Workgroup:	lamps
Internet-Draft:	draft-dkg-lamps-samples-02
Published:	24 December 2019
Intended Status:	Informational
Expires:	26 June 2020
Author:	D.K. Gillmor *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

Copyright Notice

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.

3. Example Certificate Authority

The example Certificate Authority has the following information:

- Name: `Sample LAMPS Certificate Authority`

3.1. Certificate Authority Certificate

```
-----BEGIN CERTIFICATE-----
MIIDLTCCAhWgAwIBAgIULXcNXGI2bZp38sV7cF6VcQfnKDwwDQYJKoZIhvcNAQEN
BQAwLTErMCkGA1UEAxMiU2FtcGxlIExBTVBTIENlcnRpZmljYXRlIEF1dGhvcml0
eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowLTErMCkGA1UEAxMi
U2FtcGxlIExBTVBTIENlcnRpZmljYXRlIEF1dGhvcml0eTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMUfZ8+NYSh6h36zQcXBo5B6ficAcBJ1f3aLxyN8
QXB83XuP8aDRWQ9uJvJpQkWVH4zx96/E/zI0t0lDMYtZNqra16h+gxbHJgoq2pRw
RCOiyYu/p2vzvvZ1dtFTMc/mIigjA/73kokui62j1EFy//fNVIihkVS3rAweq+fI
8qJHSMhdc2aYa9wOP0eGe/HTiDYgT4L4f2HTGMGGwQgj1vub0gpR4YHmNqr0GyEA
63mHUQUZpnmN1FEl+nVFA5Ntu4uF++qf/tkTji89/eXYBdKX2yUdTeTIKoCI65IL
EXxezjTc8aFjf/8E0aWGVZR/DtCsjWOh/s/mV7n/YPyb4+ECAwEAAaNDMEEwDwYD
VR0TAQH/BAUwAwEB/zAPBgNVHQ8BAf8EBQMDBwYAMB0GA1UdDgQWBBS3Uk1zwIg9
ssN6WgzzlPf3gKJ32zANBgkqhkiG9w0BAQ0FAAOCAQEALsU91Bmhc6EgCNr7inY2
2gYPnosJ+kZ1eC0hvHIK9e0Tx74RmhTOe8M2C9YXQKehHpRaX+DLcjup6scoH/bT
u0THbmzeOy29TTiFcyV9BK+SEKQWW4s98Fwdk9fPWcflHtYvqxjooAV3vHbt6Xmp
KrKDz/jdg7t0ptI4zSqAf3wNppiJoswlOHBUnH2W1MIYkWQ4jYj5socblVlklHOr
ykKUiEZAbjU+C1+0FhT4HgLjBB9R4H1H0JRKsggWiZBBJ6UpN0dTN4iD0mDVa0jy
sJqqWnIViy/xaSDcNaWJmU3o2KmkMkdpinoJ5uLkAHQqXjFaujdU1PkufeA7v3uG
Rw==
-----END CERTIFICATE-----
```

3.2. Certificate Authority Secret Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxR9nz41hKHqHfrNBxcGjkHp+JwBwEnV/dovHI3xBcHzde4/x
oNFZD24m8mlCRZUfjPH3r8T/MjS3SUMxi1k2qtrXqH6DFscmCiralHBEI6LJi7+n
a/O+9nV20VMxz+YiKCMD/veSiS6LraPUQXL/981UiKGRVLesDB6r58jyokdIyF1z
Zphr3A4/R4Z78dOINiBPgvh/YdMYwYbBCCPW+5vSClHhgeY2qvQbIQDreYdRBRmm
eY3UUSX6dUUDk227i4X76p/+2ROOLz395dgF0pfbJR1N5MgqgIjrkgsRfF7ONNzx
oWN//wTRpYZVlH8O0KyNY6H+z+ZXuf9g/Jvj4QIDAQABAoIBAQC6LWFU7IkZPDEA
/7ldV/huGuNPXuB67rLGelpJL7B219gwPdHPPCrLohPy3GuVYLT94AM55evJtXRv
I6GFpWs2j58kKukQ+GL7M2Ji1G3m4ndNIGS2Vu7DxEnGhrcDTq5wDjJV++pQ2r9d
7uAoOL99glcW/NJQm3FJuSZPssFHdjfzFrirRUwLPq9RoYsvst/EECxoq5WOZbeM
OsyGJ0ARsJpvBhIMFq/6eo/dFfTR4qba3BP0RksbETRNUk7ld2iQJ9huZkThNz1l
