Workgroup:	lamps
Internet-Draft:	draft-dkg-lamps-samples-01
Published:	21 November 2019
Intended Status:	Informational
Expires:	24 May 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

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

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.

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

```
-----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.

```
-----BEGIN PKCS12-----
MIINxQIBAzCCDV0GCSqGSIb3DQEHAaCCDU4Egg1KMIINRjCCBC8GCSqGSIb3DQEH
BqCCBCAwggQcAgEAMIIEFQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQI/9dn
i+BuhWsCAhSEgIID6A5pqJodSl0Y9+WLYXssoT9lDAQHO6NzQ/XBjRhx2qHtVtW7
OhG239eSt9vzMCnc35YGCfnoKgQg22qRrrBbWDr/zmNYi5fZKvxETNvscpPQKnKn
BHGQov3r+HiivO0I4eXJVSRhG30szy+zneATyc+pKgZWk+1q2X/Q32pGa9T6SPgZ
l+HH4bDf+Y9Vs3LkYw7vIM5NLefgCgiNGeiNTKHzRd9VZmAWyBO5KB4nsYdDi6JF
LGB3Udw8ETaAGYMQer50FsZwReSNgSJVnLk21zEJgKvXSsKa9A3xT5h+Zgbd5Dsx
bdaQKnvtmXZh1SQJxDregQ+QNT7GJnDbPNXABswzaHnaGOKQFl48M76An29nq8m9
E3ZYlrU41c7ud0Ik4tPShUjUHIejXIadrJTa4Xnl3jH940kmojwh/PhjxrHY/1GT
KVE/1sFLfRyEmf9vOhDVLVj+Hq+4PWO8KIzaPCYtaAcMOXAT4XC4l9gL9qomzu+/
FOHwaNMNqd2XG0J6cIIIW6xbPjKuGr3vYSEEYPYenycpv8P/6uNyj2rBWmNWgMkd
ntR/cg3NZSodo65vgW0kbiQrUMZxL0HZlBMeQjghG5ziLAKI7mZdPiA6Nt3HgpIE
EWgvdhitYa21Lb8wv53SavOQWWaxwsnyoQzqDA0R1+ChtulEBopR0bD57ypuFT00
sz8tuJy566UQ8+dF+65JqqjFAbJ+gSVTZKJPpwV23wzDkmxrQCH/+UoYq8N9dZ5A
fvvfHwiJYLojI5nEJt8ssud5M3oYJ7hR00YjNK1Ucf3lPKP3tviOpNj/pBy04zp3
0UZGRgE5dzaX7lwIIwuPbdNbdUkrAP3wpmtjbT/lu2hYzORQP5X6fGH2qpMo+mxF
JeV9570v91Pp1J5jY5atY+bImPW3P8e23oNXYQgLqpPLSxLDISRBjGVt/j0staCR
t0GSCEYtHyOnBkwR+CBKHreIppGw3fsEGxpfK3/xLPFdAoDjceG8zLz4EkbWiX9Q
LR+xkWYypEVH8SRd1A4urA21mnaUBgOU/+sFSMzGehPtlRkZ51hrvkrvreETHkP5
NQFyBHvZUlVZGxy/VN7Hsil0t1G3iGhxW8v3giVFeocVhVRdICuNMOZBOXR/X9LC
