3uZDG1W
4cAeUVXJMzGfnwtzy5TzBZZEo5nnVX74Al+PDW9wdpbv2TiriL0m29fBT+7HVS9F
Z/95XokSwbb6mmCYeGiPpNEaoeUeuU4zrh/k+JJqDuqNsU66I30wH0CFmk3aarBV
3LkEeCjKFkngzM0ZqiKZu8D2hEUjsGQ9ALsRn7P+hIWNFIgJvqgcCMTF8fLK1C/8
vYGD+H0pnn23nLele4b/qpFYx5kJ0b0K1Zo1SpGUQ7Bu6gectUcey0gi7CjRScuV
ew7918ZY0ugyYoIWA0kecPM0TFtxAn19JPXo4jBYAlwUtX7GYAlDkgZCb/0dbkv
4L+PAeJK4kVDREDQ6ch/6/hlqU8xHeNzdagEwYL6FxDiHebASxIvZzqkLd7RV9m
dL1FXst9R9G74j0s0WMMFmd9toy0hD0q6G19cat0rolCVS/CKaC0CucsJfiKrlJ/
duQkt/JwcELveU0g60u2uaGKUqHmFhd3+6omk+wNB0Y+0D5MmBZ/xnrVELGmzp94
q0f/HfZPT6sxkYBGUP2eUA/qR/zimNG3TuGvch/MdnduuVhvAYLyh1gbA8yRm+I/
zGCVuAqhsHITTx7Fqc3tyVp/mLYU00QuwmgAw6NhzwKZf5N+tR0DZGcgw8rZpeJA
yTxVFcjzXvoShxog7RrOR9Nc4FwJhWI4B02410HFEiQZeRk8vzI8WIFXnn6t42/q
j1mV7Ba42zxPEGoY3mObKwJR6rDp6KwmmfkgHPwMPU3qP2/ASV8WT1+9GIYHc5Am
9Cms0TiQmluW70Ra2k5ZMLwnbKNyMRbjUB/yHwwwggKvBgkqhkiG9w0BBWagggKg
MIICnAIBADCCApUGCSqGSib3DQEHATAcBgoqhkiG9w0BDAEDMA4ECOMzXMste/8a
AgIUlICCAmGXA+q2JhTLvWsj5SKLdMninTk5uB6Hh0sDKYR9GDg/cABQUFYxcR0G
JeJueWIRkJhsfdXJi+TSRtnQ0qpyVM9oRUdxcBGuCI98fEbLmVyr7KF8GudTgC+b
eaLjn6HYkwPv7lWdvsFG8BEy6Jqi3/tP9PgNvpCYgVVM7yx6SX8QArcLSQkxbTsv
Ae0iN18H89W9xOHEz4Z2qHYyb7f0pPHrmpTGC6qmtvo1gNRsKTF0wYeQ5Sy/9U3f
oM6bIcr0vHDKsaco4+5n0zeySDETY8W4m01K0uC/t0oT0ScYGBerhVr0DQapZGT/
Ej5LpgjX0uosAoT3IKnMwK3C00Z8oBzcvgSpeAa/V/OTKDPzb22yq6sEaHAPoUqb
cKRJmB6HC5mdLs3n0uP1vLzuYsHu7Evt0UhnS9pbklJDiCgM+4SFgKTRbd6Xt8bf
GHkwnmpv4pQL7jjzA3epP2DHyC8MJaDvleWY7Z3t/IetkzVxf1Lo8kT21edz12cm
uFVK9ilMW3eJuyiRyFXFPgVsuNi/HFniJXFgxzAncP7fFP5MCs0o6daiEjJjemKf
J3D+Hdd60gFih/ex9V+tG14y7/jtxCRA/54mit4sCy3LC0++lEp9AtFwGYrDw825
uGj27a7mE26qgGdGXdzT9UJ8fUsIoRPrG38Q4mhS10pTarNucWOGjkftZiKJLay
rFMRf3HYx0I/7iupfXyLK/4/F0DijaHzAfSdQf2Bo7csPaz2HQkK/0ny0+tt68S9
pUCjEfV6Liy22tang/jXxPFbBDK/P68MnmGR8C3PcYhPJCo/K0JR2/8F8pVVEqd5
MIIDPwYJKoZIHvCNAQcGoIIDMDCCAYwCAQAwggMlBgkqhkiG9w0BBWewHAYKKoZI
hvcNAQwBAZA0BAHo9g0tQyYTvwICFIGAgGL43SpNCoshZX3ikmK1m0IJs2Ah8Xv
94S/5NA8kwHtanXpLrjYr3CyRL93USm55uvGAtECR/Eb1ON9zeo2p0gK2JPSbDr6
