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 24 May 2020.

Copyright Notice

Copyright (c) 2019 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
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
3. Example Certificate Authority
   3.1. Certificate Authority Certificate
   3.2. Certificate Authority Secret Key
4. Alice's Sample
   4.1. Alice's End-Entity Certificate
   4.2. Alice's Private Key Material
   4.3. PKCS12 Object for Alice
5. Bob's Sample
   5.1. Bob's End-Entity Certificate
   5.2. Bob's Private Key Material
   5.3. PKCS12 Object for Bob
6. Security Considerations
7. IANA Considerations
8. Document Considerations
   8.1. Document History
      8.1.1. Substantive Changes from -00 to -01
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.

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 keys are not suitable for verifying interoperable password protection schemes, or for MUAs that require passwords on their PKCS#12 [RFC7292] cryptographic objects.

3. Example Certificate Authority

The example Certificate Authority has the following information:

- **Name:** Sample LAMPS Certificate Authority

### 3.1. Certificate Authority Certificate

```plaintext
-----BEGIN CERTIFICATE-----
MIIDLTCCAhkgAwIBAgIUULXcNXG12bZp38sV7cF6Vc0fnKDwwDQYJKoZIhvcNAQEN
BQAwLTErMCKGa1UEAxMiU2FtcgXlIEBTVBTIElnRnZmijYXRlIEF1dGhvcml0eTaAgFw
w8OTExMjAwNjU0MTthaGASyMDUyMDkyNzA2NTQxOFowLTErMCKGa1UEAxMiU2FtcgXlIE
BTVBTIElnRnZmijYXRlIEF1dGhvcml0eTECASIwDQYJKoZIhvcNAQELBQQgPAAoCAQEAg
AQgMBQowGgYDVQQDEw5Qcm9jdXJlIERhdmlzaXMgRGlnaHRzIENBMB8GA1UdDwEB/wQF
MRMwEwYDVQQDDA5Qcm9jdXJlIEluc3Rvcnk=
-----END CERTIFICATE-----
```
3.2. Certificate Authority Secret Key

-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxR9nz41hKHqHfrNBxcGjkHp+JwBwEnV/dovHl3xBcHzd4e/xoNFZD24m8mlRCZUufPH3r387/Mj35SUMx1k2qtrXgH6DFscmCiraHBE1EIj17n+a/0+9v2v0Vmxz+YiKCDM/veSi56LraPUQXL/981uiKGRVLesDB6r58jyokd1Yf1zZpfr3A4/R4278dOIN1LPgyv/HyMvYbBCCPW+5vSClHngyE3yqv0bIQr4ydRBbmeY3UU5X6dUUdK2271i4X76p/+2RO0Lz395dqF86fbRJ1N5mgqQIrrkgsRF70NnxoWn/wTRpY2V1H000KyNy6h+e+Zxuf9gIjVj4QIDAQABAbOA1BAQC6LWFU7lKZPDEA/7lDV/huGpNPxU6B7rlGelDl7lZ8B219w6PdHPPCrLohPY3guVL794AM5sevJ1XrV16GfpW2s2j58kKuK0+GL7M2J11i63m4dnNIGN52Vu7dXe0hrcDTQ5w4dJV++pPo2r9d7uAoOL99glcw/NJq3JfYwSppFhdjffzFrirUwLpq9R0Ysvst/EEc0q5W0z8eM0syGj0aRsJpv8hIq6e/0dDFTR4qua3BP0RksbETRNUk7ld2i019huzKThNzl1lxMpvypYRCkmM8CIvzv0iScBmio/5YpShP3PVb1292v5XDs/A9Yn5b46hjEX45mmHTqAz/JAoGBAN7ayderxL4C0jm8aif3wMazXetuU8dU0jeYanYCNl+R6dxtBSIKA770caDfd7wwmBdqEBiq1HYU0po3ouXi6r3wWNeZvpR35vObS9TFr0MQys1KvWAgroB7mSUG1I1/jTpuEqwn+VbXTN2Dz2bULj9U0eOgdxBqNCkbbAoGBAOJw3r2tQNGBa2TVkm5jfIv0909FaypdpqMujSkbL1IgfU2WulYwBht9ysJdeAhv7jk8LBIifiXYbXk/qc+1CcO579qU5x44lV/KiP4FcZ3kGMYm2rldTa+J90gtIKdHvZKVz6a5oxqxybgyCtN+yDcXCTBgcCpZ0CkZjIbZaG0BAPJdJ12JRU2fc616equZU8GT6Nrh+f6RhGpqACpV91uz0DpE999GZzUEDFCp6D5jlmCp1txSrp65Q9tQ0Hkpeh5P1Tj4M772bntNhcGkCshrlrvHtYNrUItkKTY4KeSHxM5PX0I20l+IHKM/0x4kktj33at1I6CkTvIxWb71PAoGACVti0Mrn99RhON5VbbAb1a684+yDhft8ONqHyaoRopa0y97JNYy5HD2ba5UddfjLavCoIWdcdvuZ65yop5017pULcv94p9G36mFgD7881thaaA4j8u+FeWo140pVLYG34v0nFubQ1k scent1kBy1jzLD982wMdf5Wqad+kCqYEajXGkzrFD71D6q805kwPz0lV8unMMsVn3U5Fb5MS/f/ubTtYFoHylt5E/YhHpryr8ZsTGJWGNv286jRPr41Cvhd22QDrv1tudNooAQAeY93nSXYDg6u+bjPx0lNL4KcF+B5kwXW0BZNnwxj6SSSf6XQVMc04LUIZBOyo=
-----END RSA PRIVATE KEY-----