PYDT/AbGE9Vr0gciO4fT5kDO3QqyJwe/VLYym5V1fEaEp4u+pTY1AXAnLMbpQCl4
+uobNB7QaFG1BP5UlrxlK3oeJwzVzmJTNZKjEdmT8rM+8pdZcfCP78zYdHw/t9LG
W1MXVmD6bxkZEaN744w39vaUZScmch2yJdUHFDhiqcuZE7y2V1HP9U7dIImawzoY
xBHbhucwggOvBgkqhkiG9w0BBwagggOgMIIDnAIBADCCA5UGCSqGSIb3DQEHATAc
BgoqhkiG9w0BDAEDMA4ECEWK7aRxpzOiAgIUSYCCA2g8qec1HwJsCAm8eGqgMudQ
bHT072jC9aQL+LGMyM9pSoyz40KGlYfyG8oWhFngdE1Hjwp6ydHrK1hG4u2RSXty
q1ABeZhEsiUeZbIpf32i1ljiMXzEdFlzxLoaAp8pwT/RX05SWYiTOKhHfrkWqs7j
QYdNCPCECgUEYpEE9mM6bhJMG2Gw0DebVPIJcCPrtES1sQr9J1aRwK/CgDe9sYUV
ft3GS7LDmjgssPWOVan2fDXMDt1vA2tNarl8c5iFVBmxKsSY0n9Rt58LVSOCUHVD
3p+Nspa2i2JVij8NbgJwIMhGlvsdrjqCFo0SRqFqpB0CplUcq6RQuWBLudYX4+Ek
5wEW/7seIxq4R8w0fewnDth6HGexUhOqwNvAsbK5ZY3ok+b2BJlKwXs5rRmLai9e
eoun3VSsyGBR697S9zvUODmpKz6wKRoip9O74dtPWtA05xrsOjx4GzvFUagMWmM8
RI2Z6Mz0qDj/2+ReGw9Z+ePHxY7mTNQncrbrMAN1qlO+VP2OtYE1d/8HJsDcemZg
9vnCPvf36r4r+45iVno6moC+rz87NYLTXlTsOCpv2RSuLrUyCm3qBNpM/geavYeZ
SCaggVkSm81vymUQseogR6DPKqBOejFTggxBA/b9mzfCLp2NRfe3gjngvkqY6aqP
QzCoumYg9pEM7tVSZGryQbVMm85e3w2R1FxOT1JmNE2YtF7W3Lo4DN33gywoFRJN
JPAMnn42gIC8N1BCC9EcGzF2cgn8XxK7LWCLxmL/1193eIqouokcichJjuMpYYQB
l056TvlVL2NuyawAXnc+L0ttWp/sN9xSI72Ti+FOSW1g/cDQ0iKvG3O0DqQd4rOU
1NM3FsZFCGOU3RELnct+4gNGnZXFLj36sIe3bDguJZAXpPeE72mHiV115XWR/+KM
nzN+kM4vyGShPOVWSuxFODfWhu8B1H2HcSlBhmqG4f553bM+z7sqp8fGvjFI8T3O
Ys+qrNalhFiHOZNRT2Vp1gSY0L2RG3TbnQSFcYSKrd1lIXR9jHMoaZnumdLCPBj5
NwkqEAUmCTlDpvySGWMCFmrnWzoAWhSvcx0x8wqxMRNuO3vJrzOIiW5cjovM6FEE
dD2ohb27WIR2ST/aSAje+EMG0q7V5c5hPlq3Gp3f9/IaMwQh9ETipDCCBVwGCSqG
SIb3DQEHAaCCBU0EggVJMIIFRTCCBUEGCyqGSIb3DQEMCgECoIIE7jCCBOowHAYK
KoZIhvcNAQwBAzAOBAjRhW3i7sf6OAICFDEEggTIAHeeSYh8F9rPFPYnChBUV2Vy
b48I3jYwIBDYCE35dvpP/5tlTTTbHSmYrRwfzAx5VY1ATaXl+xPhm/3LX9w+TdoK
VggYCVWi1J3gYyff50ZbHsbUZ5L0nQvW+RP62DxWWKdjSZXSgJGDRqqvT+xS14ae