lxMpvpYRCHkmM8CIVzvb0IsCBmio/5YpShP3PVB39Zw5XDs/A9Yn5b46hjEX45mn
HTqaAz/JAoGBAN7ayderxL4C0jm8aif3wWMazXetuU8dU0jeYAmYCNl+R6dxtBSI
KAv770caDfDD7wxmjBDqEIBqIHYUPo3ouXiGt6r3WWNEzvRp3VbOS9TfR0MQys1K
WAgroB7mSJUG14I/JTpuFqwqN+VBXNTND2zb7ULj9UYOedIgxBqNCkbbAoGBAOJw
3r2tQNGBaT2VKlp5Jflvy09OOFaypdqMujSkbLi/gfU2WulYw8hti9yjsJdeAhv7
jk8LBIfiXyByXk/qc+IcEov79Uq5x44lV/KiP4FcZ3kGVMYmr2ldTa+JJ0gtIkDh
ZKVzw6SaXnqxbygCtNY+DRxCTBGcCpZQCkZhjIbzAoGBAJPjd1zjRU2fC6l66quZ
U8GT0NRh+f6RhGpwACV9uimzDpQE9a9GZ+UEDFcP6D5lmCaPitXSrp65Ts9tQdHk
pehg5lPTj4M772btNhBcGKCsh1rvMtYnRuItKTY4NeSHxM5PX0I2Ol+IKM2/oX4q
ktj33aytIGCcTKVwTxMbk71PAoGACVtImOXTy9RhGN5VBbAD1a684+YDhfGT0NgH
ya0RoQCoyg0Y7JNyY5HDOba50UddJvLaCoIWCddcvuZ65yp0517plUcv94p9qG36
mFgD78B1thaA4j8u+FeWoi40pVLYG340vnFuIBsQ1FkIksqp1kByIjzLD982wMdF
5Wqad+kCgYEAjqXkzyFiD71D6g205kwwPzoIV8unmNMsvNn3UFF50/MS/f/ubTTy
FoHYUt5E/YiHbPRyr8zTzSGWUGhV286jRPq4iCwhd2ZQDRw1DuqNooQAqQeY93nS
YDg6U+BjPWQx0lN4LucF+BKwXWQ8ZNdwxjs8SSf6XQMVco4LiUZBOyo=
-----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
BQAwLTErMCkGA1UEAxMiU2FtcGxlIExBTVBTIENlcnRpZmljYXRlIEF1dGhvcml0
eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowGTEXMBUGA1UEAxMO
QWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDD
7q35ZdG2JAzzJGNZDZ9sV7AKh0hlRfoFjTZN5m4RegQAYSyag43ouWi1xRN0avf0
UTYrwjK04qRdV7GzCACoEKq/xiNUOsjfJXzbCublN3fZMOXDshKKBqThlK75SjA9
Czxg7ejGoiY/iidk0e91neK30SCCaBTJlfR2ZDrPk73IPMeksxoTatfF9hw9dDA+
/Hi1yptN/aG0Q/s9icFrxr6y2zQXsjuQPmjMZgj10aD9cazWVgRYCgflhmA0V1uQ
l1wobYU8DAVxVn+GgabqyjGQMoythIK0Gn5+ofwxXXUM/zbU+g6+1ISdoXxRRFtq
2GzbIqkAHZZQm+BbnFrhAgMBAAGjgZcwgZQwDAYDVR0TAQH/BAIwADAeBgNVHREE
FzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA8G
A1UdDwEB/wQFAwMHoAAwHQYDVR0OBBYEFKwuVFqk/VUYry7oZkQ40SXR1wB5MB8G
A1UdIwQYMBaAFLdSTXPAiD2yw3paDPOU9/eAonfbMA0GCSqGSIb3DQEBDQUAA4IB
AQB76o4Yz7yrVSFcpXqLrcGtdI4q93aKCXECCCzNQLp4yesh6brqaZHNJtwYcJ5T
qbUym9hJ70iJE4jGNN+yAZR1ltte0HFKYIBKM4EJumG++2hqbUaLz4tl06BHaQPC
v/9NiNY7q9R9c/B6s1YzHhwqkWht2a+AtgJ4BkpG+g+MmZMQV/Ao7RwLFKJ9OlMW
LBmEXFcpIJN0HpPasT0nEl/MmotSu+8RnClAi3yFfyTKb+8rD7VxuyXetqDZ6dU/
9/iqD/SZS7OQIjywtd343mACz3B1RlFxMHSA6dQAf2btGumqR0KiAp3KkYRAePoa
JqYkB7Zad06ngFl0G0FHON+7
-----END CERTIFICATE-----
```

4.2. Alice's Private Key Material

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAw+6t+WXRtiQM8yRjWQ2fbFewCodIZUX6BY02TeZuEXoEAGEs
moON6LlotcUTdGr39FE2K8IytOKkXVexswgAqBCqv8YjVDrI3yV82wrm5Td32TDl