4. Alice's Sample

Alice has the following information:

- Name: Alice Lovelace
- E-mail Address: alice@smime.example
4.1. Alice's End-Entity Certificate

-----BEGIN CERTIFICATE-----
MIIDbjCCAlagAwIBAgIUZ4K0WXNSS8H0cUCzavD9EYqqTAswDQYJKoZIhvcNAQEN
BQAwLTErMcMgwIwYKCIhMCQwMwYIKwYBBAHjqtAHBMlFMAOoGBQAwMDQEXzAJBgNV
BAMMERQXzAJBgNVBAMMD3JvcmwNCzAJBgNVBBcNCzAxBgNVBAoMEkF1dGhvcml0eTAg
MDIwNTEyMDk2MDEyNTQxMDA0MDAxMzU1MDEzODY4MDAxMDA0MDAxMB8GA1UEAwwBMwEg
AQIwDQYJKoZIhvcNAQELBQAwHjELMRAoIBAQD7q35dG2JaazzJGNZDZ9sV7AKh0h1lRf
oFjTZN5m4RegQoYSyag43ouW1lXRN0avf0UTUREjK04Q9dV7GzCACAoEKGy/xiNUOsiff
XzbCubln3fZM0XShhKKBQThlK755jA9Czkg7ejGo1Y/iidk0e91neK30SCCaBTJlfR22
DrPK73IPmeksotTatTF9hw9dDA+/HllypTn/a6Q/s91cfrxwry22zQxjwQpMjZmgj18a
9cawWgRycgfhmA0V1uQLlwoBY8DAVxv+nGgabqyjG0MthIK0Gn5+ofwXXUM/zbU+g6+
1I5doXXRRFtq2GzbIqKAHZZ0m+BbnFrhAgMBAAAGjzCwzQwDAYDVR0TA8Ow==
BAAAAkNVHREEFzAVgRNhbgJgtJUBzWltZS5tLeGftcGxMBMGMA1udJQ0MMMAoGCCsGAs
UFBwMEMA8GA1udDwEB/wQFAwMAHwQYDVQQIEA9tcmVjb21ibGljaGFuZ3V0MB4X
AQIBA9ggHMA0GCSqGSIb3DQEBCwUAMAwGA1UdDwEB/wQFADAOAwDAYF8aJRs6Cyu
JbEYVR0lBBBwFgZ3JhcgOg==-----END CERTIFICATE-----
4.2. Alice's Private Key Material