/1oovo7UoZNRoRBZ8pUegVWJswNWjqvzVu5JIRmpD05XjVDKHBfqiXAqtj9/w3q0
Qq/p/M9UrLWD93hyLNdIppwr2KR2it9mASTKEHX9dqXcTOG0Kp2GmrfGNteGL02j
qVKZaZyYI8gkSxhVLS9zzgf10ynAkzYQsoo+GKhDAW1fJECemAyPc3L+eeARw/SY
q1d5QVwxKfYpIJ2wiiavdeRVNBwiwV7Ti+P9PtPx/hV22NNLwMhvnJcHaSS1Pa0i
SjoxFJ1EJWGES0QwcdwM8iN3oVuqT5HU/edMgx9TLNTiE1g2GEq59I/RwBtCL8Dh
OzKnUb4PU1Z81+HimV3KPI8g3cduhYaBR4HfqAhMnc+w5HXI6J3C1NtAE/izZ1Y2
Od7l+GTJfjPgZiY0hjQfbMt8uU9D9aPr2XjN0WoKRSojae16v8bLx+dFn6RMxFUS
g3nLEZ6EDpyrJfpgPm6mPgZKSxtvnHuFcbS+utkRuVatqu07r2XpkGBIJLNVIRHU
5gLACbTj9TPcAce6RLoaYSDg0uFK0YZMdwzhsAI0YMpyHsUEZpQ5tjWSBY6ENbvF
7+QhmDnf6N3Bj+vxUtGS40pVsYCGbm0D7UM5QpUxIgVkpPrfRok0Zs/fi9sw+xy6
eQ2Brbn3t9C2TAs0RYzFbuBwuTCqFW/rXHS6iffJpx2eAg3DCqaUAJjptSV/yzj4
vxiX1DB3fMRcpNd5Je7DoHS4axuj7SLHdpNoUHs+qQsG6yDM5BEuXWGxo/L9sGhe
XQrUnkZ4m4g01sfgT0FDNurXx/oP0ym+B50q6nLUWv0tYZpmCVil358dIEGPPSMY
AMXh05tIPFdYSJ3WLS0cxy5X4sXZ15w16Pzeb9SF5topqRUB5PDTfVr2bQUMwTbp

```
99Fc0Qf6cg8HXyT+8b4qKp9WyjCBxAYJKoZIhvcNAQcBoIG2BIGzMIGwMIGtBgsq
hkiG9w0BDAoBAqBaMFgwHAYKKoZIhvcNAQwBAzA0BAgNhF0DEdzSrQICFF0EOCEq
Fie1peicS9OSXNQjLwbN3k08lYM2HqeSZoEKJ4JSF1V1kWW3xwfu5aZKrGEYBfGM
d8renRijMUIwGwYJKoZIhvcNAQkUMQ4eDABjAGEAcgBsAG8AczAjBgkqhkiG9w0B
CRUxFgQUgSmg+iOgSyCMDXgA3u3aFss0JbkwgcQGCSqGSIB3DQEHAaCBtgSBszCB
sDCBrQYLKoZIhvcNAQwKAQKgWjBYMBwGciqGSIB3DQEMAQMwDgQINFcqIEMfd9UC
AhS1BDgZruEsSaBY+Cm9WKR8HhH3JXh+AoMSrwdCKytWt+MNIXB0jY2QZHDn3u
Fn7qHw06MDthnKniazFCMBsGCSqGSIB3DQEFDE0HgwAYwBhAHIAbABVAHMwIwYJ
KoZIhvcNAQkVMRYEFGSF4zucHvRn5gu6Gn8IvsSczIQ/MF8wTzALBg1ghkgBZQME
AgMEQBHyJX30Kcho7aA/NqWHVbHwPGEYx1yP5T+GbVI3dnmpHwBqcN680Fozv+H9
j3+ocgkzQE1+n7B9euUKdG8Xw/YECJDjaZkfy4FnAgIoAA==
-----END PKCS12-----
```

8. Dana's Sample Certificates

Dana has the following information:

*Name: Dana Hopper

*E-mail 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+hVtn8pQZviAmPmBXzWfnjAFBgMrZXAwWTENMASG
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlc3R5bWV0eG9yaXR5MCAXDTIwMTIxNTIx
