lamps
Internet-Draft
Intended status: Informational
Expires: 22 August 2021

D.K. Gillmor
ACLU

18 February 2021

S/MIME Example Keys and Certificates
draft-dkg-lamps-samples-05

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 22 August 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

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 certificate authority is supplied, and samples are provided for two "personas", Alice and Bob.

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

* "Certificate 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. This document intends to focus specifically on identity and key material, as a starting point for other documents that can develop examples or test cases from them.

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.

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 the example CA (Section 3) 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 examples presented in this document use a simple two-link certificate chain, and therefore may be unsuitable for simulating some real-world deployments.

In particular, testing the use of a "transvalid" certificate (an end-entity certificate that is supplied without its intermediate

certificate) is not possible with the configuration here.

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 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 seeds and their derivation are included in the document for informational purposes, and to allow re-creation of the objects from appropriate tooling.

All 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 Certificate Authority

The example Certificate Authority has the following information:

* Name: "Sample LAMPS Certificate Authority"

3.1. Certificate Authority Certificate

This cerificate is used to verify certificates issued by the example Certificate Authority.

-----BEGIN CERTIFICATE-----
MIIDLDCCAhSgAwIBAgITD5FARp09T2LXr/FPQiI+8ZsGAjANBgkqhkiG9w0BAQ0F
ADAtMSswKQYDVQQDEyJTYW1wbGUgTEFNUFMgQ2VydGlmaWNhdGUgQXV0aG9yaXR5
MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjAtMSswKQYDVQQDEyJT

```
YW1wbGUgTEFNUFMgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAnFB71AsptFyqxG4qPtbt2VLJVctHyNXtlIUWve4q
PSo/+Oi9s3sf+t7krrosxlv626L+Wm05t99ZVKWKn7y2uYyO7/IToRpTwHN1sXga
Uz/u2gjPfS69R20ZNSKL9EiB78hgCr1UvY5elQoW2Y4zqQGR729pQYI5obT15V8n
wdyHCTvecvvvMGBiaAk66VlMQCZLG+nVU8wYVCl6fE37Z1qAs12XlUJr3DGgVKGf
ZpMz55xiV8q11Aobhmx4aPPyE4GWshDDt4DbtYJMGLEeik1AmNHBsmyaQCLBxVE3
3ZW1UrhK5Pb9qSL4gizDZ7ZaGZNudwjJu20HHVIGQT7nDwIDAQABo0MwQTAPBgNV
HRMBAf8EBTADAQH/MA8GA1UdDwEB/wQFAwMHBgAwHQYDVR0OBBYEFHhfDlp42Gvk
VHA9s93s9/Hy+sBHMA0GCSqGSIb3DQEBDQUAA4IBAQAMqotfBm1fUs18JqiTgZhW
LUo/Oo+l/rVEIMUPN8+uZgxfOwA0u9cE0IAgMdVELfyHuEt5ld+xyS300z1/Z3X0
w1NpEaLmgBNB70kmjNZkvT/aWDlKE3JVUITYkkLOm10U5J1dF3DjGH+kK+/nbeF2
mHTquWfm7420fJJNvCWgvylBHCFheFHt450G/2t5b8+0a4Qj6/QPsqGwiD6NjLrA
gD0oKIyQP6HNQ8fGpYekiLcq8NQ3sFBYsNUmfAy/Zfjo9/5o5qc+2UwRPTv+QUZx
0bBs2gH3LVOuvgkHXm5EFyfjCInWTOg0PBlsjvHjrROQHSsuL/Bd3uuqG02bJbbj
-----END CERTIFICATE-----
```

3.2. Certificate Authority Secret Key

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


```
-----BEGIN PRIVATE KEY-----
MIIE/AIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQCcUHvUCym0XKrE
bio+1u3ZUslVy0fI1e2UhRa97io9Kj/46L2zex/63uSuuizGW/rbov5abTm331lU
pYqfvLa5jI7v8hOhGlPAc3WxeBpTP+7aCM99Lr1HbRk1Iov0SIHvyGAKvVS9jl6V
ChbZjjOpAZHvb2lBgjmhtPXlXyfB3IcJO95y++8wYGJoCTrpWUxAJksb6dVTzBhU
KXp8TftnWoCzXZeVQmvcMaBUoZ9mkzPnnGJXyrXUChuGbHho8/ITgZayEMO3gNu1
gkwYsR6KTUCY0cGybJpAIsHFUTfdlbVSuErk9v2pIviCLMNntloZk253CMm7bQcd
UgZBPucPAgMBAAECggEAJ56StD0cFfYC5oTRulm5sYK1O0Sp7jKi5CkTiZJrLFOg
```

```
IVPEeVB0255RMiRIIwK/Q5o9g+f5YCyBNN48k54+ZitFM3YVGZlVrwrUwuWhLoae
4K6pAJ6vJQJ3CCu4c3NJU+Biz3YLm3wRZw9GmV/cojKeraR8djkuqFj4lmmW5yC7
mj8XLnl1snOAEZEHhi/10zibru5GoCjwFrmJT8qbmYX89gbua24wcVlmqImzV48z
lQJ0nJDJ8VPNjwvyX27DjefBw2FgUiT8J/iEmS7BZ+1laF/UyEsxqsZ4odJIVfPT
/JbGl+VkAoM1R2Qrv6ZFisDVfGZkIpWtSaBlknh+CQKBgQC82Y7gYnG3wiotvTKC
L5BWMWoknCM4LTM5AqYSZjfpnMsOEfOgzpyABUyK+3zKrzoqxokVfuvHlj2Hzw8Y
EUQ2gqJdU5iObl3dH0C7K5J/9Kua12VEcv5NFiBs5paMXTub6SdG0CyeUUfDW133
UfdW0rgCuPvPpya7lQa4k2T8XQKBgQDT5VHzRJMXRKTaI6nHw5RI2F88b89nvkib
BRvnDm2N7bxVfLiKSf2hQUhdLppIm0J8it/ksjJ/zQ197UA6DfilAjQB+mKi/fB8
h7pmElFElhy71/93T/uv2CA1RaIGSWhTMu+7Z9+/5cb1zRsorgrB2s0tTpDkDnuX
A1wRbBraWwKBgQCyNUsSi1NsaJmM2AEVwPSfobncGktR87Vmkw1MR5FzrjYfbOlO
Uip01ItKi89TJM/rFba+xiqRCUG/KrG/sGuCVPwKvZw0rAl/ZMKc3Z09ihF16NTz
JuC6taqbmW1vv3tEwVwDAudX7rOdslaV0I9rKyXhy9Y0OjPex96zxsOBMQKBgQCt
Wj7hNojf0FjN3b9YnrkBn4LKfu6/gP0FVfit3y/hnU0m4xJWkJHfCvmYwjeWju6l
1Te2cdK+m5MeIqsY07VHybWiqKVpkzbbqm7kcrfp1KVNSDjH87eE9NvkuUMEwamH
53QZbbGv3NwY2+QMM9a5IbgaCNygtviFY0o/NqIBYQKBgQCyki2Y/sKDolNBbjwf
nFMsdYb+nRmbJMSvLHbJSVhypB6aX3qjHhBlPrTW6WT5KIjumCtSadsDceUtr9tT
2ofP0ZOXP9IDIF2v1X3165LPsieGZv4VzhLivJrfMYfI4p4GkiK44RSUWcxrBAmq
9SGCNQ8nx1AsXLZn57U52Oji8KA7MDkGCisGAQQBkggSCAExKzApBglghkgBZQME
AgIEHPBUYbjdNRelyUPep86pkRfIdEPM9N+yPctTfB0=
-----END PRIVATE KEY-----
```

This secret key was generated using provable prime generation found in [FIPS186-4] using the seed "f05461b8dd3517a5c943dea7cea99117c87443ccf4dfb23dcb537c1d". This seed is the first 224 bits of the [SHA256] digest of the string "draft-lamps-sample-certs-keygen.ca.seed".