w7ISigak4ZSu+UowPQs8YO3oxqImP4onZNHvdZ3it9EggmgUyZX0dmQ6z5O9yDzH
pLMaE2rXxfYcPXQwPvx4tcqbTf2htEP7PYnBa8a+sts0F7I7kD5ozGYI9dGg/XGs
1lYEWAoH5YZgNFdbkJdcKG2FPAwFcVZ/hoGm6soxkDKMrYSCtBp+fqH8MV11DP82
1PoOvtSEnaF8UURbaths2yKpAB2WUJvgW5xa4QIDAQABAoIBAA7vrwuIG4iLDwGq
EHjFdRXJSX5D+dzejMTHkxA1NMbYSl3NCp1s0fCf0b+pmmYRkX1qg3qqfzsS2/zR
ppZDUel9+8ZK0H6nTJDWRsJb/mYS6GwCMkHM3WTwRLl9oCkY4ryEksHA4THjQo8t
dPtWla6drp7crmHClXMYn143HdSdCIB9StRPkSgyHjyFLOThReOog2Nsm7eShmov
7WkMuESFku5OHFPLUw5FyLEzHJar8ZI7qYbT7X6IamXOf9aTMPDA1rqAcix+4KQa
zF3cNY1xgq/yIvtsv6oyknTStw1i3i46PWzMWf845Eayunrg8e6F3hWt7zndjXWQ
Jg/gAAECgYEA3SLlO2tGdb5gWHwzzZAnTzBMo1Z3toEN25LetuSmY7mxkjMTRDAi
5VOdpSXrVFaT5r8qwU9yFEm+OuB6k52CVbTE1Fp96JlbzYjZnKaLn5OG8+HSLdtn
1vj1XyCGRDJKJ8GaZpZp+WvBfp6449WpSgupXMdIOM8jfekgTEh6rgECgYEA4tKM
Da3tFEEyVy9ZSxZV9ep9dhE7kmVQnr2pvt2YfJTiKnSo2kkj/qKoMi2PhS8ZO0JQ
J90bDngqI5sIo/OGi+hwYRmcKCrvfnfJUEq3v+3BFQYPDfwktgiBu5TGDNimFA2t
l+23SwwCPfjPh5frk8GTq0IslRhXY3djNPhhbOECgYAojSegN9HZ8alVUKFnRtIO
kXrcURTu4MebxlkVDOT+UKUhfEBCNtmPWEAGcueutZm1rMS4Yks3MTazMUsJGs81
zEpz7ow8RTMyg6/0LA5amwEaZATY5+0o3MqSQTKd+uLiW3xm55pTZNE82PpqvVmn
/G94VgsGb+XARynnEzt8AQKBgDER356t+9Yf7KYT5jtqT5pt6kp6m+ql5HUTDv/t
rKl3BB6vMkBXBmR2B/EjDiN/9vNs+y5ElS/iKyucxJfDfV4TIQzAn5nJABraC0FF
iM8KvnSv5N3fqImA+Z/9JYNt8y/vbZiqoranmGyTwUHSSfKjNDEelcqDg5RPJbU1
7s3BAoGAdqDEx0K1sW/e0pOtb97fBNIRgUemSUctUiaV1imwIku1wuxVvD8z92xh
g0DszHZfhSIvZwrhxF0VqPEgh1mDWVfuSHG1g74gDyPy5p3OnEnrk4bloBhXit2Z
pUSPj7ME4rNqAEXlfdVUPq4T1Yq95lDMafQlCmUZU0DnuAy19dc=
-----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.

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

```
-----BEGIN PKCS12-----
MIINxQIBAzCCDV0GCSqGSIb3DQEHAaCCDU4Egg1KMIINRjCCBC8GCSqGSIb3DQEH
BqCCBCAwggQcAgEAMIIEFQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIxzMo
cGN7mdMCAhQ3gIID6L6IPosvmOWsvjWwTaxivUEtkMgTVVh7Gk79/JzaHKRw6Vsb
N+Ji8GrrjU/Q24DQ8G/z7T3afyEWV18Kbiduxq5m9ZPLEKctF1HETwutywp6rBOd
tOYw1jrj7C2QsJOwMElf5nHeA+XYiim2KR6d0nFtX/pwZAaw7jnaBCGci2KQNOgL
9QYO5ulHkOBoSaOABKXuJcCIhFMgf4wRjgwFRPdzCzxOEEv7njAeFHz4msfqScVb
hdi3ZqWFdklFA2jiTtg0VvrkH1cOHlSMdG98JoYPw7FSHFMVOMNUEyHnJ5N1WlWy
2A4FxcHo50CKX5vN+5aiNmRynU6h0vEHzKFT6IcyI6BrArfrLAl8BaihU7As4Qae
EQPiH7A6ENs9dv8fzBST02UlZK9B8oLvh2YmCNMDuVRLrj6BvriDfAgRYCrLvUqf
oIQM4wPEQMKf5V/UMCBUHYLVXPxIlzJ96Ai5JEjI6gAPVSfFDSZbsYsX9SPXAG3l
Edd51X1PeEv4ayc1cbhQ4lEpyu9g3M5jzP9lteiYyygAxGUrPZri4tNJ3in55E2D