MzU0NFoYDzIwNTIxMjE1MjEzNTQ0WjA4M0Q0wCwYDVQQKEWJRVRGMREwDwYDVQQQL
EwhMQU1QUyBXRzEUMBIGA1UEAxMLRGFuYSBib3BwZXIwKjAFBgMrZXADIQCy2h3h
hkaKDY67PuCuNlnnrQiHdSWYpPlgFs0if85vrq0BrjCBqzAMBGNVHRMBAf8EAjAA
MBcGA1UdIAQQMA4wDAYKIZIAWUDAgEWAtAdBgNVHREEFjAUgRJKyW5hQHNTaw1l
LmV4YW1wbGUwEwYDVROlBAwwCgYIKwYBBQUHAWQwDgYDVROPAQH/BAQDAgBAMB0G
A1UdDgQWBBRIA4bBabh4ba7e88wGsD0sVzLdljAFBgNVHSMEGDAWgBRropV9uhSb
5C0E0Qek0YLkLmuMtTAFBgMrZXADQQDpORBZitZXGYUjxnoKVLicWL5xner97it5
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+uNI5ZMbZvyT0ltwvEt13usjnUaw4N
-----END PRIVATE KEY-----
```

This secret key is the [[SHA256](#)] 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; uses AES-128 key wrap, as indicated in [[RFC8418](#)].

```
-----BEGIN CERTIFICATE-----
MIICMDCCAeKgAwIBAgITDksKNqnvpypa02gkj1IdwN7zpzAFBgMrZXAwWTENMAsG
A1UEChMESUVURjERMA8GA1UECzMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcjZm1jYXRpb24gQXV0aG9yaXR5MCAXDTEwMTIxNTIx
MzU0NFoYDzIwNTIxMjE1MjEzNTQ0WjA4M0Q0wCwYDVQQKEWRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzEUMBIGA1UEAxMLRGFuYSBib3BwZXIwKjAFBgMrZW4DIQDgMaI2
AwKU9LG8CvaRHgDSEY9d72Y8ENZemwibPugkVKOB2zCB2DArBgkqhkiG9w0BCQ8E
HjAcMBoGCyqGSIb3DQEJEAMTMAsGCWCGSFA1AwQBBTAMBgNVHRMBAf8EAjAAMBcG
A1UdIAQQMA4wDAYKYIZIAWUDAgEwATAdBgNVHREEFjAUgRJKYw5hQHNTaw1lLmV4
YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAWQwDgYDVROPAQH/BAQDAgMIMB0GA1Ud
DgQWBBSd303UBe+a7GCGvCdtB0n0WtyPpDAfBgNVHSMEGDAwBRropV9uhSb5C0E
0Qek0YlKlMuMtTAFBgMrZXADQQD6f7DCCxXzpnY3BwmrIuf/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-----
MC4CAQAwBQYDK2VuBCIEIGxZt8L7lY480Eq4gs/smQ4weDhRNM1YHG21StivPfz3
-----END PRIVATE KEY-----
```

This seed is the [[SHA256](#)] digest of the ASCII string draft-lamps-sample-certs-keygen.dana.encrypt.25519.seed.

8.5. PKCS12 Object for Dana

This PKCS12 ([\[RFC7292\]](#)) object contains the same information as presented in [Section 8.1](#), [Section 8.2](#), [Section 8.3](#), [Section 8.4](#), and [Section 6.3](#).