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-----
```

```
MIIDbTCCAlWgAwIBAgIToTV4Z0iuK08vZP20oTh//hC8BDANBgkqhkiG9w0BAQ0F
ADAtMSswKQYDVQQDEyJTYW1wbGUgTEFNUFMgQ2VydGlmaWNhdGUgQXV0aG9yaXR5
MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjAZMRcwFQYDVQQDEw5B
bGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0
iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LCOwI2juwdRrjFBSXkk7
pWpjXwsA3A5GOtz0FpfgyC7OxsVcF7q4WHWZWleYXFKlQHJD73nQwXP968+A/3rB
X7PhO0DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZO63dKvIKp4cQV
tkWQHi6syTjGsgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/
2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGJWiQVC
CpDtc0NT6vdJ45bCSzsCAwEAAaOBlzCBlDAMBgNVHRMBAf8EAjAAMB4GA1UdEQQX
MBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDwYD
VR0PAQH/BAUDAwfAADAdBgNVHQ4EFgQUu/bMsi0dBhIcl64papAQ0yBmZnMwHwYD
VR0jBBgwFoAUeF8OWnjYa+RUcD2z3ez38fL6wEcwDQYJKoZIhvcNAQENBQADggEB
ABbWeonR6TMTckehDKNOabwaCIcekahAIL6l9tTzUX5ew6ufiAPlC6I/zQlmUaU0
iSyFDG1NW14kNbFt5CAokyLhMtE4ASHBIHbiOp/ZSbUBTVYJZB61ot7w1/ol5QEC
Ss08b8zrxIncf+t2DHGuVEy/Qq1drBz8d4ay8zpqAE1tUyL5DcqZiKUfWwZQXSI/
JlbjQFzYQqTRDnzHWrg1xPeMTO1P2/cplFaseTivyk4cYwOp/W9UAWymOZXF8WcJ
YCIUXkdcG/nEZxr057KlScrJmFXOoh7Y+8ON4iWYYcAfiNgpUFo/j8BAwrKKaFvd
lZS9k1Ypb2+UQY75mKJE9Bg=
-----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+gIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC09InoWDgWPk2a
f0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHUa4xQUl5JO6VqY18LANwO
Rjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z
34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3SryCqeHEFbZFkB4urMk4
xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQsaqpo1d3f9jSkbtAV5w3
vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgEykRiVokFQgqQ7XNDU+r3
SeOWwks7AgMBAAECggEAFKD2DG9A1u77q3u3p2WDH3zueTtiqgaT8u8XO+jhOI/+
HzoX9eo8DIJ/b/G3brwHyfh17JFvLH1zbgsn5bghJTz3r+JcZZ5l3srqMV8t8zjI
JEHOKC3szH8gYVKWrIgBAqOt1H9Ti8J2oKk2aymqBFr3ZXpBUCTWpEz2s3FMBUUI
qCEsAJqsdEch+kt43X5kvAom7LC1DHiE6RKfhMEub/LGNHSwY4dmzhaG6p95FJ1h
s8HoURI2ReVpsTadaKd3KoYNc1lcffmwdZs/hFs7xmmwXKMmlonh1mzHqD1/BqeJ
Hc8MP4ueDdyVgIe/uVtlQ9NcRQbuokkDyDYMYV6hzQKBgQD75ahYGFGZznRKtSE3
w/2rUqTYIWxx2PQz5G58PcsTZM89Hj4aZOoLmudHbrTQHluRNcHoXEI62rs0cVPs
D7IlZOLfs+SSTeNEXxD57mjyyufpV65OcNc1mSJAmMX2jWQ8ndnOuWPcc5J6fNvT
au0a7ZBOaeKHnA8XXL3GYilM9QKBgQC35xKi7f2JmGtsYY21tfRuDUm6EjhMW6b7
GWnI9IXF8TGj15s7oDEYvqSPTJdB6PAb/tZwdbj9mB4qj176x1kB/N7GO974O8UP
/PdHkU7duyf5nRq1mrI+yGFHVsGD313rc+akYdKcC207e6IRMST1ZFoznC6qNgpi
nNTuDz4ZbwKBgA5Dd9/dKKm77gvY69Objn6oBFuUsO5VaaaSlcsFOL2VZMLCNqQJ
+NLFZ7k8xJJQVcEIOT2uE7X/csBKdoUUcnL5nnsqVZQPQwI5G937KQgugylMZLte
WmFXlX/w5qzKXtWr3ox9JPFzveSfs1bqZBi1QQmfp0skhBo/jyNvpYUNAoGAMNkw
GhcdQW87GY7QFXQ/ePwOmV49lgrCT/BwKPDKl8l5ZgvfL/ddEzWQgH/XraoyHT2T
uEuM18+QM73hfLt26RBCHGXK1CUMMzL+fAQc7sjH1YXlkleFASg4rrpcrKqoR+KB
YSiayNhAK4yrf+WN66C8VPknbA7us0L1TEbAOAECgYEAtwRiiQwk3BlqENFypyc8
0Q1pxp3U7ciHi8mni0kNcTqe57Y/2o8nY9ISnt1GffMs79YQfRXTRdEm2St6oChI
9Cv5j74LHZXkgEVFfO2Nq/uwSzTZkePk+HoPJo4WtAdokZgRAyyHl0gEae8Rl89e
yBX7dutONALjRZFTrg18CuegOzA5BgorBgEEAZIIEggBMSswKQYJYIZIAWUDBAIC
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-----
MIIDbTCCAlWgAwIBAgIT3r7MRJB7qx35ms1tFWj7th3y5jANBgkqhkiG9w0BAQ0F
ADAtMSswKQYDVQQDEyJTYW1wbGUgTEFNUFMgQ2VydGlmaWNhdGUgQXV0aG9yaXR5
MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjAZMRcwFQYDVQQDEw5B
bGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqV
KfqLwaLjj+gBUCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID
lB/wlbdmadXPmrszyidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdS
NRFxrfKeoQEFXgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1
ZkuE4A6l41koaZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv
9w43GG8FtpSX+TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIB
aVv4wPxAf1iPsIVKarUCAwEAAaOBlzCBlDAMBgNVHRMBAf8EAjAAMB4GA1UdEQQX
MBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDwYD
VR0PAQH/BAUDAwcgADAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj8OeOr83zdw8wHwYD
VR0jBBgwFoAUeF8OWnjYa+RUcD2z3ez38fL6wEcwDQYJKoZIhvcNAQENBQADggEB
AEi3/4eQPCAAbdgVMVbA7CplI+5LIV+7qUrORNdN8E53zu1oBkxktmDPWpQGiGYJ
fsQD2Gu1sz0Ofpqzaw0QHo90ghEcz3GOb9/JFEBRwV8Ern1rHXKRis56PPdBAlTg
3D7QKgwkGolETHH1TFv4mY/XC1CWzWq/wKPActIDt1cujjUKk2ILsa1kqYfbEQol
ZGil0pxx9jdMS5qaTdjb66GvPpkQI1uH4E9xiYbJu5bD+SX0Sgzih79GEhaP8vjc
w6+P//nJ3ExJkVT7OvIJmwGvV0ULtmsghoigcd2BBc/fOKdbyIBmJBe152dd02EW
6FwMfHKDtHO8k+/XBeZcxF0=
-----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
z5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs165ernT9O5NLFflHUjURca3ynqEB
BV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZuTtMc1zy++MxQlqdn9WZLhOAOpeNZ
KGmVwjeVy+8FkyzC3jX/Qcm+ZLCqlLqhBwDHdZ5qDTII2PVX1X3K7/cONxhvBbaU
l/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy6SCf58duq/AOEksCAWlb+MD8QH9Y
j7CFSmq1AgMBAAECggEADgxoWEDDRE5yEZ+s7TMw+WH2o+3XOOrryqnsLbOyv34I
wAAUWK7qZyjd9rSDOAtBOgFhQNXYhWZlT+0iHslCIfqJMZ8wy1iFHBCIphoMSWs5
/D+idXrUef5Y23rClBxXH0g1UnSGXnpUH4ehV6p1lvZMh4OJKEoMC4cpyd1SzXrw
+VGCc1+pXv/tTW3Rb2qoWO9JoWY+Epcssrw5N8OFIFODh4QfbLN6pVTt28aQ4pf/
1KhLoapjFzXSYp/jrcNjYJ9qRdSAbZsKOJ2yZ0yqjLHDCDipFty+W0pkUZcJhsgu
Cg1Stt7tKgSvAV/nEjN8e/vA91/AACKBCNcLzEoLgQKBgQC4eTM6BDCzlusXJBK4
SRC/WwUthJZzfOk2Gmwr0DCTRYhWQSDjBfiQNboazHObVPz45qP10fOt2iPEHeX+
VWAXTNrN69M9lEzxygA3s76lAejBR3FbLWkzLYqPB3oZwSIE7CrWHTXJipFWZv+X
FG1R418fnRCUMJ4j85qem5iyqQKBgQDWhQMJu7FC02fr83qsIdLwqhiDtTpwUN3j
qfp7JoEZOxbm3TgM1xPAkrQTUgfr2ZhXGtUwsuKHyifxQEycrTkBOg0gqAfG0fnv
ybyXK6/guctHJQiy64lL39kPuvQkKB+YO60B/oF6zbyFvqanoKXjpspObN3i3yBU
X5/EOu/LLQKBgQCUVwHWeWAgSg+pgBx9jGOnPK4hOCkznRJ7qyuo37Tv+E317lFf
vYFvlYSd4CJmmiUCkZTvK3FkL7HrFo/HwSeQFQEt7aDkN8jX9bPPFv8K+UoNgkGp
LA8YVFrDQSPyadfNVYvsuXhzJLZSYGjPOGHgI5JufYLDZ4UDK/T97ekQYQKBgDDM
ORCxvXTyGiW2USVu3EkaqFDtnMmH27G6LNxuudc/dco2cFWbZ0bbGFN8yYiBCwJl
fDGDv7wb5FIgykypqtn4lpvjHUHA6hX90gShT3TTTsZ0SjJJGgZEeV/2qyq+ZdF/
Ya+ecV26BzR1Vfuzs4jBnCuS4DaHgxcuWW2N6pZRAoGAWTovk3xdtE0TZvDerxUY
l8hX+vwJGy7uZjegi4cFecSkOR4iekVxrEvEGhpNdEB2GqdLgp6Q6GPdalCG2wc4
7pojp/0inc4RtRRf3nZHaTy00bnSe/0y+t0OUbkRMtXhnViVhCcOt6BUcsHupbu2
Adub72KLk+gvASDduuatGjqgOzA5BgorBgEEAZIIEggBMSswKQYJYIZIAWUDBAIC
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 3.1.