AJsze8FNWhGoHyoWawgf2nm5E+U83gFJkzj/9HDe/owEOPGPgJvRLsMaizdiCLJG
jgAGPCCvZW7uqOl/YSu1GIZg/AEZMJu+hh2Q3asOPkpZ3rGEFeVlSeU/d0CIZQqA
SZpULDhtq4upRsq5aA2nI91HHPzr7v7XV7jTpSx2ycbuu8kPGvmvlWX5pvE7ffwj
CWHfSAokYLc8FNXluneJi7ePcGTSbNHg8eTMg3AWb3vGOCgmIbqt896AgsbcYsAr
+049yZL5b08p76A3ZzNkkNR8q0BgYenCiuT+Bs2VB25kbHbkozPJl/BaMYN4uAuA
sLc6peraLilf/gv5jTgcaHlf9gqIv3pn6vKha6GptrZL1u8AU7XX1lA8s2ICBY92
VtqUpffBEVLg2qr84Br4ZGIJ5iW4EQT6FASVvXtKenP0wNAe5ZX/HD5JnhzhQww3
bxpzYP+vderrbYyyUBKvnZUd+wgfiGjVxcuv3MGw/ca0KxdQ/7OCpatJnFmkaBk1
KSOzFG4kXzGYl64PUvJy0WYcO+sCtNze3FqjWWKTXTuBoeccyuekWDXeEL/6UocJ
pt0oRGxF3PqHnC9RTwGXtfkF6dBmterFuHFrQYgs2m5vMX7/80SgZ11NL7t7H4OO
7Wt3GHgwvK5nwwgAYYn5crRIxy1awpjmQvtA+0F+R/542w3Otyc1bmoOAzj5R8Z1
PGA/oeUq8Q7VkwCq1cMi6eX261vvXvBdcLr42hrnrZRYnsHJ/XRg6uz7hQcaKH5+
qul5JdgwggOvBgkqhkiG9w0BBwagggOgMIIDnAIBADCCA5UGCSqGSIb3DQEHATAc
BgoqhkiG9w0BDAEDMA4ECH2Bt5G6lvBfAgIUbYCCA2gMr1bPEerGCQBxD+3Chj3T
PU5Zc8ij1MQJU/UruW2mM8zaZSEMxpr7tHw1YvcBl0YrLACWfvOpAtDahD3RPGpF
Gk7roO039CJHdCU6bI3IKkdCyNuYdIwhKuctbhXxhD7V0aUuWF7SVNmG7Yin9OWj
2Oyw3NkzaD2jZV1HxKACwEn4gn8Bc5T6jJ4FzQjaf4THmVdvqthjFmUVSYfz+akY
l2c0x3xggePOdf3nH0ReHl/yXUly7keILIsYeDq5Tg4SC7kFntbxEO5VPbHlzxQ1
XQfaQvl5Nzz41vOOAGgW1h0iliAU7qlpT/ej+PKJZwtLa3pw+LrPwqaVWTXfWyBq
NA89QfuoGXbqmIPNaC+wNjE4II9r3Uc0i96Jhhkyqz9Tni/42JuxTR4mo4bbixn4
qBHTZ5oUicHSto0EMaydWnE32xBbqEOUF36lYC2Xi9SAn8CIqwtV/J3WwFQRwji7
YcABIXsKo5dw9RLIWJw2yRRhcUw1+VozS4v4G0GSdZVJGo1r1H1Oc5e0pJwHX7pW
7LrLYN1ZBmiee+kkafPafFdojbBl77aUk0qkoBmhAt4XpXnfMoFBDQH7PfzBNy9d
USFsKqv0ALSsCNBdse2hBbTTr3xst0R1ulXcZ2rwbAQfXk/Duy+JjtWO7O47rAvR
t4+KzQm6QlrHBWS8vv24HrPlgeTjRbXGH5clTYgbDknypHpmb0e9fGI14ECnIB3K
q9ubADclJsyB+K+dUzkfaQjEMKLfWWKYPWNmo2NJ1uKknd4116hlD4r1HW2e07qk
NbUn2XroJSBknK0+CqxMJqYkL9IUgiLxxB+dFA6GqOIbcD3PXLD/klO3GgveMvV7
8az3LfpMuKD0WJfCw4RidGFRgU0AIu2y/GdawRERLbEA3u6ayxe901c60oWFI6td
3bBpaNy2K+hryq2u+NByFa5EixBO+U9HQd7xcYL6Z64DpKsLJRENkWquiTYdzSji
KECQIIC1iQEv/WNWzYFE0/Mw5TutLjkP95E1NCZJotUetGgxISLcEB4NhzFHLsgg
RA27SvtDZ36sD8LTEqwSBrw4f/b+ER66ZU1rJB+N99rmMRg02wGd/9si0S15Ntww
TkMiCJv/7dv2kTPTD1dG3kuNSH9EspnQ7Ih4LF5P2O4SVswVUC4GUzCCBVwGCSqG
SIb3DQEHAaCCBU0EggVJMIIFRTCCBUEGCyqGSIb3DQEMCgECoIIE7jCCBOowHAYK
KoZIhvcNAQwBAzAOBAgeMVJxqpj2fQICFPsEggTITkrmiezeN/JQ7nBhIMPWgFWZ
KGsfA5h7jHKKj5qaA0KssGIUEstvfPX5sz/X/zwQv+V4gXeHUP+ODoOcD56wiTWg
VBOO1eZ439bhyRCMC5cQUbjeSmpTsABvQNIHUaJ1i9DMzVwct6rBfODvS7mr8/wi
wF+sQca/NoxltbiH+YXn7qcMq9dC7U0Nm/b65djhgp0lhP2/zSelvwFssUx6c/8s