Zt1u0z2095modzg7BCsPP9nzUxovs5wTKd5gCcPzuR+8xxkqJXQmJQXqQ7Vz/XSD
JXlBQE3UwBTege3eAS2SBsYGTkCgLw7aFfAlWE7KKZTL0iTiD6k5eSYSG3hO2BwU
LXyc4uztag1A30+vcy7oTeop7NkNvDUcaxK5NO+/+rjf8/h9aLAa+CLSITHuUWhH
PeDCbPzpUWnMVIQ8eRO5qC055/fmSrJNXyOXy6Bmf4Dgq9wE36BSNafSdaA64Dr8
5S/amMG31SgvT6+gB2TfTYwzUH3+lVZWsqRgSHcDKreAeKZSciZeViVQpGxjy4aT
RkvWJtyxqZD5PF5q2P3YPYmDbf1jy3Zsj9tOyViqbuws0AzilwIgM8MWkwkGtXdo
8UKmp4vMJMnJ1RD0tzeayumConDM/ACnsada9jBLIN8oN5tUYZfYbifTLm9OmIzK
ci4/zaUHxoG7X9v9b+6nrF5PxTtMLikU6yr38rXKZqr9KEwdIlZENuajkZQ+kpHP
AoUrnK7qjxGXC6gssHamLQB/PFjmiU/OVwDzWi9sbJTPdeQ0Jzzkdr5HjBkSeY17
```

```
nxjNz4PWAOLznqG8SmSSPGgQYQg8OB/kNcSey7hX/vNCmlYIdJEZSMkDZ5hL/PvZ
SwWq6U09JN2bAgH4Sum03CNAYPrysMrJLm3OvsFq9zme0znSnBTe4jLzEJwaR56O
e0ythLIRaSQL+gxHy/Oi97z2IubuDOVy+aSZsTtVKr5ByZU3oJHJ5qsWTIHFBZmn
FvZNKM+3XuEa4Y3fZt2fdyYtV+FkEoWfkx2/lPVcSrQ/oOH0iXQxB1qsiuGYwydp
mUPo9qIqihPNKmbQzcym8EX3i71/HElirUHSukyF/qO0PsnQZCRj/veLm7Y4cDAW
EDH7lVB+DG45aAXZHZI5OkkTwytptbEvx2bJQFCbB9wyb0c+7B9SO/dCY95pAIAt
MHsWTroG3fRwZ/i5638VRu/wiK4GNE9zxYyIPNuOHPGDtfH4/V0vBWturB+iOp/1
awZLqSbeW+ySo4g9au5eyqsdVVlBFYPW8hVxmyiZbSd67gHNNrk7HaM/vBMUjKz4
WmzF6e5PLGT2PR1PlHbMUx9saNGGGtWHTyAYR8sWynazVa5gFFCxEy3gWwcatFgB
OJQ2gZfVN/SSoOixwUs4O981r80W+ZHeOH8WXWpdSzS4+CIWOMwrsfFBprUeguRQ
hIj+uUSsuuj7FMOQt3K+enuWORhPu8b6f89qh5dkJl5S4+tKLZ6Qo43mAmbhUakx
w1JR+DNmOFtLjCBgi9G6aCBnV+gJ1wWYFkVs+0cjLw56TevSf7j2I3Q4o5+w4FBE
TrcSKUlRE0cVIqSv4RloWaBzWul5LnId2jYZWk+4F97SMt1oX5ZwTyU90zGL7f6M
FAaEFHRu+JjxWZfUWMntIdjGeUsYVw8BRRx8dcKBryhfmXwT7iP+EKsOUf6FszNN
uha4gBKcMUAwGQYJKoZIhvcNAQkUMQweCgBhAGwAaQBjAGUwIwYJKoZIhvcNAQkV
MRYEFKwuVFqk/VUYry7oZkQ40SXR1wB5MF8wTzALBglghkgBZQMEAgMEQN2V6eSI
57sRTBc+I8Ah5tbc+6Rs5i9MI5n8I4wFjBU5QCJM/cEGnmEXlJv20wBqoCekW9N9
j8JjCFJI20FoI0IECEHWKi/gHZBmAgIoAA==
-----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.