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


```
-----BEGIN PKCS12-----
MIIXsAIBAzCCF0gGCSqGSIb3DQEHAaCCFzkEghc1MIIXMTCCBC8GCSqGSIb3DQEH
BqCCBCAwggQcAgEAMIIEFQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIWQKs
PyUaB9YCAhTCgIID6GT96ewG16YBcazV7Zo8cZ0AWul+It5HDTSG2EYFtJB8nqhG
rgKuUeD1g1xWJw++M7z3kAtEn1Vxi1KdHtzZ9S47GRd69TWSpbA8l6X7nY9WcdhW
N3OcpdBcuJo7PQ/PFk1srsXbqrKpnDkHn22twIN57/ZR1dvicpvsRbmjWf73ia4w
GfabS7WUGTt6Kpdd/kUzWNdII07B+qjcqAOlZ608Vql1MD75Jbb7nXTP5DpSP7WA
kCAGD4b6O7MzqBwGWLHXnLQP3RniraqgFwLKOAOM4G2G+wJVQ7ig2GhJoD0qfd9U
+dpELWZs5hWXU1E2Q5mx8AkQZHesAhCHsONLMB38rzCeWGRODHV03+U9EjQOusOu
jzHEEPtKzZa+c2BtzwnVxYi1Tz9BIs0OWLSE5hlYuT8ZQ13/bDlaUmKZgBvEubzZ
t/fglGTlCczymabSpaMpQRzXO0eT+/enDdILpDT2cBf6Q3+a521g38gaf0CIKfGf
NLCCfL2YxLbjHJHxCq5WqyY8bLDNreCxffQ3wV154eIvwYdLfiq44uM2s2vrr5bM
LAV9DhomAuyfQJixk8I6YejlEwZQscDeh5+037DTzDc0AFQDe8d365hQMcqMYC9w
aey7X1SUCL9B9coEyR2k4NM1qFNnd0n3K1j0bY9N0o2kzI/02nCcO9Yq2qMHkA1m
XShpyrmkqYMDtlM7DXQDPlYGumIwYu8tSPuFJzXSq64BNmRxgvOhFnrqytwBeAVS
XTe8HelM6EOW6z/KUffWOYwuq/QHCgNRODJN3hB9oI7Ij5g6wn920WNTzoFjivoi
QNEivXhyEakrBwZF08fJFUJHoJg4N7M1nV3F6I8/pgdPyRMFHO6InfDD+/Uoitwg
51BxMyAvejGVzk0KxolG5NQoUOXhje7qFURxIbqXrSI1Xui6jSUPXTTyGLj5rcLo
mpVMLbs5tUQFRDBtN5qBmbW1SWf3ZvkHScMrPAgpZ/cDSKh5w2ykUGWhIPAaXClA
+WCWlMOuzrk+JDRjmO+Mzptno9b4NCiFCyGJqQSyEo4dD4ftZVciNK6fCjnArkz3
mgQroeIDf/VpoExLcf+Kp/PK+X9oTbyW5pShH2B1sKD57l1qT5AlBfmpKA0lrw9D
KRvO8kfLxaNBbijOU1f0YTQIwoykq6k8YqH78RcjoeOoEcFriknBYqc3ay6tNbgd
IhaBuRXnxxv0drXkMLReZ6EqPBz8NmYu+vhYKtaMxg3T5+H7BEfmLy6qIJpsEqtV
a4vWrVbhMsNtfjVQnDhbeZ6Tea+U5kxXAhXfKE1A9LM3UkYcvn3aBg8smKIrL/wu
/LPJSKIwggQXBgkqhkiG9w0BBwagggQIMIIEBAIBADCCA/0GCSqGSIb3DQEHATAc
```

```
BgoqhkiG9w0BDAEDMA4ECPoEFEHQGB9dAgIU5oCCA9BEuCtcDZvvbXNHI+j/3C3U
zI65UbgkDQL3S02ZMP6Ooec5Mrx4t5GekUR6hyZJqkHpcDP7UjdnlU17TYH01bfi
lcIaaNaJ/5pkNAqfPKKT9ZXNTh/2iVauqBPcQVS8tNWMPsOSl3V+MlaCz5GJPSH0
H36rXRZV3cEq5KppiG12CHmNTpumpcRoeYAn6UMs8iaFPyoxNUircsNBtr4BpWqL
qU0cuVL6aUS0mWwC92UXNRbfo7MLhmn92myE1FuiQeeda04dX4HTVT7l+jEiBq4Q
pXIGBOu2pOJlmc87ruUl3UEnjXN8NSTgIlmuzu/ohx0jDJRf13ABRoJtYC2kw/iz
Pj0Yu4ux18uZ/FfN7qgKAAMB2Dx1UJLCC713LbUj1zaCMc4uEgt+9tnmMe5bKMg0
V3eMa5QvHp0yxGZpqpewisaBI79z9ZoIkY3gqfnZhzRg1uJyHOLNY3hvMTK6O2XL
XgvW9mNbx6YCOj+SSAVKQIqt6vswSa7G0Zfc0y26evVOdOMJcfYJ6D1Q+NV9/nlj
st4pFf8orZL2zrMoC2ISvjEJKku9dyh7DIUxVJGQm7Kc46MYBV0N7ZLPHrlsq8/j
ap2q4glZfYRefqFKzD7ZnIcRKu1dLIRCji86m9Ic+n8Jox2aUAICm9Cx9TdE74gP
9+uHpGfI51sMlU0Q8Fn2W8xHfBiwzbcyEAW+YZj5iKuGCcjPAx+dJSMLkFU9/Uun
wgO3VOPoYyLOluO1e8Uc3nw56eT2x5yV69gnK19s/K0zyOELm43Ex1JiJKWOO8Xa
UbmbYlzZEgxhfp3fP65KN3FOw8ehHEuTTpXTIYJQlKFzODzm+fkYpZCdXZDjCxli
o+LPHjrhQIR1umBlGaCL6myNTSeFbyJAF5gUy1VqD4cEm2bxDSdBefBPLvR5Z+b/
4aGPaqpNTb5n/vXeWY6AHOyDA4aLtuKUo7TWTvp4dSKLzPGhTUdu00WGTxSj4rs7
9tyeHdTlbhhugLvpfyrBzDWA4BvyVHpCOfnj26UvCKLQgAvjzKEXsiqiYuQdsgQz
rgc9mwLi6GuJLm3OjMhonGtaRCgF3vFvKUuki3WY/7EcClFn/kjjCLQhP3EcP7wi
uH6dpnlu9l5R63a7Tc9pvhCnYyt5Rt9kTCh+NcPEH18eAHj+2nnEDsN+nUfLzAgV
NHrNBq9ZgEWibC6/8ihy3qaYRAuHFK+zQseWT0vEgJCBqvo0QwDnGit0NhtLczAt
gan1xOL4/N1VE/bZ7Ydxm/dDpBcdvspiXg9LHlGI6tS8UDfAlGi2BhPmiE3OAR4e
MIIDrwYJKoZIhvcNAQcGoIIDoDCCA5wCAQAwggOVBgkqhkiG9w0BBwEwHAYKKoZI
hvcNAQwBAzAOBAidIqBxZFwvagICFCKAggNotP/z1THhMYAjuY/0fDNvUslKV/d2
```



```
LU4mkt/mLD72DZCkQJx5MYl8dw4JbQv6TrS3wWPsvJSAEG2XlY1PkF6MHqPfuWRp
B7g5Q972q4TXKqiffDXQa/GyGaUjqu6q9te8uP1u+duQ2qbfZWGsWSTBSu5NYLDY
tYNy9xWscdGzCG8fvFiYlrc6cdyUl4G6aw3dZ1kcDk9ki1TwsL2mAagktorzTt5H
ewu1DVkpQ4OdIXuD9uqhZ5P6Mbb8zyVPkFDBUPj28zIA045T/gEyAuuJRTU5ndTO
TGzXzXgC4b67zbSQqzIZsL3Bld+uWlQhS8xkpaOKUzdexN4pu1SnLAJcGE9xOkcW
1c9Ro+yj7mkxTU/UzoYzyKWQzduJtl033iE8ocZV4kcknJZTPKcNvgdPCMKvcjSH
YD6HDIVUBU+Frm1yvXQz8Jvxi2WMy/+ThTUwJF1HJ/CXVITECAg0rbCCMbxwq+Ys
7XzzqhBYdQWEJJHEUFDb7yo1qK9hDkxu0ZWHA8PJf4YhxUcUFCKyYOn2VzfTgbpY
b0Df2MqOossUGeIfWn866rsRQLFaZJNpJSJMgWbc7ASeq0hL9s6cRTtN19Afyp4G
pQUpdMbYKcRabkuKZDCPdmSnaNCeQ8KlRdF517O0Bv3uYH2xaWIFGXP3nh+54czF
yxC5eEALTW1fDRH+xf/AzkaRB9uSB6i4ykZfhdGyAI8DpccCT7/SI99KJmQ+s9S5
WFRmBaepqV40a+VKDVO4wIsdiGiz27GNocRumfKdNjaREDIufWlX1s2PI2b3SJCz
ncyZvLY2fOpumqZYXemWUIWiPE44IsZV6mCJ0UsqEFvZNrPNyfzo9w1s5SNy1oIl
d2NxpNkLRAm8FIA3MbyIuvFYGhyo124sHXLGjXJOhqpnn4q5dhLCnB/Y2HtRSlih
raJyNO1GE1PwF6Y5pdbYHkIr9VPlPueoHFbPiz4rIgHMuUa6IRkIfZrm3QEEagzo
ZgFudPJAokWD7hy9rg+fXj0SW1O2yFPesBCxWY5OQd3j2/2WYHUwwx9y6GJl+C1k
I/71/kxATWchmg8uRoq/DigGlbxmvBzPUZmpbvpvLwBk96J9M+Bxg34gC8xj0G6K
YxdZDBMJoqQmTn4xeK6qBqjlFaRdg4eKN8JHJqA5Xa6u/t4wggWUBgkqhkiG9w0B
```

```
BwGgggWFBIIFgTCCBX0wggV5BgsqhkiG9w0BDAoBAqCCBSYwggUiMBwGCiqGSIb3
DQEMAQMwDgQIehcRLmVUApMCAhQOBIIFAHb5dXZKzCeRUo2ZSj0oyuFS3zQ5HhKy
fapsyCqbYCKv/lSzNYWvuda7xfa+uOM7/wCB9sWdz0MTpaBMHWx9hvibZIY65oM+
ry4tTuKKqOJl37OsnjB0dSNTKszsI3faPUjslxqIH3aC1shD7OqhIRGZzRjK44PJ
yWv626oQrgVtTYR9NYTdee+SbBZbkEt/EpWipwftWXGR6tSYJQn99eO9Vih8HyQv
wIpidUh3pCFOlow4VZyAqIWOHcw9TAjBXNv+qfdH7fiX9wM5/GvnQReIsqjXCUoc
6pSQIAqD/f+I/d1F2ZmqM7KwX0LGRER9OWZGyF734pN9GLbNetWm6rKxmlSI/5m6
+2Jxxfann16P+vBSEgWJ/I8GnJAdzIbBTyfjog4Gi2+lmrPzK7+C79ntM9nfsr4x
Vzy/BknwZIaJksd4VvOGkS9nfM6shtBJB9uR+GJfthtsvIVUHN0kz2r/lVzMSRbO
g9yR53hv1H/nXCmUjWz/BvobmoaVBcCmmOnnYZTHMNarIVYdLQFif5ZLH7WV/XVE
VIoRntNRiKsK96VAHm5XboWQGCqL0hehIX3Nily1genGm1aFlSQNMvLDko1ILDTK
rINvPmjG/WFoLntpJFPtYZsooT1jjXLw3VTSodtgKQNdPYOEidSJqwIS87fzrCB2
Wmwys0iGfdsuNhSaqNqa0dMO6FiW2fkux7H+w7SX1/n9YeZUNLOcewLcC7E8IA1I
arjglZE1L6Yb2ldXxV9q3PPOwKuGnah0TKnD6mLn5BIGOGTzF1VspXRrJhFrcLe+
xsJR1r6niI3bcMWXXy7gbm1X/CRE902IynxE1oDR+xZ6rjPWDJP7kVf4GvA8trCG
rot4pbJbmwlBeMIylScdQoHEnyqrenOnRMmXZaKzl3njtq7Wk78qoJq0a6Vh/sde
0KcOPFkyTZdMBlTztm0K2VJU3jUVzPlM0WY2fyGDoA89ol+/MiNsgiaEghGybXBY
ipOex+p7j1GIRN/CKmpWsqjZnB78kyXmZ6AE1vC6neD/7zANInDkzXiun6ic72Lo
BX3JGiCSuM6hIPJ0AcDwlzTDu0H2rCQNw+tivJ2v4KbgeKoc6beQb5fZHs7VsWHi
kIcpwqB5ngwt34wHgFG0nTS4lZmvzSJ7FMRVGmsDYkDTpZzgNOaxiUBQMcEvxNIe
3nAmA+dvB7w6XRQVSUsL+vBFhHiWGZ7hk5sCeHElewXK0SyJADgfFlYq3EfEgZ13
h4wtoSfbBVtzbbyg2LNegUCLfIJkc7fmT7X7JSxbjOgndMHEeMdVb+NFxbgsXYrY
D8rC2A8l5cQzZrsxb1bvgybEJz+NU/52UgGrPmdjJKuGBK/V2zor6qPvKyId1Gb4
QQuIoyClwhZ+qk9nE4Eft84y7ISgMywH+lw87HrSHKfpqzQhCxlrLu53IYK/4PhE
7BYC9Q4tvIsZXSGZ+nju4tyzERSlaNe5njUeIENr4B/+kXULwVDcvMFHqUFJMkFa
i8FUga7gyipZ+654clGgJjnNBO1va8JcdtdPRRW4gwdrVn8u8J78KBzt6ChkrpKR
V8VeWKBk9lhcT0ZNpJnNqhDrkfzHBqP0Uo133I7P7C+h9sNDI153W6IOIodyQE0A
v1WxHo4y/1d1VeGDaB7hOSDq9ZMpm9n1En7F6/1/s4IUZHja/qRrK9hD4M0Xq0Lh
FXuUzuipo49OMUAwGQYJKoZIhvcNAQkUMQweCgBhAGwAaQBjAGUwIwYJKoZIhvcN
AQkVMRYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMIIFlAYJKoZIhvcNAQcBoIIFhQSC
```



```
BYEwggV9MIIFeQYLKoZIhvcNAQwKAQKgggUmMIIFIjAcBgoqhkiG9w0BDAEDMA4E
CKq4DtyiayOyAgIUpQSCBQAKQtkPOS4sLE6Os7nP4RaJWBuyXl27V/o6TusBRBgQ
oPzP+aC+O99wgisEKedyB47bAzcO4sba4q8UkERAsYHcEhdD2hGRCL7ou9jTtrr4
RgZpa5V9CJcBO0t4bqy2lUefOpm6no+RX840uyM4q5Q+cfH1rTQ1a/a+gLglbpto
EkH/4dfR3ELYiXcM5UrBYTJOHcyME8c+TXbpf7kiplTtlsrlZyU5zrWcxngrBxwF
A+O85W/uVR3QZSW+EGx/VCYwGruZlNytBvBYjsYsnC+yKYXbqL81DgOePy+eh6VX
64SwBLXcWcY+NK2EZrhzrUFjl+PXFKY3IVVPJhTE9o7gJA0hzvAanOluWXozD3/W
PQaXhyIJDwM2MjznjL2MBydpy9K8Cio7XaV6PX8DszIZkfI4DAz5f7G7WbwUq3Ij
PPPWiUv+JsR+dnqzWDJ22SXc+AdQP2sKqMvP8gOpHOsVlXXE76c5rUcZCZD+gGv1
avO7YttWqbDqLj6oQEIJ8LX0Qvwd0YEhetE0bJ5uv2njhQDhLkH/JIbmFSgJZeM8
dtKHb8f5wZc2B+nXGB+TFboGzSuP7gaWu1vKsJNqT/J/FYEqcamI2F+td7z1sGfb
```

```
R9ckAcxXeb2uPVbCJ1a50gRlz9qVm5Hb5f53X7aoQQp3F3LDGQmJ+GFQ/oXXwabq
n4TvNO9KDhxpGcMMU9RnugUfNU9GBec0vfrzmVKZdmJ36HOmMnLvgRakRhCV3kGA
BXY83hwUv17E1qASLKcAWIachkCCGpBGyGtP2IOZTn7PsLJR1BzKnePa7MgFcgoC
ToIpdQnCTtAsalmBm1s480LN3GB5ojeGbQvNf9TAviA0tg5VuT4/O48V6uYSJsIZ
sawm3tGA/LjxyfV1aLddQT5Zf5ZX9BX+K/PB4oYAFxtUpMK/aL5G1MvppUJ9CjqA
tnoKE+EkdQmyZ1VoDO9ih44zuRx6XV4AEYafNB8ygjRHGsvPW0/M0Es0w16wzJHT
uf/15fD/nH7Xh5MzhCF0CtvLn8v+S1Poi2/40O6pS2byjUFRbeCpzEpRxdv90LCb
9ALdy0yG9u41W3yInKNFnaWBulfOPFCeZT92M1BgwJA8ZcydtiiunRNAH5iWLSPl
oUpOD1v6En+rat+PoyRXIy2fLHBL25awLhABoZPgRsCiLsiNiohfyngksrQKeRgO
laBMT92J8r1E4sUKirQlcOdiWBE6vmBSXzyN/twvfgPNIXgR0rw6c7VhhS+hNTrs
ttg/xcfvJ/bftDbKm+RZL+yQoOkkAf9R5tizyMdMBlaMrpfrBxvNtMiykbZ88SYo
A70Trwab2aHQluVhs8OjXGBEOqmSudcSdV1EhBpo9HBsDZZi0IwOp5/B9fCHdnTh
CTiUm80eQ6mX2/DB9LlNh7gHOyLL3azTm12D0ZpZNaXyxLzdiRiAdwpWZmmegOOG
70yi0D5eIxh6cbnbuU6Ygdp+pFFVYHfAvc5Czpne2OPhXX2k0Okbwawr9AfrFjIf
AEmBFx5GBGr/lSiUQSkbUC/s209YgaOgWTYt3KXPzrThJJGZnnXZRTGfIi6vp8Rs
nPX35+Dxe/Lp3gXDdIJeWG6XVA8t3fspcoTqPkm/XGNMmOZ81KX/ReVdP+dC93so
v2DuDZbYGPmHlD47bOOiA68GD64DEuNtQ8MhWk8VRR1FqcuwB0T0bc+SIKEINkvY
mDFAMBkGCSqGSIb3DQEJFDEMHgoAYQBsAGkAYwBlMCMGCSqGSIb3DQEJFTEWBBS7
9syyLR0GEhyXrilqkBDTIGZmczBfME8wCwYJYIZIAWUDBAIDBEB46MAsz3IW/otz
UKMFDfWTViMUL7zfR11eaXJwLbIeYN0LvgCPONEp+hUMwXfnwDNTB89j1Ly5arzK
LfOLWHXiBAj1OQCGvaJQwQICKAA=
-----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-----
MIIDaDCCAlCgAwIBAgITWeEgizhkG2crS8Kgl56AnNft6zANBgkqhkiG9w0BAQ0F
ADAtMSswKQYDVQQDEyJTYW1wbGUgTEFNUFMgQ2VydGlmaWNhdGUgQXV0aG9yaXR5
MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjAWMRQwEgYDVQQDEwtC
```

```
b2IgQmFiYmFnZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOZwBdIJ
UaH/TYwSpHuoPu0S6zoEX8EI3B/ts5tAH+uxSUTaxME7jrrZVmplAN6ffsG+16os
1RzkIVXrI8IKfDyaaPAHZvGq/OHdrbXstTlXcWgibjXu0iY368EoQejbwJu0vAgx
t/hGqZDvX859qVsGkREOrcFrR4tUE+dT3bkbYkNaKrLiZPCwQ4FDGZSlLGl3xfBi
syZRrmi0Zef9yn6/fm+lZAg7sU2WC2cbevmt/0JGgtyPZtsoD7m7RxSQeT+frPG6
ETkiptTgdYLC6MPHhfUuzrXBhnqKGSYiVEAkdeDWlOWyMnyhGVdmErV8Hc7aBCSd
n0VESCvvGJ8JQd0CAwEAAaOBlTCBkjAMBgNVHRMBAf8EAjAAMBwGA1UdEQQVMBOB
EWJvYkBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA8GA1UdDwEB
/wQFAwMHwAAwHQYDVR0OBBYEFBfFhHvQp+92kDi4s28IvJK1niuUMB8GA1UdIwQY
MBaAFHhfDlp42GvkVHA9s93s9/Hy+sBHMA0GCSqGSIb3DQEBDQUAA4IBAQAT2G9y
JTWq6FS7hBYLjeBijVILmvwRiy+AucPJS/DtPM10mwObdrTnvOoLKeEIQWDV7gg5
RNWiHlhSUsjUdXcsOvuQ3FxsKp5scFd9xc9C7EAzaoorvpQOSiJsFEFnkvQwjdZ0
rfHH2Y+k2Sa5YZZdhZJWwqyNWQmUavWSmazqkUb5DAlOx7Dcfb4AzEX3sO55LAYF
XKpqLxzoVPsiy1JsEmSd1IRe5ux/b66xdwpSTx935A0nTQ8UcBvndM6o+4UIFZOb
PPLBKORIXiHNtoWqjsxIcQaGDE8kY2LEc94wDUXcaJSOi2zCHuF+DOuUTXTPmCJC
pVUZ9OWDKfM54rYh
-----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+wIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDmcAXSCVGh/02M
EqR7qD7tEus6BF/BCNwf7bObQB/rsUlE2sTBO4662VZqZQDen37BvteqLNUc5CFV
6yPCCnw8mmjwB2bxqvzh3a217LU5V3FoIm417tImN+vBKEHo28CbtLwIMbf4RqmQ
71/OfalbBpERDq3Ba0eLVBPnU925G2JDWiqy4mTwsEOBQxmUpSxpd8XwYrMmUa5o
tGXn/cp+v35vpWQIO7FNlgtnG3r5rf9CRoLcj2bbKA+5u0cUkHk/n6zxuhE5IqbU
4HWCwujDx4X1Ls61wYZ6ihkmIlRAJHXg1pTlsjJ8oRlXZhK1fB3O2gQknZ9FREgr
7xifCUHdAgMBAAECggEABcQg1fTtieZ+O/aNdU149NK0qx97GLTBjIguQEDDBVFK
2lu4PhBg9AdgAUqLH1PE+eq65JaGZwvFH8X1Ms2AKiRzYsPOQIoJ4n1hc69uiEN9
Ykcv4QHOvvqtCtWYjJyb5By9WPeLH6QynJ6FlBoSqxhURSWyYfTuwqt1OHEhsUuH
d3N5BmbFiRBNj4aIA9zz+i5xL0m33kMKai/Ajj3sI0AJsZ5ZVAhYbC8sCt1Xevb6
i41p9S6GSwGC19by+1y9WC1QGtb5GDotvChMvmZS/O3NeDc6xC/LZoQcHNVgiZd7
f1g6iEkJlCYK+D7xsd7Y630w75Haj0vnlhiJObSA+wKBgQDxv8jp2D6IVRGgYfaC
nUU3Mg70wagX1fgPHO9Sk6e9c8CgORh2uwWjpTawu88xBGFyZ+xnWqr7GCNsltas
3m94ri4A4R94+5uL8+oOLC26gMDfzATd1Q3k/h919YLk89tonQEUbCFZJdphThEb
vg2W+nNsEVcQGuClzhX0AyGMswKBgQD0BYk3sdGQbBA/hYD1EYsZfYebUiYv2lTt
VGRgTohKFclRAWOtGP9YRbKyEVkBLhjgkXzS9xGqKywP71z9Iny+zDGbzk8ElB/g
lS7GFGX50TG0ISfaFWTYdxt4mN9pduZE2blT/26uyU8DXCEBhF/OqhwQjJqKTYTT
Rl3Ara5fLwKBgQDQyVtjIyD2q8naY2D8c4mo3vHtzyc21tQzcUD8Z4vSYps1hbos
KN/48qJmRv3tjqP+o+SXasYKsFE/4pIroLxTVNNkbQm6ektfttwpO1yPG834OwLk
97HVWOig/tX6mOWg1yBsm+q9TKTrrvm1pRGlmE6BQgSYYy4r5O4u3VlnYwKBgQCl
B4FvWyDhTVQHwaAfHUg3av/k+T++KSg6gVKJF1Nw1x8ZW5kvnbJC3pAlgTnyZFyK
s5n5iwI1VZEtDbKTt1kqKCp8tqAV9p9AYWQKrgzxUJsOuUWcZc+X3aWEf87IIpNE
iQKfXiZaquZ23T2tKvsoZz8nqg9x7U8hG3uYLV26HQKBgCOJ/C21yW25NwZ5FUdh
PsQmVH7+YydJaLzHS/c7PrOgQFRMdejvAku/eYJbKbUv7qsJFIG4i/IG0CfVmu/B
ax5fbfYZtoB/0zxWaLkIEStVWaKrSKRdTrNzTAOreeJKsY4RNp6rvmpgojbmIGA1
Tg8Mup0xQ8F4d28rtUeynHxzoDswOQYKKwYBBAGSCBIIATErMCkGCWCGSAFlAwQC
AgQc9K+qy7VHPzYOBqwy4AGI/kFzrhXJm88EOouPbg==
-----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-----
MIIDaDCCAlCgAwIBAgITO17BWkcdhfwmHN7ueuPziuUW1DANBgkqhkiG9w0BAQ0F
ADAtMSswKQYDVQQDEyJTYW1wbGUgTEFNUFMgQ2VydGlmaWNhdGUgQXV0aG9yaXR5
MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjAWMRQwEgYDVQQDEwtC
b2IgQmFiYmFnZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKrRwJQT
TIgSJPIiasB5P8g6BVsI/D/WdbmHatWqiLqH746AMo3QPE27AURnZr2iDkkDnqbD
Y1tZKO5RPB5Q7PSR59RPrcx95in5/htnq2PmpZDCU1z7zAFHQgPPntTie5PdYGFw
6cyFqz9ynNMU5bCfLRiepocnSV98D9Px7sh6XykEHw7rDx/EuconT3Ilrge1o9F+
MWNaVAM9q0kgJZxr4RMyhW1uNwT42Fz1J0VjLVxcmtXY6uhG/TP5JW4XWYXgyy7I
y1El2FO9K/VVxjP6nI3fzYVmKYQngXKrMGjOZly2HZtJhZqqHnBetplBNA4jXYcC
k7Z3n3dHJZfg9xUCAwEAAaOBlTCBkjAMBgNVHRMBAf8EAjAAMBwGA1UdEQQVMBOB
EWJvYkBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA8GA1UdDwEB
/wQFAwMHIAAwHQYDVR0OBBYEFEqzrDFTAkmcTeNueeAlYZU+iGIlMB8GA1UdIwQY
MBaAFHhfDlp42GvkVHA9s93s9/Hy+sBHMA0GCSqGSIb3DQEBDQUAA4IBAQCCgLLW
tCBYZK+DatWaOVNiJdTxgQBRXtspGV79bejJgFV2YG9BwvacdKx3ZnCNiUprr69Y
WOjP/l9GP4bCKHNfrp6j79rGxe8MtxEWswF00cBj6QYZaWWjMXQS5G6NJqSAWlCl
cQfNSVMIgtD6vCf3ibyB22LDRYBokLFSK63B0y0OXbdGZYaQNVFqCXBPT5zhB3p7
lZAU09PukACJI+7lfupW6Xc3Brhqnw9pkouNElBvMSx5rAcAxsNK4/Jkw+sQSEih
VinpFedAz36YufvpHUNOmYspiHFz48iGPAaNbDREEoDUSRB2PxXVMim22EH6iBXe
t1oEQxqwa0AMz5Fn
-----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/AIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQCq0cCUE0yIEiTy
ImrAeT/IOgVbCPw/1nW5h2rVqoi6h++OgDKN0DxNuwFEZ2a9og5JA56mw2NbWSju
UTweUOz0kefUT63MfeYp+f4bZ6tj5qWQwlNc+8wBR0IDz57U4nuT3WBhcOnMhas/
cpzTFOWwny0YnqaHJ0lffA/T8e7Iel8pBB8O6w8fxLnKJ09yJa4HtaPRfjFjWlQD
PatJICWca+ETMoVtbjcE+Nhc9SdFYy1cXJrV2OroRv0z+SVuF1mF4MsuyMtRJdhT
vSv1VcYz+pyN382FZimEJ4FyqzBozmZcth2bSYWaqh5wXraZQTQOI12HApO2d593
RyWX4PcVAgMBAAECggEAEvPt6aAQjEJzHfiKnqt1U7p4UKb5Ef4yFrE7PdTLkeK2
RjncIhb6MeevVs8gO6co7Zn8tuUT95U3cOXLhVOWTvaHYeurTXaknICz3IeOoSl8
skiVZko70uJ8pR6asWUlr/zOjlEwZ7RnEUWet97oM0YeA07LDFDkF7eUq//6bfzT
ewr/QfDDsv+erwJBh+9CRHOJyTuDH1WeGxYV8VK3M6VhdTjFxXxFhrQ4pBe5J/UA
17Bd2GM8Urg6VYzVo6x4ajnc1H/ezYLdc459poTffv6Fg2trqFVAj2IrQlAeqjda
lemsa6Np801mUGknq3fjKS13RYGBv/48rCHOT8eRgQKBgQDM5TuS4ANQjOYoOgtF
xoVjbVlndOo+SmdFkZihzQHxcbLY9HXe5HlbLf1IMXz/nERxl+SmYuuJk0EdiM9r
HOCcHRLfBmC7t0GdVvLDHSAX8Ec47LbtKZqyM1U9dn7Z+5q4iywqpaP8pP3+oY57
cgtQax1jle3xhRAj65cl1RBmQQKBgQDVbLqK6wKDfSdZuMZGUtOY0rtamBDCgEU6
rEqBAyCPy5NpF1pomUFcYKWT/wbReFqtuyq2OyiATB0yHHMko46BUtN7qX/m/skt
DHWXVWs1+G4IgEMVokM9jjrkgdY5grrJ68sagKC+bgv35BizHPIqgQuO6qnPSrM9
bevwbQEj1QKBgQCiPE/zeBSnzyjeaTdLxGkR1R+ZX2WqdNdYqnQkiWMkflaSmt5J
4raEj+GhLC5BZsZ6+z480M6XXFWOwSkbMv5WHl824KHvgKcfoh0OiR1EVyjN1gDx
wKOQvjycMhs3FpXn0arjCczS2wGSgPGEpUR4JJhcpfaF6kphZsWDWzVlAQKBgQC2
ivbKltNhj4w2q1m7EGC3F5bzl5jOI1QTKQXYbspM8zwz6KuFR3+l+Wvlt30ncJ9u
dOXFU7gCdBeMotTBA7uBVUxZOtKQyl9bTorNU1wNn1zNnJbETDLi1WH9zCdkrTIC
PtFK67WQ6yMFdWzC1gEy5YjzRjbTe/rukbP5weH1uQKBgQC+WfachEmQ3NcxSjbR
kUxCcida8REewWh4AldU8U0gFcFxF6YwQI8I7ujtnCK2RKTECG9HCyaDXgMwfArV
zf17a9xDJL2LQKrJ9ATeSo34o9zIkpbJL0NCHHocOqYdHU+VO2ZE4Gu8DKk3siVH
XAaJ/RJSEqAIMOgwfGuHOhhto6A7MDkGCisGAQQBkggSCAExKzApBglghkgBZQME
AgIEHJjImYZSlYkp6InjQZ87/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 3.1.

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

-----BEGIN PKCS12-----
MIIXoAIBAzCCFzgGCSqGSIb3DQEHAaCCFykEghclMIIXITCCBCcGCSqGSIb3DQEH
BqCCBBgwggQUAgEAMIIEDQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIe/d6
qDQ/28QCAhQGgIID4OAnlsZankpTStcSJpXiMtvB6Ol+f6XhgDJ5hOJLHyYerFHQ
6BaMiIgPQ3ycT/UwYjtIE9yo6NxHz94jCsMM74OgzUMYc1b62VChOcADCRpZ2HYy
EGfGQPUdxKuOzbeS7O9LQNrCA0/B2y+Wtu4D+dthoO84KK9916Jq87+eDrA8qXQm
sy1jVGNBA6Y1n2DWAnR4H9+Ghm0tYCcRDPhd6togL533EZ8FsbGw/eZbkojyAYGj
wNjkk+DfJcIIxIxuN4OMY9lFnqakj3OcQA5vChL/2qa+DhkDAkEwqBKDwNv6eMol
gyvLbusIOxsPc9ejLPoXn4JEURtkInN6zUr2j9OVpQzjqaJx8lSwDS04i0fmUzqi
RzaCy3CKw2VQZyEfXmtbad2fVp7yXP/Bx2R0ddeCpj604PLPe0kxPFrdCIIVIg2y
CZmjcjvJJCWehiDHsmVvKVkfmthJmoS0qRLZ4Sc2AVQZwA30zc4hFEh6hECUBmS+
v4Nlp1IOocSPLTW0nw2e/+I1+Y0nfo3wRpQMHNL5DHxhgRRa73IHKdpwY2dGOmw5
yKzJnhJAVoiTIy1CbK3Rfd7buuWTpOyL14AbFFfW9N2LP8QWYWi0m/fZs/z7MPVL
kTi63kzk7jHpOzxoy8Xzs5QlrDQlTaDrG8yqGmVTSxvvGhx243xonNja1A8TWaf4
5GBuZwEDyehmyclX+G49rz7PewVyXdJuUDgUKub+Y/RTKUh55oGpbNKNK2WLIYgH
XOQRVJa/VZJfc9IDqF9ZfPiyVCACx3tSzqeCzNW8n2bvppX68vpUT8V2FSFBVB6c
+VcBNJ5MdpatpqH0CaBOmfWmOBA8him76FSSQokuANZhI+wxGw8+mvcrJTpZnuVq
xndKasvJxpHfARrgTk8l5ijNXnxrGzWktMH3lWbhJciIPtw4DJhcO17dhoptJepS
enF+cpZXRoXY5HsiengdGpDgXP7aiWIgrdrWqr1ktzX8o94+EKeZrEU0WoWDZHo+
gCjtLUwKH6f/oyex2dWfe8ABDyjat/WZRFwf8qpJuE5vbL50VDNbLEAMgGFXPuE1
ih/sgi7ZBcSmlY704dEpS6HMVcMGoMr3NPlLUruiYZanr3eYlWMd98C+FoJwb7Ca
RdDK/Ud1Q8E1GvQi+59cTBABLANiWPVsh7rWOLo4d84dJyiDcb2LAGNLxXN2uTXH
1oadAPHVOwYSe6H1B67tlFJhivuRcS/dumTFUW4hI4HGzpq+XwnQFY/qBwjZsf5T
fIQgJ9+3wEx7w/AXk0wR0l+ITKLauH10IQFd4BEvtTOaZZIbR0Wf3RvJLaKGMIIE
DwYJKoZIhvcNAQcGoIIEADCCA/wCAQAwggP1BgkqhkiG9w0BBwEwHAYKKoZIhvcN
AQwBAzAOBAjiGuDSkfG4UwICFLWAggPIqZnFK5vMsK5cy32va9aHXHjKzzCZf/Zj