hQIqn+6/vDOEVwPYg7KqZdtLn2ulIUlzO4WCvpPckGoBb1pOT+dNWXLqsYWQb9aE
hmQYjSeteMDzLSaaz9Qm3yf/sokkT/tUtq1XOLn9oT7ZAgahl24T422SNCQKglGJ
wmw91YuhLK2hhDEfP1Ax7q4vvT9b23qkRybYtOov+IBeQw88lcJ8bqKMoWUE0BBm
fkmqrfYXAaK54ZUlEm2MQMwuTDTNmns9IzVSeULaA3SUGXFEVhs2rvjgMcG85lRz
qz8r/wqZhLpoAuNo8rvCueAE+O95svpFCVXfsp+ehh+yCx8xaqLLJnIE6+1r51ls
LUcIw3S/DyoJwVq8Q06J1cQpZzJoS8697TCY6jHtgzKchGV0HauPX+44kPn2VnSF
sVxazp2binUO/r/Mdtxkjxpfs0cwM3hcxQDllGJDs1AIj7xQvV9YwzgbVb02U8Ln
IhR9qLSCGEXsl8pndM+GL55Q+TWhTTBRPGhTCsyHMpLORif4Qwh005eVMOxKkGbk
```

```
/5hdl3/s8nM6yXFiZ7ZDH/LQDcOW13TPVq1U7Ws+4zUbvYl1a4Mfqn0d2KIBv0tf
NEO1BzwHZ3XRq36RP8srR8pFPwW/yQywQhL/k3pdH2guTJHBTC/HGFLa0+RbQjGh
zsKHjef00sAR4WTV+/Dw0/afGNUgJ69288BryEasj3+tji4RDx/gMPQs3zvoE0VX
MPOlxqNrVtBdJiep36sxokssPNutQQauDBPG0nvMejjyvjHK2oFgz88dwRIxeWOI
dr81RYN9ak50hJfEG8li6c5W3NpvtcMncAGLFsgkxIKW7PJqT6jYZ51KQlxhzv28
5KlU8RQT6qOZc6IM8O6gPMNUoaDh2mcuia4qChutwCzjHL1ernrOy4OihmLu/X6I
uoY6MJPb3fdbWK7y5s8ltwh2ubTKAh5MvZhox6p7007nfRAgMenHh9bx0sgho/pC
tp5V/8EG/WL8/DIDQbuzYeqPVJvSX6EUDnHdkZkTnsNYWEHi0f1BMwqDOMEKLaVa
4it++qCQbrMJw/gO1eGWFfzQ5vYP0mqm/OKWKmbyfgo2pRkhqlmvgKKM9Y3Cm4hr
t85Y/7Q8RSXxOiPnwUl0vYLx4q6/c0/1tEccVdTRN+YB3NTQk6ONacs0EQf8WKoW
2U748qgDb3NCh+tliCf4Aw9oWR478rzU36hkLRmSfxRHJwJspHF1v3xGrrWs9syk
YTqv6tasytWGG8trwGJA/HRFrQ0QlWrMkNVyw3UjLQW0T8YVi0xGyNtx3K4bw4ir
lZIdZhLe+JoVHaAd8FEtIuvUlC9KCI5YJm9ELN7D1y6PyQ3Cm8U7R7zRcYkruHtb
hukumLkKBYKukQb3fJNyeUrQU0QBNct9j2YQ5ssX3BL27OFNQXxay5eF/i0IJkf5
baAMsso4MUAwGQYJKoZIhvcNAQkUMQweCgBhAGwAaQBjAGUwIwYJKoZIhvcNAQkV
MRYEFKwuVFqk/VUYry7oZkQ40SXR1wB5MF8wTzALBglghkgBZQMEAgMEQDazWV14
R5Ze7BE+lc47t07S5FAX8y5JA8ocPsxl4OF2br4ekbv4hroGjK3Y04Mklsm7glKQ
Mr2Ty/Cl3gC0fOMECENNGvi+IeEtAgIoAA==
-----END PKCS12-----
```

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-----
MIIDaTCCAlGgAwIBAgIUIlPuMG0CCx8CzfXJwT4633mmG8IwDQYJKoZIhvcNAQEN
BQAwLTErMCkGA1UEAxMiU2FtcGxlIExBTVBTIENlcnRpZmljYXRlIEF1dGhvcml0
eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowFjEUMBIGA1UEAxML
Qm9iIEJhYmJhZ2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDCZjlu
Li00rpoCsq2s8SHqb91QPP5bdfzfaJg/G61lHUhfavEX9zZluyMwPPE50wqwV2RJ
X5dg0kStyH9s9Ja5D59pPnX8oJJ7XEqNKwxqSfJt7lRmM8BrDvSP55iP7Ofx+O+2
MzVA4tA6WUaUy2j9984CMmXH/CHjBK/+w21vSTmzFVGmeTqxxHONbd2zOqQ6Yqr/
LBaHjAWl+tj9Q+2nIjEQFKlWs6vZll3Xwid6+dAxrtpEO5rIpKZcbn40qT1pyDpr
ylNk8h3P90nwrOISpdlAJ2p71ZDdLfLd8c6qZGBPjmHwTUnjmH0oy33uBukT73RU