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAw+6t+WXRTi0MBsRiyWQ2fbFfewCodIZUX6BY02Te2uEXoEAGEs
mo0G6lOtocuTvdGr39FE2K81yt0kkxVexswqAqBCqv8YjVRdr13y8V2wrn5Td3TDL
w71Sisigak4ZSU+uawvPQ8y03oxuimP4onZNHVdZ31t9EgmmpuyUzXOdmm6Z6509yDzH
plMaEz2XxyFCXQofPvxt4qcbtf2htEP7PyNbaa8+stsoF71KD5oz3yTYIdgq/IXgs
1lyEAoAH5YzNGFdbkJdckG2FPAwFcvZ/vhoGm6oxkxKDMrfY5CtbP+f9qH8MV11DP82
1po0vts5EaF8UJRbaths2yKpAB2WUJvqw5xa4Q1DAQABAoIAA7AVrwiU4i1LDwGq
EHjFrdRXJ5X5D+dzejMTHkkx11MNBs5l3NCPs0fcf98+pmmmYRKXx1qq3qfzszS2/zR
pp2DUEJ9+82ZK9H0n7DwrRsJb/mYS6GwCMHHM3WT4wLM19ocKCY4rEksH4AT7jJQ08t
dPtWadqP7rcmHCMXyn143HdScCIB95rPkJxHyFLGThRe0og2Nsm7eShjov
7WkMuESKku0HFLPUw5FyLEzhJ4ar8ZI7qYbt7X6IamX0f9aTMDPAlrQcix4+4Koa
zF3cNY1xqx/yItvs6yoynTStwi13i46PwzMwf845Eayunr8ge6F3hW77ndjWxQ
Jg/qAAEcqYEA3SLl02tGdB5qWHzwzZAnTraining1Mt7MejKMRTRDAi
5V0dpSXrFvTaT5r8qwU9yFEm+0uB6k52CVbTE1Fp961lbzYjZnKaNl50G8+HSLdtn
1vj1XyCRGDKJ38Ga2pZp+RvWbp64499WSpqumXMiQ8mJfekgTeh6rECgYEAttkM
Da3tFEEyV9Z5xZV9mp9dhE7kmVQnr2pvt2YfJTLiKnS02kkj/qKoMiPhS8Z0OQJ
J90bDngq15o1/OQi+hwYRmckCRCvfnfEUeq3v+3BFQYPDfwKtgiBu5TDGmJmFA2t
l+235wCwpCfjPh5frk8GTQ01s1hRXY3d1NPBBhEOcgYAOjSegN9H2a1vUKFkNrtIo
kXrucURTu4Me8lxvKVDOT+UKhEBCNtmPWEACucuteZtm1mMS4Yks3MTazMUsMgJs1
izpE7ow8RTMyg6/0LA5amwEaZAT5Ys+0o3MqSQTkD+wULW3xmm5zpTZenBE2PpqVmn
/G94VgsGb/XAXBynEzt8AQKbgDh356t+9Yf7KYT5jtqU5P6km6+qL5HjDv/t
rK138B6vMkxBMmRb2EZjd1/9vNS+y5Es/s3kyuxYJIdFvV4T1QzAn5nJABraC0Ff
im8KvXn5v5N3f7mAm+Z/9JYNt89/vbZIqoramGmyTwDHS5fKJNDe1cq65RJPbU1
73s5BAoGAdqDE0K1sW/e0gptb97fBFNQrUm5suctUiaV1mwiU1wuxyVVD8z9xh
9G0s7HfFZVz20rXhFOVQEPgh1nDwvfuSHG2q74DpPy53oEnrK4blQhX1tZ
pU5Pj7MErNQeAXldTPVzq4TrYq95LDMaflqClmUZ0DnuAy19dc=
-----END RSA PRIVATE KEY-----
```

4.3. PKCS12 Object for Alice

This PKCS12 ([RFC7292]) object contains the same information as presented in Section 4.1, Section 4.2, and Section 3.1.
5. Bob's Sample

Bob has the following information:

- **Name:** Bob Babbage
- **E-mail Address:** bob@smime.example

5.1. Bob's End-Entity Certificate