```
5gFAAl2KMJZ04AyAFR8dLJxEGHUQgDUCgQklDf0RfmfxHjIPSaNirddpb96bJnkY
0EkNIo0rsAfV4errJwZ2zItFP+h4jVMYM6FerKGP1Cs6fWf4m8SWIIJ4afGhh2wF
vnGs4weTulxxosmxli/Y/l+OxeGfhhtiCtTkiX01WcPNO5vkSsTIrZgxMcdVV8PR
Vwvf0NgY5zS55pkNVlZSmmAfm5uwZNDd4Wgdb4tC0mBLaXxmsxjSxVJsxoA94tqw
2JkNo6jqRhyKpEJ+4cAH6e3YidKX7D0V51CItVBn+0GFHrEJzFkwtiaB7GYwBebZ
kKAILCFejgzV8iC18bvIFY7cRr5fo57+0M78SM/WrqmC9zbX5boQcwcaxR3cN7ya
wGcfZzAbRv+fViALCpARgmz9HnhNZ+PjFgfX7KrbyM7+NWILfJ6F9UTuwXW2OVTR
F4+WJaXry0pMC/0YHu+3Kbdf/J6hfgEPcjmeczFprMJPuWY1aoHySAGg4a+Ngb8h
OgvhvKQvh/HTgVDsVik2TWfDAgsS0NB61c1oi9fRLwuHOaK9jeR5I9i9/ZgI6K0g
xe/LgfRfVHr5awnO4akRE4G1Uh6cxwsQU3Bt2WOeXSO9jfofTfEaw7Tax5C0mird
GANd/5B14u5goMGRk3B1XOVq8G8K970rjGu2Zh8KCz4qGgWROvK+ee33K02gNii3
qQis0ynO5b1ylpEMrOf+GegUbYm9pccduN03zEpCwNPnIY05pV95IxGCWfIcOJbt
c23RnXfqQLAlNXn4nrf9g9sxtJ6iecVjCHoJXrNhyMLy2uF2/eJaM4WWlBR95pSP
DO2u2gI0aEfCYXAN1CkhvhKpm/Zl8QHG7tXc8//U1bhWgpmx44+bXf5T4hG29HpD
Zl9r/+CkbWJofF/86FqleyFEhiZ9cMfznKuYtvegMhDsQ4z/YUU/2U0/hEhsQVpF
YtCCxcrXzXmwXfZZ3JrgYxbfRzc6UG9jhvSTR0fvKPfVW03qRC4Hxy7AjMOxbADl
GCh/NiYC+h07b3GCsHuJdRh87JyeL+x5Y1DNgcJdIzwEIetB6cKPYOX4Na2kyInk
LgAfwZGAQTHN1IXB4gbYUnfuYgzSIc07AE13sxORgrfRWL/xRW8egWyDIVkHKITJ
rM9Zzid+sjkGte3RQKTPw+wYvPAbhprlB92lxeB+gKlODVe58ZnpUALzY9+BS5Tf
EbIOJiHcjlr3vGTUBLp/xhuHpkzdaPysQDqE5vYR5uIwggOvBgkqhkiG9w0BBwag
ggOgMIIDnAIBADCCA5UGCSqGSIb3DQEHATAcBgoqhkiG9w0BDAEDMA4ECEyHXPVs
ncxTAgIUQ4CCA2ivLIdvKuViOkHRZXgcOxBJkBxK2m0tDslwbMSITMi1KvQ7NVP1
```