W6raD8MwM4AhQ4ETAgMBAAGjgZUwgZIwDAYDVR0TAQH/BAIwADAcBgNVHREEFTAT
gRFib2JAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAPBgNVHQ8B
Af8EBQMDB6AAMB0GA1UdDgQWBBQBrAKQ6Dj0kN4Z7pXzMnThZgAopzAfBgNVHSME
GDAWgBS3Uk1zwIg9ssN6WgzzlPf3gKJ32zANBgkqhkiG9w0BAQ0FAAOCAQEAa/tJ
ZPgdlmc7Zbn5bccc1TXNn8qBhECGHma4iSTWczDUmsNjezmDNniM3hs8QOqUZvx4
ey6diTlEngrKZ8bnwsX03k9Bn8UDPT5Y5sbxwEHpwKew41LRiLPOZFSh3DzCKYS7
HDSXJsJEGop1AwzKxtRss06C35g4ELK0Q2MwLw1u95f0+rC4q+vYndS9NzFyS3Bj
MIt37gN+Yy8h/r2wvtPVJ40mYNGmtQhdNuYnr56LOuFMmGiMIYXE8owo6L/kzCcy
YxxCy71lbnBOWLGcJz4HmRMdWJMRDV+mgLmTNnN8mPltgQU9gE3KNrYcST9v2kk+
N+cfxLhC0caHFL5G8g==
-----END CERTIFICATE-----
```

5.2. Bob's Private Key Material

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAwmY5bi4tNK6aArKtrPEh6m/dUDz+W3X832iYPxutZR1IX2rx
F/c2ZbsjMDzxOdMKsFdkSV+XYNJErch/bPSWuQ+faT51/KCSe1xKjSsMaknybe5U
ZjPAaw70j+eYj+zn8fjvtjM1QOLQOllGlMto/ffOAjJlx/wh4wSv/sNtb0k5sxVR
pnk6scRzjW3dszqkOmKq/ywWh4wFpfrY/UPtpyIxEBSpVrOr2ZZd18InevnQMa7a
RDuayKSmXG5+NKk9acg6a8pTZPIdz/dJ8KziEqXZQCdqe9WQ3S3y3fHOqmRgT45h
8E1J45h9KMt97gbpE+90VFuq2g/DMDOAIUOBEwIDAQABAoIBAAvQiKcAmXC9N9D4
KQP8t7H20H2C53aJii/NvIsBVJ1zlSVva22ocZ7nK7FP0t1PzTOAbDDlZV7WCKSD
LfNiPhLLN0X/LM6It75VkpZXym5fRiOWO3zmokgfZY+lZKlCnaogFfl9zTu/TSZu
rJJ4dk4RFG0fwP3RfgG9FDEokWsU7fNS52VCndOWdGIt0EmsZIfX9H8rnnSrSTro
Dsk9cQjyjMcCH7X340KDUaVJlRtx+1YlbPTyuKF2nbNjSWfsYhuIOGT4xGm6Trda
z6bWjuxH7nNrGKrtO14aE8Xv56sC+J5ulwaIjf/V+eDZVfpVgiXyq6oa6JioPv7u
rx7cIQECgYEA9ovqOi/OYdDNQTJXB4LNMtS1WLxgrpzE/SNPEV5XknQ5yf6rrKZ3
+lr/r6w2Opr4PY+3/igMoBZcN7YgIM9Drkg6bDLzrS354A9dZLDBNAgCnDR0yY87
U3f2ljjpCA2zZrahYhhKsfyMxt2w3cUso299OYgjNwLaLI7LrXvPa4ECgYEAydpv
fw+zdEc0xbGGILb4xiiFpJY2s604auZ3/s/y9W3v8LSKrytHHopQOg3GALvQi+Ay
LWRBIaJTzEueE6lIYInZI2+WvK2zP2GB21/JX5MI3x7AcRp//1muyhnW3GfyPGpg
6zRE45dZPm9nklywl4+yl47ubdOvNyxifBmDxpMCgYAQHb1F6HIZOsjwBhZiS06W
kAj6r/Wx9FV8Jp64h+45iJdueNNICem119T26s7wrcikXYytdHi+zjdg/OrEuke2
UMpg4EPFgkffOaHlPxiiChQBmfw4YMCECEd6MmYpPJwJjs6l1uirEdMx/LPfC1CL
rnIFHL0Qj4MrfnoZ8QnyAQKBgQC6WT2ryPv8MiynAi/4jdL3ZbuTadYQZK98CU7o
YGRFbnwf9R0/gC3FJR3RqpuMW9e4+n54Z2C1w12ncnv6XMLj1P8wdrlrcNTVg5hV
xYVsBZsgGQzCnhtiyxHRpK82hYQdgHv/SB79GeGbAVBVz9p74X6X6q11mQLeZcx6
EzgTnwKBgQDjWmtDk85A0GQuJBR7QOB+CXb39j0a78Qwywpx+XYibmg+N3aD1yJB
8VVtHWYbq3wM51EdjxYVagyKd3IKIjnPbBIWIjFWqEgDXmBROwwR8DBpfvff3jh4
JjK+LtvnHhhw09KtfCvZGplZYfSfC1tLuodBMNjxUX9u04bqTyqx/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.