```
-----BEGIN CERTIFICATE-----
MIIDaTCCAlGgAwIBAgIUIlPuMG0CCx8CzfXJwT4633mmG8lwDQYJKoZIhvcNAQEN
BQAwTEMRcMkA1UEAUEMu2UtPZct6ILxETBTVTENcnRzp2plyXRYLIEF1dGhcwcm0
eTaFgf9W6xO7ExMhBwNjU0THaGAy4MgY1MzQ2NzQ0X0owFjEUMBIGA1UEAxMl
Qm9iIEJhYmJhZ2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDCZjlu
Li0rpoCsq2s8SHqB910IPPSdfzaIj/G61IhUnfawEX9zLiMywPRP50wqwVRJ
X5og0KstyH9s3a50pNnXo80JU7IeRQlwxq5f7LmM88RdvSP51p07p0fx++2
MzV4AaJWuUly2j998CMmxh/CHjBKI/-+21v5TmZFGmeTqxxHONbd2zQqGy9r/
LBAhjJwL+1t90sn1jEOFKLws6ZUx3xwmc+axXrteE05IrIpKZcbn407IlpyDr
y1NK8hX890nwrO1SdpIAd1p71ZDBdlLd866ZQGBP/mhWUnjMHOy3s3uBkT73RU
W6radBf8m4Ah04OETa4mBQAIAqIzLw4IzDYVR7TAQH/BAIwADAsgNVHREEFTAT
grFib2JAc12p1bWuXhhbX7BtATBqTBNVHUEDDAk6gBgBEF80CBDAPb2NVHV08B
Af8EBEBQQD6AAMBAGA1uuDgrBWBBOkRA06j0kN4Z7pXZmTThZgAoaZdCBhBNVSME
GDAwBqS3Iku2zq9ssN6Wqzz1LPf3gKJ32zANBkgkhiI9gw6BA00FAAAOCAeAa/T
ZPgDmLc77zbn5bc1CTXNh8Q8hECGMha4ISWCDZMsNjezDMMnZM3s08QOuZVx4
ey61dCLteneK2Bncwsx039n8n8UDPT5Y5sbxwEHpwKev41RLIPO2FSH3dCDKSY
HDSX3JeECOp1awKxtRs06C35g4EEL0K2M0wlw1u95f0+rCq+vYndS9NzFyS3bJ
MI37gNYy8hkr2zvtPVJ40myYNQmQhdNoYnrr56LOuFMMGMYXBEw06L/kzCcy
YxxyCy71lnB0WLCj40mRmDwDJMRDV+mgLmTNNn8mPltqU9gE3KNyRCST9v2kk+
N+cfxLhC0aHFPL58g==------END CERTIFICATE-----
```
5.2. Bob's Private Key Material

-----BEGIN RSA PRIVATE KEY-----
MIIeAIBAAKCAQEAvm5b4tN6KeArKrPEh6m+uDZ+w3X832iYPxutZRlIX2rxF/2Z2bMx0Dx0MksFi5v+XVYnJerch/bPSWUq+faT51/KCse1xKJssjxKyt5ySe5UZjPAAw70j+eY+jn8fjvjtYjH1OL0lOglGmt0/ff0AjJlx/w4wSVs/SHb6k5sxVRpnK6scRzw3d3szq0MkJy/yWwhKw4FfprY/UPtpyIXEBSpv0r2Zzd18inevNQMa7a
RDuayKSmXG5+NHK9agc6a8apT7P1zd/dJ8Kz1iEqZQcde9w9Q3S5y3Fh0qMqR754h
8E1J45h9KMT97gbpE+9OFUqZq2pMD0DA0IUBEwIDAQAABQao1BaAvQ1cAmXC99ND4
KQP8776H2HZC35a3Ji/NvIISBYJiLSVvaa22ocZ7k7FP0T1pZTOA0DDZV7WCKSD