```
NngNw19Hsql9SHXPzSk46aalvaxH34WRNXs2GtZrWOFb5XDwuxqNcTOxGaxVsavG
X5psJ3ubC907kWykkqKIKhDjny8NkY7K1UcacWI8OY86WGgOUjryK9oCzIjVcLGa
pt1fzimZqezwx3ArSbekOUoCkDxLpPYaTbqMcogcp93yTK3SvaemkzgtKIVnVt3m
6FDrihnUifcPzSrAUqZk3UfGeaELCP4Y9oIB5Xak4o1qI9h+eR82mzEKyoFfI0Z7
FjGsDhNXoldLPFYZIDdja9ZQya7X+0AmDoTWzjTqY/efDeaD26Z7E2Tkfdp34XY/
3oDSKmggX8k48P+I1gWVTONmeIZm6i5iJs0nQJX0dsRfBgSXHvTjptejINuh8MeJ
IRiRA2YPtSqPSDAlcTC0HzEAlOMeZcKAfd/JbrXvgjK/MUDx1IRGgmUi5nKIaKpQ
YqZ8tTBvWSm86P+JhAlUH5RXZa7tnLsn3IAZ3sc7JnVmB1bIwVzNNLzZg5p4gk+c
2gvHWecLTkJLrdpESKKJX4xvLomD1x4TI+YlKpCjnbArImlO99BsDPCBliRsGx+u
OFuVWXzdgLBkz+UN+OMQs4pBhMGIFDA3Q7VrgXtbcik/LAWTECEhTR8Jf/d0xeaz
+d3e+VA7lZlyELr4pBlqelHD89a+8UtHPGR1esw3EID4h5nt1oP2S8nGGcyYwd4b
sX7AAXV4sozPIjSsyG1I9N7QYCY7b+Cyrdvy4JSGVa7vz+7q8IHs9K40lG1kKUv9
p7Y/w0vdfPWhT6+NZvlXsQknYBR3+IPXlHDsqwNB8oYA8xtYsy3SzBi+BZyLIiDa
SkeJ6RNxbjYIRBqPckCW6XmI02unKbiD0E2z919GjtI10hx6dzgdhAEDnzTJ0NYA
vT+v4W2dXDTmZeJD2EYb9r2GFFUErYsEKzBgRv21HmJlZMjk7lM+XbirRoSJb715
VrH+bRdYnBAOEiIamsND3wIq/LoZ4O/wQqeSY9eaza7qEtVzZ8d+r7qqCQkl8lQG
iC7Ce/VzaSZ8823m9LoMw2AX8Us/bdT5kR60w+WMYPrq5tky9XYLILuTh1bwTSps
AO4NH42IhpH2Tg+mmaS6M2MQzDCCBZgGCSqGSIb3DQEHAaCCBYkEggWFMIIFgTCC
BX0GCyqGSIb3DQEMCgECoIIFLjCCBSowHAYKKoZIhvcNAQwBAzAOBAiO/0ICbTbZ
```