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

```
-----BEGIN PKCS12-----
MIINuQIBAzCCDVEGCSqGSIb3DQEHAaCCDUIEgg0+MIINOjCCBCcGCSqGSIb3DQEH
BqCCBBgwggQUAgEAMIIEDQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIKuAW
go5aXBwCAhSWgIID4MdnJrlVYTYYFnsWs8tWL6AD8tW3DBy4QlEpWdIMjCfetDH+
hPblFWNAPEYgDid6Q8XHa8FBVAHQwdLqOMNonlj36WnQeDrMjxbPQiJWDsmD5kw+
opnmG3fbi0pvAfX1fichlee3OmIwOqphr5mypPmgJo9SYq8QVCseXLaSyc3F3Mao
WEdEvzpUZCY/8vPp8j/dnTZtF0kcCHAehOXYA0MMB56Eb2DhX3k1eaqeuYhXnu0L
joR0tKa1RY5T+hm8n2XHo8pZiIKRZE71oO0PEB+hdqrZsHEJqKYgXOZ+owsiT6cR
E0YRcOlqJwX8xfYB6RrQR4iiEZM8POsHFud5W9fL/toQmh//4kU8Jz7HLeKSijRD
SzYtYhHN0GclRZsGoesCS3cOMyBR5j2ANgkS6ROrQjtQ239We/9EpeRdcOSaCr/X
efcSQwBXRJVdcVe30RFjsjQFmIfbrt/ZOfUW0s7iMNkI3KcwMBppVfPU6wy+XhJM
P3MTjsXNl3iHKstvDnYCKq7BVxCH8Q7evGr407QqFfFpRP5sno3HbgN76JkRgD1Q
9B0GClinY4b/6QOvccWsa6v32iKCXGJ9ARTFa4ebLCt2N4GRzYKj5MuuB3cbghk9
tESGkfyn/iarLg6gYgeUIt8wo+qpo+I7Yw29hiVk3ZH4GSfdnvZbHFUpuVLdVtfl
/L4ep2BvNXbBw1DDPm8I+GcHJrTfk8oeTTXPKLvvO2TENMN9pBc+DeQ+qK3Mmt2u
UrrM0OmDS1uyS0N57U6t+GWZeAT4Zeu6oU30WjsqM5CIcAfA/2QAbkhGab+nqp4F
hEPNMYVvNHXqwAfwbUTg9qDuCqLVjqhS1T8nOVl/bB0NtuTSRjwF3Oz0fbYOulm5
IYWl1NjpSY3qnsb7CMGlzeJUGPV5tjqLOOBgVtlVyZSCzw2lZp9nJXCcsboLkF+B
l7ZmIzNFh1Ut2W5UZX7bxwJgvW+BIvHY5wuAzMF04GxgygKenCfub01C57hY1Mp+
B05Roe4aqbiaiM7doEKCcZQTAgYzIIZYZxVv0lva7Zl+Qq6UA/uOKAdAIDaZ8b63
NRN6KU8ncgATrpNpXA3JRxHirkpp7pBC7Ft0zblD6Dhmo+NzHQEPAALNE122BWzR
4PnrUWhvLwN1Tqq9klrXfTFIyvKwoLIwGBTZK69u2uoLX+HioBFNFhhua9Aj6eXe
sGBGnMNqFhSqhMlS3amKlDRa9k5kYx94eWgac44DOB33icLPzjAYvwq1EiLDXOB7
Q6g05D2zR3nKu1qKAq4NDkRwgaMITvqjwlcf1QXYA8SMeMdsVLTv63bxmxNmMIID
rwYJKoZIhvcNAQcGoIIDoDCCA5wCAQAwggOVBgkqhkiG9w0BBwEwHAYKKoZIhvcN
AQwBAzAOBAhot+9QPhtLWwICFK6AggNo49L9gonFWOJJv1Q31JN+Y7pc5DHOScfc
NSrBBNAM7fcTwBpJzciusYu/HdYBvqG7Kd5hPXIVwdJNXzFphQ8DPd4wcoowJb+8
z1zjY/8armxwFGuTz4Zhjnl1xo+32WPdX0j5tr3etKFvRbH5tOjppwUY7kLk6L5X
RCLMfVwZBczsB+aIuB02CowxRpj9g5Kb8OsfZbdqdo2A3uDZ6ZjWNalam6VOI2q4
SD/iEGqRs7H+lmLTywMdmxxjBVzrcbE5KwczBhr1eMMSwW+hN+EV0cOTZd5A00Rf
vHb7LxaKQwqJ2mpSP3ym0YY6r+BENa4Ciok3CTYuti8i2dKWBgmujBBua/aLWfJa
xHSwMFeWa22fMgn1KLmEJr0yT9W1i12Li5W47L8mIvAj8PyjZ7ElTAASPWuocrqH
qDoSepaufvid0GtdYYE3+2MWMn+RZoyt3ZjJOjtI+N5Zob1MyVtKOdJLSsAaJj0o
BdoPK7C6cjXNxw5DGHcKOfrSvPSSNfisnxw+8R/AlshS6DmvRscA22qzbpfDkhFq
ydpMa+/K9vN2u07v2ja5ayIaft2NlxorAUF6NMFcI/uoHWweAozfKXb9BSrUlNck
X1z8H9m28vkKw9lguUf0TLZyLP8neGD+jMV9vpuH5uuu7nuxdLbbZXsEm70BtUPb
k0ZVPYRc6PAqm+5nNGYyp/IsS/iCOV7S/8rUmo0xuzPzj1+K/3eSrjTd8UHxszYo
WxP8ph7cJWinnlKNaTBDiG6K7Du17AxcQPjkAvv34iQRgmhmjp1Ae0ZlCEO9p9Ve
AMQRTMTG9Ki0XbUTd3Xf0RO5Sy2OBqgUc55kPzrxpmLhT3Si4QFYuRyNXCeSvnaW
iV/oQJCSflA1EWqvYKAnCK+a2CUEVQHyiJ1mX9DBeBRACHJhqXJqoHLJP3sqPd9i
akrFhfLHVEO5o9FCPb49pxBMg2ElEXxPIycewfDFAUjrYma+FBLELGsj4EZdVAkb
YJPzVf5JIq3mMhRQ4v66Ns6G0rk1rp3FKk4CRFygjmrM/jADuWy6av6yViH0Jqew