LfNiPhLNOX/LM0i75kVFpXym5fRi0W33mz0kgkF3Y/L2KicaogPfF9-zTu/T5-su
r1J4d4kRFG0fwP3Rf+jgq9FDEsnWsuU7fNS52vCnd0Q4G1t0Zr50msZIyX9H8rn5r5Stro
Dsk9C0jyjmCtU7X340KDavJRL1sx+4yIbPTyuKF2nbnJ5wfsYhUIOTG4xG6mIY9
z6bWjux7H7nNRKrtQ144aE8XV56Sc+J5ulwaIj/F+eDZVfpVqixQy6a6j1ojPv7u
rx7cIQEcQYEA9ovq0i/0YdDNQTJXB4LNMtS1WLxqrpzE/SNPV5kXnQf6yf6rrkZ3
+l/r6w20pr4PY+3/igMoBZcN7YgIM9Drkg6bDLrZ354A9dZLDBNAgCnDR0yY87
U3f2ljjPC2ZrahYHksMxtz3wU3so2990YgjNWLaL7LrXvpaECqYEaydpnfwzxffffffGILb4xiiFpJYs604auZ3/s/y9W3v8LSKrytHHOPQ0g3GALvQ+iAy
LWRBiAJtEue61IYlnZl2+wvKzZ2PGB21/JX5MI3x7AcRP/1/myuhwN3GyF7Ppg
6zRE45dZPfm9nklylw4+y17ub0dOVNyxIfBmDxpcMqYAHQb1F6HIZ0sjwBhZiS06W
kaJ6r/uxx9F8jPld644+45j1ndeNU1cem119T26s7wrc1kXYytdHi+jzdG/0rEuke
UMpq4EPFggkfoAhPlixCH0BmfwYVMCEEd6MMyypJwJiS6luiEdMx/LPfC1CL
r1fHLQg0Jr4MrnfzoQnyAKkBqC6WTzyPv8MyinA/4jdL3zbuTaqYQK98CU7o
YGFRbnw9Rq/qC3FJR3qpuwN9e4+n542ZC1v12ncnv6XMLj1P8wdr/LGNTvGvNHv
xYVbsBZ5gQZcNhnuYbHrP62hYQdHv/SB796e6aAVBvZ9p74x6Gxq11mQe2Cxc6
EEZtMwKBqQDqjWtmtDK85AGQgUIB700B/CXB39J8a780wywpX+Yy1bmg+n3aDyYJ
8VVtHwN0b3wMs1d1jxyVavgyKd31K1jn/PIB/IWFrFwQEqDXmBROwwRBDbpvfFJ3h4
Jk+jLbvxHNhwo9KltCvZGpZLy5fsC1tLuodBMNjxUX9u04bTqy/g==
-----END RSA PRIVATE KEY-----

5.3. PKCS12 Object for Bob

This PKCS12 ([RFC7292]) object contains the same information as presented in Section 5.1, Section 5.2, and Section 3.1.
-----BEGIN PKCS12-----
MIINuB1AzCDVEg5CsqG51b3DQEAaCdUU5Eg0+M1INOjCBCCGC5qG51b3DQEhBqC5BBAgw9QAoEAMiEwDQ0kZi=HvhNCADQwBDA5OQMawDg0IyZsWw8h7V7wCAh3r/sGID4E1/66Kqzr6wz4v0nKv5tjE06epiyJP0fYLafLzAQyFkYNo6vTE jr7l/5799bh2ZpDmd3DQj6fwsMwK1CRUc8T7py40g/3JNzTm1sWZr3JgjG9M0OLEwXnLwLrRvp5H1WFXGhiKcmwTm9b870n2970xjm8TPAvJ mlPuveyeCB26iFpvrnobaAxah1FvEmXGWgVhlcKp01GyHywVUBa350qbeQIESt