```
LQICFOwEggUIFwT/JI8UjJQPfYTFonJEo8zEbpYWXKboqw6/zZsMGmAnUPgQNQDx
yuLVprs5jUc437kVB2M3F0x8DjmEppebtHfIoyjoXF7jdnA4EF38tsso0K1nMPmS
gl02iYZtOqsOvBpfeO5Hj4Ovhi26J9PzTwPcgl3QQPqfWv7CwgGVn4/hntBAriPS
E4gAlfAcqkxtJBm01QwDoAdsOKOMsYntgWajpr1J3Hm+34NPL04Usf1OpcesPUJ4
CBxNyLXxjjsOzD78WVvKY+N+j89xTsytz5Y0fEkFqrcl8pgBQxH72jBwSCm5YwHz
3BhWQgr2bpWJ1f2LWcVsnrN9tx6RhQtAAkcyNgX/ksp5EW4JTo+o6oXLRhXIYauR
rUrisMY++b8ZJTp6C1t0RW2QdqgMZghSZgaW6FSC6Dy2Dd/ezdkYUCgiEtq8eSxF
/8WDw6Va2iGVSNt4/p/OJ97yN5yOJ0K1g0hATebU+I3E74PQ9RK84FfJvyHDBC6f
vYZW/ouMcgp3YmAF+dTm74Hq88X4daV+/UPYf/cVpyiwcBTg6H3jrkrs0yKoWLIf
rIvMNBeeKZ+fl2Enw1MFzkLI4VGD/UeRwrbhN0SHkh5lIGtu0yRTfq6msYQpkw+j
r7QwJIdQyrAoaaVaRotVyvgTOLlHw8r6o7v36yoNov3kDPW7DfbSVTWX5lIyQn8N
qMwa4N1clWT8ukfZXSaYykFSqF3w5zala4iIhu03GjDcfiWLMUlYVAUcvSmcIULE
1oW7FKiJc8OadeIu0JBySRSEvf7B3w8leYUs+u/h1ptrZZKhe1JdAtlszvHJ0DD0
kMqA6Ig4yomscGSol/sRUqpecIQwVZTCRRq9dJOFJkKhKD5Eo9E0Z2snp01fpUF5
qlMeBjpYgkX7jhyFyvq+qDqBAY8izvkcruE69WooBVyorqKHURjWtY+rhzcB4+HL
72wZKzLnY3iUjJ1UANxM8mC9fpD1NJt/7epqzPyZ2Kd4GJVYi8sQpFKf4tRHDr0t
I5iUB78qj1EBp1w4qvRn/jC4ii7+Bas8mz/AJ25QeviC44Vj+eT2YYXafDivrmoe
BuVMIBbD066YnuBC2CeKydNWdiARzc3IfhcuhVwq7riotYfyDqd4e0Jy7Y57pbwv
4Qwz1yCxRjSwiFQ7/fRa2Cx8xtxKcC/A4LGnXAKISy+uNbDWA7AYaP6RmGgMCaNi
Xy3F1zvxnE3bv68tXRF9vjuEChUq56N6992qhoBuHP0J/mRItw+JoI4m/OFnEUGT
3bNyxpEFyA7aXBE91aQdSXl4a97nC0/RSFH/fRwPFYgxr3XdCIf3Cw5PDs25YNsX
WCsDCVejWMFrwOzmDwa8sBkY270+rGv76qXvb/uGD3M2C+DySVy55Zd42wjghSez
gY6taT0tqKfLOS6Vl4ELU78Q6va2o8MlcUdi343tOi60MZgCDUwPP8TjKZINh8u1
KNhzgpwNLz1gE0dd200l3bbzdZ6uio3R52WQWRCk17Z9lUesCJavytcAi0mMefMx
BPMOdnUi6O8TPDRA0mcohbE5rybwDXAoB/VUbwgM0/qCpZ7VcSKN1lUuoe9+Kho0
NK/gyMEvntMxGNNI8arV8UkeFollPhrtumvdwqbVCeN8TBj5vXo6Hu+eKB7AVwjB
k/rRHpZxnnVGXbm8HzM+kjib2cY1diusVRJ/1+Q9GXuo135tQbobgcMzAmqAqZp9
kDE8MBUGCSqGSIb3DQEJFDEIHgYAYgBvAGIwIwYJKoZIhvcNAQkVMRYEFEqzrDFT
AkmcTeNueeAlYZU+iGIlMIIFkAYJKoZIhvcNAQcBoIIFgQSCBX0wggV5MIIFdQYL
```