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

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

MIIK5gIBAzCCCN4GCSqGSIb3DQEHAaCCCM8EggprMIIKZzCCAU8GCSqGSIb3DQEH
BqCCAUAwggLcAgEAMIIC1QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIZNqH
TA2APx0CAhQXgIICqK+HFHF6dF5qwLWM6MRCXw11VKrcYBff65iLABPyGvWENnVM
TTPpDLqbGm6Yd2eLntPzVJoVe5Sf2+DW4q3BZ9aKuEdneBBk8mDJ6/Lq1+wFxY5k
WaBHTA6LNm1/NkM3za/fr4abKFQnu6DZgZDGBZh2BsgCMm09TeHgZyepsh3WP4ZO
aYDvSD0LiEzerDP10BgjYahcNLjv/Dn/dFxt003or010TTUoQCqEHJ0oq3hJtSI+
8n0iXk6gtf1/R0j6JRt/3Aqz/mLMIhuxIg/5K1wxY9AwFT4oyflapNJozGg9qwGi
PWVtEy3QDNvAs3bDfiNqQAFJ0EHv2z3Ran7sYuz3vE0FnPfA81owbazlydjB0P/B
OQ+s6VLbsAosnZq9jv2ZVrCDaDA1/g7oD7fY8qmaC602q5/Z3KusfMt+r9En2v81
H2vjgrpxnDIXjYulZdrnNE/slRtqad0GR/WQ358RG+yUmRUbHYHGnkjn9f0GLasI
ZUV0aowivcwYf/kR7QV3VVexgqJMX6k1vzSXRoJ/tnA+1/WPwy1mCJe1jG0gYqSV
txtVB61Qmc2XP48F7wyaQZvdAU9zfe11/tHAaKKJWBpE11IuAEkGtIP6ozYJBFjH
I11tBA8fijTnug+S40vSgjtSRV/+kSEiW4F+pwE8RuTYfUu7q+Ew0LYdLgkH50yE
sn0b62UFpR/E1D9exWzohrFbIdUCbjtssXucruAqPNhW/abT0zicWu5nvf+Pniow
2VxvhwoGt5jZ+1kaR5Z+1/GpbMgq47EUyGCgKv+5GAcJxUxINZqLbACJ/MhLfYPB
eJrXz8f5Cigm1wZLisYCqnuc8cGCXjNqNkU1qtzodM8xv4gcgT/zILxmJTZP2q4n
YA4yBQx5/n2G2dZC+pf3kAfbXcp0MIICpwYJKoZIhvcNAQcGoIICmDCCApQCAQAw
ggKNBgbqhkig9w0BBwEwHAYKKoZIhvcNAQwBAZA0BAjxuoiaSZDbnwICFH+AggJg
k2hcNYt00+15uLqXdiNhr5Q0JkYcrHdo0wR6G5AgLmwi+TYi+P8EZUjDIJ4TJ3b4
6xv7+3pT8cbEFf6PXcfS8/sCfM7FaV3SpLACLZbBJV520KE0CAgALZOLuIz5mGVU
tWI2h1x587KeIv5GRPIxumDebT3Gmkkp9Qoi55hjTgn68o1SgDaJF8o5wnf0Dhks
o110a3x90wkJSN1AXfmBfj33KnT8Dc4bTfAZy1S5o1zCtaEqnct2Urb4Pe03LfHB
ErBsvY8HE4D7qh6P5ftXHQHax/b3hbU8jQP1tR0N90h0SiLi//ebCeGXWQRdVjL5
+VQrh1QF5d4Kz9Zx79oC36g7C2BxCQomur/F9TT12NPzPpaEGGo6ljB6myAHnYw9
rCxbSxBvbtEtlgJnxxb1Y5Q4ukgyjzK6431Bwq2+iNL0vGc9o2c5ELUPU9zGeLBZ
tXWvdX27a0HjusPFdZL70C5zHiYs1FU6Tkn9Aotc424Q3d2IRTTcYnnjs1VS1sSr
4bRyB8zBAQmdQrniBW++7eJm3m/E0U0Yy0noUT169m8KNJrmSspMvKS6pyiYHR4I
BvAIkRIjvdtQvJdQJ+Uyr+HH5daE6golW1917b2bXj/41mvXYkJY6W8x0km1RYhH
QJZphwlvNcrHKO46Unk48Qc/5J5tI+6UDTXFr//V34vcpQ2ktP0MAK11rBH549ef