p69kd/nlvw44us40x95EzFyaA4tKUICF1J29Rcb6+N51cQj4+g/08b9I2xv9lo k539x/nghGcCl/PnCmDnLqQ2b5u2wYyX4GRklkAaR+7+8h51pg5fTD5h8VBT wo2Q0fPvMNnMIPfF5XKv68aPoIfSrqzD1t7tLvl8iRvDvqjLA040pvYytfj1HPhMn uXwXwXjB27vDnL4JDwpaj5R1soBkgZw8JuarU11L40E3y8ca6agbLWMqcmGr ix29pbyb5/cYoel5JwyWp9yPQdf0+t9PH91nDMa3lx1hnrwCsk1j1hLqRmWkDE uKSAMUW16d1iyyQ2nQmiKULLyDx11CzaUPNjSi5vooXW/0QGdeb6T0ykwada81ame jhvr9b8Afj1IRZ/G50ULCcRq/iC9jE2qu3ylXVQW0MC+4xPkYMU0K98r8sFlcF dRnQbAqBp0fSd6mBYo8GK7s6dWmN65yGRE6yYzryVicC+QeAzV5N55kk8d8USlS MS57s/y47EaiCpa0lzClRo0hNPELsrjsyFSS6GpPOj4+EcOq0qj8B3JQ3P3RdL yr9FlowVGhikdH1R7geFgUwzdBBeEjKnhUqPif7PhcsNLOzVzULDdCTKg8KpG8T9 N1JlnMrxbBYYc6ElGhcHb1Hyuwdw8vB1J1an/a27zGy+FYv5QgZK6+g2o6qHgcycyP+F2s5QdoNtCujz8s1oL5o5uGg72JFqDcDggJBUc8ttxVMQpm 2pwBEyEBBwB7gJ0w8hDcJhgsB2XIKi1c9lWN3DPJPJt0lCrjJYra2/6FCOC+ 813nandaiYZuc074dytQVULljymo0UcPKK6wzQ30/qjA232CZI2Q5z/S/c4yefv Z+j3529zpqnPh4lCJt7Hlcqf51swHmo5c4e4WdMrbksaIN5lQ3tx6c9u2yM yGuccA5MmRsF51dFy+L8atA8V8hMzGasRvXy8vtxDd5qP0vTF8HajhKMIIDv rWjKY0ZhcInC0o1DODCA5wCAAQAGw5QG0BQgkhkiG9w80BWEBwHAYKkoZiHvnc AQPwvAAOBAIBXCQxXTji1GFCAGqNomRtKzKEFruatcbbz5pKakWste4bq96y zhB+56egj/XPsi9MlJw9+E2Wn08ByfDpcfRSPHPHYhyhYWJ04X1anP9B8EdDCKnqP bKAwqylOQTRsnaff6yic1juZ156wNssBiirDwMGKqZkrBzIDKvHn/Tu5jrujDQAQP 9T83P0g+4Cahyl3sBj5t7883oT3dC5LZwiRjB5fZaul/A8Exm59K6W6e/a8XudCI 8Z8G1p+q1AzUcuqAtPhm8U9A/ybWnOB80s0s9XtdChtBhnt9/hEtcEyl1DNRF NNNmDswmNq8DB9kkdpeKePYyZmazj/jbesAWJv/WdTBnkqDYZuqf1lulYw 01x0w/MJmTVCvKzqpxa6LAIMlbKCywbf+mUjdfDLy063mU67wzge3HfHuQX Z+4mNnScIQ6i6uVRUsA181CkCyD1R4e1eiQaBpjqsXyUAXqgirVcJ4yeUbleFLmY ooczX4hikaZow17q77ycCFC8gnd2xP8msrn+rIstHtnaXwqlkK055mlLzeBbzn 8fbuf7tm5zFqH/gik5ESelCdq2zq7vq6gbzty37q6Oq9x