```
KoZIhvcNAQwKAQKgggUmMIIFIjAcBgoqhkiG9w0BDAEDMA4ECCNi2K1bMEiBAgIU
dgSCBQDLIXo4ExcyE8+4aiZIj/Wnh/SVVVR0n7s4PGCbXt+VrOHd9YzTuUicAqIc
HH62dv7NSy+fgqZG7SmVR1IodadFe+5usAzXoyyhhEe2c+ToeVbr5rs+vBvQUyh6
X5XTV5QVOAkwSyKGjyfdy86x1Q8cL2D2BM+Rpkm1cFtjgWcB46U6S6w50sG7XOKS
CMI4a6rnHPVgPPdXMrj3VSPJY8bhBqEDPVTnfSHf/wKZrIi54O3F33B5jt6Cm9+9
m9Fed8n+81w59rRom72CY9Xii/ULER9THwjxOZOQ+dIml23KauwexuOGjii0UR8M
eM/A0n7UNys+bZTulgdpWW/mDhJ+eLATnhJw5ro/AWa6YVXG+t5k9LjdJ1ZmqS4b
JxvBwilpEGoh0MM6Yp0dr1XM4mT/E0JMWD458Ngs05CuCpwAUXGdQmgrVsFrrV0H
TyHeVLDhe43J3GI6HCWJVOeDQzzmaO3AM+IooRDkTHnJMaxUXphKTag5+f/smNYE
hzVjZeIc8GFZ36eSI4BNGHSXFACwLu2ThkzpXMmg50JAUhBYxqE/fVevLUH4JPLg
z869wk8gRlUBo6ihQGrnsx7ZO5IsYahEYjz0N05PVPJYMLSyMovG9i+LpzQ49gIB
zPu2fdLR41u5n5O5mG1Y4aJ7OCJxMORYhWHuctHdGdpJsgiq8+1iiUwmfyCfb0ZL
```