```
-----BEGIN PKCS12-----
MIINuQIBAzCCDVEGCSqGSIb3DQEHAaCCDUIEgg0+MIINOjCCBCcGCSqGSIb3DQEH
BqCCBBgwggQUAgEAMIIEDQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIvszW
w8h7VVcCAhT/gIID4El/66Kqq6rDw4JuvnOKupl5Tueo6piyJPJ0fYLaflZAqRIY
FYno6VETexj6Jr8QoakjJLP/75t9hbZpDmd8DPQj6fWmwSlC1RCu0TTpy40/j3Nz
TmIW9vZr6jgG9MkOLEWxNwLvwRpSh1WFXGhiMkcmwPmb870n2HZo7RWXjm8TPAvJ
mlPUyveC0B26iFPvurobAeSAXhIFVEmXGWcVhlKhpQ1GYhmUVnLBa03Q4qbqEISS
p6Kdt/nvLwW44s4Oxq95EzFya4AtklUCfIJ2jR9Cb6+N5IcQj4/g+o8b9I2xv9lo
k5t39X/ngGhGCl/PnXnEmwlDq2Lq5bu2wYwYX4GR1klAabm7+h8PI5gFTdG18vBT
wo2QFpVnnMNiPf85XVk8PaOf1rxSqDiZttVlziVRVdvjgLAO4pvbVYOtgjIhPPmB
uXzwXJXB22VdNAiG4DWdapj5RlsokBqKzW8JauLlI4oFl3oyzGcaGolbWMoCWmGR
ixz9pyb5+Icv/oEL5ljWwPY0pdFfQ+T9PH91nDMa3X1hnwrCskJex1hLqRMnWDKE
UK5AWUl6Diiiqy2nlQmiZKULlyDX1ICzaUPNjSi5VoxW/QGLdeb6TOykWaDJIame
hq1jrmq/o6yoH1GFtUn1VUEI9mjR2k6Pod89IW35FZQz7hFMX1iBv3nwcgIoQapO
eiy/vhvr0bAFj1ZRZ/G5oULCcRq/iC9jE2qu3lYXVQ7MCo+4xPkYMUQk98rsF1cL
dRNQbAdVpQfS0nclZOTvwGsK7z76dWM865yGRE6YzrVICck+QeAzVN555kk8d8US
SMS7S/y47EaiCPaiQLCzRoHp0NFELrsjgryFSSG6PJQl+EbcNQfdjJQB3j3PLRed
YI0ixGVGikdHF1R7geyFgUwwdzBBcEJkrNhuQPiF7PhcsNLvzUhddCTk8GKPg8T9
NJIgMxjBBYic6QFlGEhBb1Hyyud8vwrLB1Jan/aZ72g+FyfVvgzKzEYg+B0qCK0m
0gs2+g6HgcyfP+Pz5ZqUxNBtcujZ8sIOL3oy5OuGg72FqdcDgqdJBUC84txVMQPm
2pwBlEYBbZBGjWQ+vX7y8DCjHgkSsBG2XIKx1c9Nw3DPJplQtCirJJYRa2/6FOC+
8i3nanDaIYZUcO74dyTQUVLlJymoO5UcPKK6ZqW3O/qiA23zCZIQ2G/S/c4qyefv
Z+Jl529zpqNBjZKWDaK7Hlcqf51sWMho5c4s4WwDqMrbKsaIN5lQt3xGc6q2umYC
yGuc/A5MVrFSIdFyt+L8tAvVBMHGpYRz9XRvry8XtdugTtD5qpQVfT0aHjqKMIID
rwYJKoZIhvcNAQcGoIIDoDCCA5wCAQAwggOVBgkqhkiG9w0BBwEwHAYKKoZIhvcN
AQwBAzAOBAiB/XCQbXHtjgICFFCAggNomvRtKzKEFruatccbzp3KakWSte4bq96y
zHb+56gj/XPySdMJlW9+AF2Wn0BfYdFpcR5H0PYHfyhnYWJ04XiPrB9EsDCKnpQP