CsGQTGoq8XHPksehEEMRm0JDeKTVkKx8xNhbwb395yFCixfF2NHeDLXP+JyW+nH
Iy2fnBDlyTiPF7YXyGiPjPAgK8LS8GUE+Zq2rWqrGNkwggM/BgkqhkiG9w0BBwag
ggMwMIIDLAIBADCCAYUGCSqGSIb3DQEHAATAcBgoqhkiG9w0BDAEDMA4ECOfJ/s3Y
f5bgAgIUUnYCCA4i4NaYP4lpAtuXtE02Zqgl9aLFwsj9B/rikBo601ZR/lSryJ4PJ
VGyY6NyBPjG67glJVMYiI3Hge+j66FXKXD/AaiMVD21ZmfrH935S14ZUKS9tpTJL
QDw3ejpDEDqJUFJZJ/ybgpRAKOnjhce3B7F7+WMI8Pr70M1Fbw7ytUCAjOf18sIW
prUA8f809dLiGgiWyjE5HMzSXEib5IMRpq5x4Q28pBrT8rVYgoQSSyVkfHtU7LDi
Bm68RfBgEl7jIqLdr2kKxHC3/1C4xXQgFNXeQ056aRp8Yu4VpoRwraVLU03tJk+
pf1zFfmUei/JtiF1C6uf0PvC2B5h6kAZocE11LxGIDFH7fTd6dzP7qTDbUQ+uEk3
qsgktT2pcoVnxTanvQmTCEZM9ZKCX5/z7Gkm+z831GLDDU9oNyRSrxHrRBIVgH4w
3aGH1v6kfYOWwwwaghQOQIZFyzGVRKXsP7As1L+n4ti831TxqSUZX2qy9LpI4Tjp
5A/NLMKo3uqmHf1LnnYUqoppe88FNY8T/LXnHp0KTkuXFmdKJtp1/ydqh18jBk7
nflcQFdf1R/5okysblRtaMujlhelymT7MoM8u5C8ceIO7uWX8NI5B/IB+Yn2BvzZ
9LXoSia/wHjTu7UK610o7W0q9qTYei1i1x+HsmJa0C6hpaQh6b33VWDrHJb17c/4Z
tvQ9qAzqkqIhFWMRXNK+32jFVAgXrD8U1QHW2ip5s7W/Xtm1AegrhG1nSQgJezY1
OnE/t2PDWuPew94kR0uv1fNsh6p1LYZYf/BaqhoGCHsa/ipD86viVSZDgJ8ASVLF
eLUK3HYFMhJ+MLEZZJffYZA0nbYoyNPnc0vc7dpbk+ZMnlb5bDFcMCpm7+fw0jsC
nsNNL9nqQ1NHHCJRKGuX05rujftbPM7R3GLT9d/u5e9YY5cX0RiDLxomFfflj2Yh
uRoyX+8WzEst98I/KmAraWKXnx0P1FEWajtnCrnGCezDK03xEHTQhECpg+z704mj

MjN6MIHABgkqhkiG9w0BBwGggbIEga8wgawwgakGCyqGSib3DQEMCgECoFowWDac
BgoqhkiG9w0BDAEDMA4ECL2Bz1vW+YZkAgIUugQ4Y0yEjke53NDvCFR0ciUHZ7re
f9/wPx5TgV3qzGhFR4bP2rdpi0t9hAHVK5cmUAR7+wjAJiYdLUQxPjAXBgkqhkiG
9w0BCRQxCh4IAGQAYQBuAGEwIwYJKoZIhvcNAQkVMRYEFJ3fTdQF75rsYIa8J20E
6c5a3I+kMIHABgkqhkiG9w0BBwGggbIEga8wgawwgakGCyqGSib3DQEMCgECoFow
WDacBgoqhkiG9w0BDAEDMA4ECFw78Uk8K64uAgIU+gQ4id0jRb3JyEM5fdpaeQR+
YEeMn+Y5KavplVD5HtgQQY9hhppbQqG4af7KY+MT6xus6oNEQeJAE5wxPjAXBgkq
hkiG9w0BCRQxCh4IAGQAYQBuAGEwIwYJKoZIhvcNAQkVMRYEFEGDhsFpuHhtrt7z
zAawM6xXmt2WMF8wTzALBglghkgBZQMEAgMEQEyKU+C+RuVmgTZpGN9FEY/LofSz
3TZA0x0TJ3EN12kuTzjcGNxJ+7e4w4xI6CZxP9RqrBM/N6N2fThoArRC6uIECC5D
kkzl2MltAgIoAA==
-----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.