```
3ePMU+W0zkAsyn22aK8jDBLLVZlvOZIVqR3Gx4QFPSk6qCMQ0E58VkMUMxYvClzT
wSeEMu66eND/AKTE+XXV/d9bmSmWGk7Y8XrDKLKfmRdrlIeondVJv5mk12YKxBPQ
GeUqK5XJUa2dzH9zvfEX8iYzdt4281QCiXJ3qwmbT+8RoOLBt4KyOs2e2ZSZnjrL
9OO4oUsHIOyEfjwnWoLhKbkmun8GJxoB2yCzTawVQf9/qIUXaSzcp23AV6Lf1k9O
f79HYPW3cQJAtjf6XBVE1xVZPkfTuC3yVLufljs2ed/ctpHg9nuId/xHFH7t4Hbm
U3/ZufE1GHnsRQ3kbnqA5WXerd9UzeoDaVDjFXGrITp8env08GXYvwWGXLL150l0
DuJSv1E+1yww86SNjBYUTx0r0CJjjTk27vIUhAYUEA+J71IeifqqPDKYXnrCdUEa
jbfEdek30WiLR+ChEvEp48Mla6UVTLm/mjziwbsxm5QlGccmz13e32RiyrfseB+R
yllmzeJtydP2IHkWK7pww9yOlPK0QtZs66IGZKqeXrWBk9QFYDX42gAy/xTfglco
4KO7akhp3UzTIQyTXnt+OsOScc+ArVm/dwClm+ZxybtOcVyadjpKWydyfAr3aTkG
xX6RmHrEWr1R9BnMGPYesDs+yeVNs1QdDhff/bQLwCLXdGLWwLe6kitUiyi8F3bd
fPjR7R61lEUvJrBm7YLmgdxRCJ02LFLGn09iSMNe5vmiNaKiuzfb4Dp9dqEMhmJf
dsTURagfJIyqULoe08EIIozahivbzoWVA6oPAkk2D8DnTiMegX4IZ/Zb3LPxJKAe
XO3Ys1YQrNSNZ3B2ZISBapzGzhFZfRVzPOmXhN53pDhlxkw0btkKblYA9CvP+kzg
wekzCy/Mlq/HbO38CV1NKzay3yg4ntehJ+v9/k7gaqKmo3ZWMGk0WGBv/GFxYhme
Nd14Y65D9TlypM/zrXSyGoOqZgSA6HlAgogzwwSaGwx9n/o6czE8MBUGCSqGSIb3
DQEJFDEIHgYAYgBvAGIwIwYJKoZIhvcNAQkVMRYEFBfFhHvQp+92kDi4s28IvJK1
niuUMF8wTzALBglghkgBZQMEAgMEQESULk1nPh/xbTET83QqxpxbEpCxkvY1zrpc
aWzzbehThKle6bJRDM3zlpr0dHs8Qxs3ocSpAQ1XOXjuXlqFfKsECJ1vqXe6ro0F
AgIoAA==
-----END PKCS12-----
```

6. 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.

7. IANA Considerations

IANA has nothing to do for this document.

8. 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"

8.1. Document History

8.1.1. Substantive Changes from -04 to -05

* PEM blobs are now "sourcecode", not "artwork"

8.1.2. Substantive Changes from -03 to -04

* Describe deterministic key generation

* label PEM blobs with filenames in XML

8.1.3. Substantive Changes from -02 to -03

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

8.1.4. Substantive Changes from -01 to -02

* PKCS#12 objects are deliberately locked with simple passphrases

8.1.5. Substantive Changes from -00 to -01

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

* set keyEncipherment keyUsage flag instead of dataEncipherment in EE certs

9. 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.

10. References

10.1. 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>.

[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>.

10.2. 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>.

[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>.

Author's Address

Daniel Kahn Gillmor
American Civil Liberties Union
125 Broad St.
New York, NY, 10004
United States of America

Email: dkg@fifthhorseman.net