BkAgWyOTRfsnafF6iyc1Iuz56nWSsBIirDWMGZkQZrvBZlDKVHn/TSU9juRDAgLP
9T0B3og4Y+CahyI3sVz7j86803TdCLZ5WR18jBF5zaU/A8Em8YK965We/a0xUdCI
8ZGgI+qPT+AZuICuqAtPnhMU89AY/bYwnDQ83Os9XTdCtHBtnH9/etrCey1qDNRF
NNmDSWgmWSB9KdabdKePHzYZYppMzajs/jbesAWWT/jVbdtNXpKYZDyUq0iF1uYw
OIxOw/MJ3TVVCklqzpx6aLAIMlbCKwybf+mUjfDlMIYo63mU6p7Wzgje3HZfUHgX
Z4mgNnSCQi6vURVsA1K8IcCYDlR4e1Ei9qBAJpqsXyUAXqgirVcJ4yeUbleFLlmy
oocZcX41hkaZOwi7q7Z7ycCF8ng2dxP8msnR+iStHtanXoWlqkK055mLiZgeBbsz
8fbUTmk5ZFgH/hIkSElc2dq+kFvq6zgbtyc37qz6o6qx9gEfYvpiBt8bZOlkM9av
iWPlblbzr0PsD6mBYgVa7kld/TEBxX7DoyluxHBcRRYCsN7u19jZgIRemUQkdzno
zCjJ/KavJLGb+JJNDoD/kParRsYWrdzJuQ2Oj2T4ec56hWIbb+8ngC2Cjiq9EJZk
515+ELC1/4nIAbX1qjK+3Azw8OUd+OPnYrzrxD2ggktoOHcdhsPtYpmTM0WrdtJW
kfQdMueddSJTDj+ZMew3qyKNo1FJaIVRQE64dw+m4t4nK3hgAkvEuQ2HXO6/abo3
WqBsMZ8nv+mn39iaXGEbYPbWyp3WA69oEpiQ+2Su78TaJ2x0eBmauoNaqJVhkEVJ
NDhYbgOiVV1MPDi1/TaZ2yc1TKSm0CQB8MYWkB8Pl+eDTftxI7wUP7WHvPA1Wzie
chMMtyQeA7fWL/6M0g97UmGDYm1y8atM8OT+8uHFDHS9ZXLYdVOX1dMPa8R51LIt
LKTCSM2kFbMkPy1q8h//nKYktLnNgD5Mg7Z+n0OYcQEZZ+Znkq3a8KqaVCh8fsMx
6CeYk1hDd4O2udJpdAiq5MuSaFsdHTklI4+S0e4LCCswggVYBgkqhkiG9w0BBwGg
ggVJBIIFRTCCBUEwggU9BgsqhkiG9w0BDAoBAqCCBO4wggTqMBwGCiqGSIb3DQEM
AQMwDgQIyPYWEdcyAm0CAhRwBIIEyDKlQn0Ac8GkTFU6QLlMaVStle2bQDTtfF9M
1/1FFNKqNsssNbPwOpvAUrowEugT0/I9DoZzFJnpQEMS2Y3IE/gdy4IGAYDSYUkx
ygTqX7iRgnI/YgibzQeq6yhp/y01jEDzsEaqEm7tRRidJdgk/J51v45LAB/PmAtC
7VURjhPq7NakNgJ5vB2n4FEJJke38+dlb+Xq008+rjzPPQ0XgMLRYELeHAaeWhvd
3c1EYqyi/J/i+Lc3COOc0s3ArPIXKAazzKAIShOkF7rIZyLUJMdQOaEd3JvJlgs9
nvAj5io8XyvpWOEdxjpsWIAybltB2gZmb4JjF1jNSrBogSyt2a2QhGBy+mUeRL5n
Utml6D2pMqKdwI9aGrYRBn9waaNw3OD0Yh3J46++2w6Mn058YbCQvFBsNbSNvlVP
1QiaLULuso+rrT97d3GvPK/HQIS5Zp4FsPbD9xcoIR9TRxueqwpDA54IpSdRYjpZ