gestionever1qImY0ePBF+B20Lkm9av iwPllbzn6mB2yq6/0q88Yw7dC0jR6LJt5eHBOgG7Uo2x/4dXwv6y3hKu9K7m6oZPlgD 52FQ7x23F55dGj84Cgcn4fU1s3e4Fs3aj983oX0zklG787l/m/Grn3y8uEB1 515+ELC1/4nIAbX1qjK+3Azw80U0d+OpYryrzrD2gzgk0hCdhcsPtympTMW0rdtJw k6qDfuecardS7Jy+ZmV3mYKn0IjA1IVQRQ6E4dwa+m4t4kH3agHa ku0XH06/abo3 Wq83sM2Z4n+m39aGx8yBwpwZ99M39D9ojP+25u5787a1x2e0bmaunoaQjVhk0yKEy NDhBzh0yi1iVI1PD11/TAzZyc1KSm8C0BM8WYyKB8Pf+edTftx17wU70PHVwlfAlWwz chHrMMyTeA7/wL7Mo979tM0y18atB08+SuHFDHS9XLYd0X1dMPa8S5R5t6L6 LTKC5M6K2tF6g6s1Nqih8q/yMKyTnnLkNq5DMqZ7/n0ycOZeQQZ+nkk3aB3a7vhf8s6x4 6CeYk1hDd402u1dpaIaqsMuSaFsdHSrHT1i1+A4o4LcssgwVYBkqhkkiG9w80BWbGwq ygbYVJRFTRFCBUCWegwU9gbsbqikIgkw80BDADaQCB00QwTQmBwCBGqiS5DQXk AOMgwDQ0QyPIwEdCwAm6CAbRBIIEEEryDKQLnI9ac68GK7TFU6QLMmASTe2bOdTTFs9FM 1/1FFMKqNSsBPwBpOuBoUwrouEugTF/g19D0zzFjnp0GMS2Y3I1e/gd4IAYGDSYuKc y9zq7xRgn/G/1yjgbseq6yqby8j1/yll1EdzsEaq6r7Rrdjgk/J51v5f45LAB/mPatC 7VURjV7pqNkAnQnG5jv5Z2n4FejKe3e8+dlb+xq0+8rjPP00QxGMLyRELAEHaEwWd 3cLe3Yqji/1/i+jC3cC0c0s3a3PtrkwaAKS1h0K7izLyUuMdoQaEd3Jvlgs9 nvA51j0y8xwVp0EdJspwIyAbm4zB2mgb4iFlN5rBogYtza2hOgby+uMeEl5n BkfDw2pKmdwIa9ryB9nwaA30D0YhyJ346+2w6Mn058ybCvFBsSNvSVP 1qiaULUS5w+rr7T3d0vpK/HQ155zpsrjP9co9IRn9R+xteuwpDA54lPsrdYjpz KBzmn7f3/3BJmuy15SB7qtGnxKzm52IZV5rYrBsh2M3M1T9g/eg2J753V30E5kehR WwNPBsvgvAe2dSML1stC0eBxava4gmb+0Xx6b00BFtFCwz1slr9gqWAwVAx/bq5lSM Wc2Ibubbst7QOwq50KmnnbXJNurk1yDYMouDFkQck7c+t8foeYTA9r2FgRasfdn1 irTdd1k3oyaproSnialzoJ9cv9+9feLSaegTFFtTdfnvW0A1AKw95sttN/Smplj9xv6
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 -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.

10. References

10.1. Normative References


10.2. Informative References


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