uqEY+zcT/mRiRoiACTqciIXsKnSwnXzf+mcowF7PSMEYxYNk1usverEsUL4XlXv/
eIKBepm/FjVOk1l5pWk7JKfY8rc1zyrXnKOQhTMDpUgwggVYBgkqhkiG9w0BBwGg
ggVJBIIFRTCCBUEwggU9BgsqhkiG9w0BDAoBAqCCBO4wggTqMBwGCiqGSIb3DQEM
AQMwDgQIO4ck/+gdo4UCAhRFBIIEyPyarONCAchxW15LB6KUfF4AdiHfpTNAuYBF
6A/zb8Wz/J4FOcViO+9dx7E/VxeNMvJkmNtFqUEofRlAkGqeeyLDMNVZqLv1N1SU
isA5d7Wsu6mfpFx4zdfFtFzHCnUt6DAzcXrlX4gtixthNKbsnrgB+D3YS7oofza4
EnPny7xKEBS3XCi6IXefhI3+gzOtg04PNCpeI3d9pt3ew6rndn25roNsIEr+P121
DiMCiE3fkxp8bQw4mE2fhWBhPsM0VvwCnGCdLhBP/ihoV2YAF/rtxfb/iI2SlOXF
fFh8zE8jlOVTVqF1rBAa43Fcapa1QbEHv83WSmZy4pHObOfGCqU0TFNLwxvbQRI2
Kxk0Ljp8dD6d6uatiOzOLr2vsk61AewNDv523vCvuviMlXvMUpJE4LJQ4M2H0VDD
4EuSMBmdJyl1P4WE6nMQgKE8bG5d8+YYfcgAY71KXnpq/Kah5zNqkO5RNAhg7LuV
ujhFjB6ypA4TRiVrVOiMtK8U+ZAHS54B2VU3LqcHv4F7cf/xZ5SRfRBnboDF18A0
WCtpSSf20H21Xl9BeSrZhjc543G4s9e9vjYD2AhCbSQALJQyadXOEUY87ryyTiGZ
G6/YoDO7rcsxZVufiV9TK1cz+Kx2pxEb3VgDfLLcziSi5xvYPeFA+HPZ6jGbME4Y
KNOtyZBQDINHEja0P5lAfQ1ePg5OfS2lI9k2D5URV6q+LvksElI86tetcUnU8nCj
```

```
y31M66oJCbQ4v8TKyzDm1WOBAlN8yhfWG6W9Ttapt4qVBfKmPY2Ak+rLNP5qTJ6X
m3KDAlqSVNd4KNrQW0FtORWbIU0V2u1+0F3njleGGsXplWfKwwVdkD2Tc462qWdZ
CR/Lp4lDrVe4+Ezf52emkaaiha0uALlzU2VGVWoBTgFeHPBUSGG78/tLPuzSfsVm
O+8GCPmgLqrZv+QoezGpdFbwcDF+AXaDTTKE90kqMk0ActULlMJXZ7S/edNs9XSL
qevUe5u+y3IyV9T0cShd2/xNdBTfzEErT0/NIYJiuGYb3NOxFvjiziOflW2Newdl
pM/kh4SW9cJiaDv7zAziztAUK8U4EqoS3N5deM+lK5newIaBBX9fdugEc2lDluPK
kM5Jic06B+u6WpcUlMIsDyiH0zXMNoILd1SoU+XvKFXPVDOmg8rpv3Ff3INJE+OQ
ODo17XJZGY9FdQiRRN5A5EQsQxYzdeO5ax9sVqGMs0o/5YrXvGzAmQ5KT8DL6qxZ
m4fBxomvlEfxbH+vxlKpbmiMaWrAKm7NdrbE9QQlUztQQUbp1nRyV15LzE+v0A9g
LXH1ZJNPQjeK5awoCtYeQFKrJCI9KqvmAKXAJqYMbrf7iFo3GPWMvO318vuQhTM7
sQiCcUuOGa7mqNGweICWVWJG8qgIbet996oL8N4UJdKk+zg/kVWqP7iaUCKoUArP
udFo6+h1fia+EhjcLcR1UJvWicsoUCuUjJsFCMBHUuaYJ9uItVQY3VE301B88Z9M
vTxBkS+USLvbjwjHV5PJ38qYUo7y02L50gAi6UWKg+2v2OCfXIg1VmOhfaPUUfSi
yn3TOiVGhJeC2uzmuqUoPSimgakY4whGVrzkm82A7C5yv2nMbrmyZACkqqa98TE8
MBUGCSqGSIb3DQEJFDEIHgYAYgBvAGIwIwYJKoZIhvcNAQkVMRYEFAGsApDoOPSQ
3hnulfMydOFmACinMF8wTzALBglghkgBZQMEAgMEQFP+9F1uFuKVThpIjkbWCN05
g57aXR9DKOPLzHQoZ19wUYyP/Nn5D8bG/c2y0+U6BsTe9SEe6pIviN+ul86tdL0E
CNLOBlp8HmeXAgIoAA==
-----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 -01 to -02

- PKCS#12 objects are deliberately locked with simple passphrases

8.1.2. 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.

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

[I-D.bre-openpgp-samples] Einarsson, B., juga, j., and D. Gillmor, "OpenPGP Example Keys and Certificates", Work in Progress, Internet-Draft, draft-bre-openpgp-samples-01, 20 December 2019, <http://www.ietf.org/internet-drafts/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>.

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