kBznw7fJ/3BJbImuY1SBTgQnxkzM3i2ZW65YBsh2M3M1Gt9/eg2J7SVZ30E0kehR
WvNPBsxvjAe2dSMlTsEcBxava4gmB+OXx6bQObFTWCzSislLr9qw8WAVhX/bQi5M
Wc2l6ubbJTQ0WsMq5oKmnxbJNUKirDYMUKDfkQc7k+Tf81oeYTAr9ZFQzRAsfnD1
uRtdi1K3oyapSntaIzjC9v+9fekLSaegTfTfTdnvWNOA1AKw95stN/SMp1j9xXv6
```

```
/tPXP6e2cF/cHb1OOobhm+BckOQ9Y9RSbmpYuJLMPJz/kMiwi3aeR8h0U9Q0qSHv
6Hep5q9mjWRyjEg8bHMF+450zYgurHp4vW5hiZ4WW4MYxkO8v7XE05qJ1OWJMHl9
IE2uJxgP2YAYF0xn3xviqEChGT7LxgM4K2F5JMDqwUyISMqPkSFcrz83WlyZnft+
q7NuISpgsfliHJwnVbODjn4quMeUmvSWeCx6k4gvP+tK6REsSRWcrGzp7LG1a7Pj
U7C2BvVn/n1CAD+v9qrlCAj7XKAVNQ1h0S2yS7dCf2lcQjPRh7XS79OjEcdHlJzP
9+xcVsex4EpCyvCyBNjz00phOsoXy1kdiPJ+xghNHQEwE7ghFAfBmqeId3kpGs3j
dl3Jxk23B6qfLxxMwpJ8caXvc5I7XeHDWW9wG5c0hD8rFIpHbKipXlsLkVtbOrcj
MhD3cuSNvryF6ZwBuKkdvGhTpU5Ltpi4sr7Q0ArVXzC8J/OVxTPoOlO+R89IhB39
2+I5KOSQHsawLOWeK9fDO+elIh+5MXkH2UdwGwazjOdAnJVQUZFN756CrDIQI6ia
G+PZb4xtFfMV+gl09uRExVm0o31CfzrTz8TQ9KOhv6loRJMUftSFFxhQdbGnDtrE
Osn2wgwmpf0u3le1HZ7lxL+7w2XaK3z98lRma2eMazlu/YqoXbNZAGlzaMaBnhpp
z1S1qPRPp06WWXE60YlrqxdQMU6zVWqxSIWbWNR4o6ksL+VSZFF8EaB/IsteaeIJ
dyVPEUQRJZg7Ym7DMunSRYI2z7M/q42RVDz0OZyhu6vSKXHm67G+hL7NOkI1+id9
qEx7hxPXKtm7xA5tlPYXEzoEJ8AweV6FqGPsDp1FQbOUXuSZ88ksp0rEXO5ZfzE8
MBUGCSqGSIb3DQEJFDEIHgYAYgBvAGIwIwYJKoZIhvcNAQkVMRYEFAGsApDoOPSQ
3hnulfMydOFmACinMF8wTzALBglghkgBZQMEAgMEQNtkJG/r+MMQQ6SBx2QWOarf
yXDT4tFGtCrec547Oj5mN13aL2fKBuz8pzNCec6NM6SDbXb50IR2B7k8VWi/O8UE
CMK3E7w6ejgaAgIoAA==
-----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 -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

[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-00, 15 October 2019, <http://www.ietf.org/internet-drafts/draft-bre-openpgp-samples-00.txt>.

[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