Applications which maintain blacklists of invalid key material SHOULD include these keys in their lists.

10. IANA Considerations

IANA has nothing to do for this document.

11. Document Considerations

[RFC Editor: please remove this section before publication]

This document is currently edited as markdown. Minor editorial changes can be suggested via merge requests at <https://gitlab.com/dkg/lamps-samples> or by e-mail to the author. Please direct all significant commentary to the public IETF LAMPS mailing list: spasm@ietf.org

11.1. Document History

11.1.1. Substantive Changes from draft-ietf-*-03 to draft-ietf-*-04

- *Order subject/issuer DN components by scope.

- *Put cross-signed intermediate CA certificates into PKCS#12 instead of self-signed root CA certificates.

11.1.2. Substantive Changes from draft-ietf-*-02 to draft-ietf-*-03

- *Correct encoding of S/MIME Capabilities extension.

*Change "Certificate Authority" to "Certification Authority".

*Add CertificatePolicies to all intermediate and end-entity certificates.

*Add organization and organizational unit to all certificates.

11.1.3. Substantive Changes from draft-ietf-*-01 to draft-ietf-*-02

*Added cross-signed certificates for both CAs

*Added S/MIME Capabilities extension for Carlos and Dana's encryption keys, indicating preferred ECDH parameters.

*Ensure no serial numbers are negative.

*Encode keyUsage extensions in minimum-length BIT STRINGS.

11.1.4. Substantive Changes from draft-ietf-*-00 to draft-ietf-*-01

*Added Curve25519 sample certificates (new CA, Carlos, and Dana)

11.1.5. Substantive Changes from draft-dkg-*-05 to draft-ietf-*-00

*WG adoption (dkg moves from Author to Editor)

11.1.6. Substantive Changes from draft-dkg-*-04 to draft-dkg-*-05

*PEM blobs are now sourcecode, not artwork

11.1.7. Substantive Changes from draft-dkg-*-03 to draft-dkg-*-04

*Describe deterministic key generation

*label PEM blobs with filenames in XML

11.1.8. Substantive Changes from draft-dkg-*-02 to draft-dkg-*-03

*Alice and Bob now each have two distinct certificates: one for signing, one for encryption, and public keys to match.

11.1.9. Substantive Changes from draft-dkg-*-01 to draft-dkg-*-02

*PKCS#12 objects are deliberately locked with simple passphrases

11.1.10. Substantive Changes from draft-dkg-*-00 to draft-dkg-*-01

*changed all three keys to use RSA instead of RSA-PSS

*set keyEncipherment keyUsage flag instead of dataEncipherment in EE certs

12. Acknowledgements

This draft was inspired by similar work in the OpenPGP space by Bjarni Runar and juga at [[I-D.bre-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 draft.

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

Lijun Liao helped get the terminology right.

13. References

13.1. Normative References

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

[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>>.

13.2. Informative References

[FIPS186-4] "Digital Signature Standard (DSS)", National Institute of Standards and Technology report, DOI 10.6028/nist.fips.186-4, July 2013, <<https://doi.org/10.6028/nist.fips.186-4>>.

[I-D.bre-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://www.ietf.org/archive/id/draft-bre-openpgp-samples-01.txt>>.

[RFC4134] Hoffman, P., Ed., "Examples of S/MIME Messages", RFC 4134, DOI 10.17487/RFC4134, July 2005, <<https://www.rfc-editor.org/info/rfc4134>>.

[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>>.

[SHA256] Dang, Q., "Secure Hash Standard", National Institute of Standards and Technology report, DOI 10.6028/nist.fips.180-4, July 2015, <<https://doi.org/10.6028/nist.fips.180-4>>.

[TEST-POLICY]

NIST - Computer Security Division (CSD), "Test Certificate Policy to Support PKI Pilots and Testing", May 2012, <https://csrc.nist.gov/CSRC/media/Projects/Computer-Security-Objects-Register/documents/test_policy.pdf>.

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