Workgroup:	lamps
Internet-Draft:	draft-dkg-lamps-samples-00
Published:	18 November 2019
Intended Status:	Informational
Expires:	21 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 21 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 MUA

3. Example Certificate Authority

The example Certificate Authority has the following information:

- Name: `Sample LAMPS Certificate Authority`

3.1. Certificate Authority Certificate

```
-----BEGIN CERTIFICATE-----
MIIDizCCAkOgAwIBAgIUHpcl/2XJM79WIQ37OWPRVDomvz8wPQYJKoZIhvcNAQEK
MDCgDTALBglghkgBZQMEAgGhGjAYBgkqhkiG9w0BAQgwCwYJYIZIAWUDBAIBogMC
ASAwLTErMCkGA1UEAxMiU2FtcGxlIExBTVBTIENlcnRpZmljYXRlIEF1dGhvcml0
eTAgFw0xOTExMTgxODU0NDNaGA8yMDUyMDkyNTE4NTQ0M1owLTErMCkGA1UEAxMi
U2FtcGxlIExBTVBTIENlcnRpZmljYXRlIEF1dGhvcml0eTCCASAwCwYJKoZIhvcN
AQEKA4IBDwAwggEKAoIBAQCxl2hhvIJP+TubAJqFkGkv7lhqSFuPU/zkJcPxALcY
psc1xsn4KLzEbqc+mW0MrxnSdvPzBUaOHiQIynI6Gaaf+Gbd4r/GHBkrOul8aby5
KQ+4eQwDRd0AkQ6FH3VvXDXVk5oqflZG2IUjtGtnkrVINOBV137zb5/rqrsyOKdq
z4FFpOwB6jEourmC1WaAjf9OMWO1/8TdpWdabt98QHLGcVl/jBbI+juwoLDdiHbG
GeovOxY3VXDXlsImeXCa+sEKmW4LG1uU1v1bbLopoAEvL2qkriSpzhnkD7itYzC4
49lXXuQtOCaRaUYAPjk2HgQb4U1XbiNxDzgRf4KqoAw9AgMBAAGjQzBBMA8GA1Ud
EwEB/wQFMAMBAf8wDwYDVR0PAQH/BAUDAwcGADAdBgNVHQ4EFgQUye9Q6FjJCQsn
4uurcnOQIboj0OEwPQYJKoZIhvcNAQEKMDCgDTALBglghkgBZQMEAgGhGjAYBgkq
hkiG9w0BAQgwCwYJYIZIAWUDBAIBogMCASADggEBAAZviKON77fohdZ2PSvXmY7m
/WPU1mXU7bPhN13kDWr1wKe+b/ITL+/zlwmGgW6/G03a4gFQ4rFjHoAhp1UdhCF0
/VYc7tbffo/Qsr0EZV2bH7eXmvjTDkLcbPsQgym55TMswHAoNCiiTV16aDmgU11u
TltRD8vGBzmi8FVfbLWETWGS+2632QLwMOKkbmDgQ7Eq0EGAHVa0+dX97SJ5rVVo
mq7D1hDYMLWw5KgRDriq05WqZJNTo0FY9r3FCrM6Vh3BUpWhppJzmt3EPSEE42s0
rsczjQgPhYBz/9Tg7S7rKiuPqu5yE6ajcW+nsbbcKg3UVhfuiBJhNIKNjMaoTJ4=
-----END CERTIFICATE-----
```

3.2. Certificate Authority Secret Key

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADALBgkqhkiG9w0BAQoEggSoMIIEpAIBAAKCAQEAsZdoYbyCT/k7mwCa
hZBpL+5Yakhbj1P85CXD8QC3GKbHNcbJ+Ci8xG6nPpltDK8Z0nbz8wVGjh4kCMpy
Ohmmn/hm3eK/xhwZKzrpfGm8uSkPuHkMA0XdAJEOhR91b1w11ZOaKn5WRtiFI7Rr
Z5K1SDTgVdd+82+f66q7Mjinas+BRaTsAeoxKLq5gtVmgI3/TjFjtf/E3aVnWm7f
fEByxnFZf4wWyPo7sKCw3Yh2xhnqLzsWN1Vw15bCJnlwmvrBCpluCxtblNb9W2y6
KaABLy9qpK4kqc4Z5A+4rWMwuOPZV17kLTgmkWlGAD45Nh4EG+FNV24jcQ84EX+C
qqAMPQIDAQABAoIBAHs9DbOdZHTpCOMEpTaAw23+oZ6HvfoVl44fYv0QuP7DZcS8
wZWTd4N9IlQ/ljxSGsJByAJiK9cdtXXgPypweH/UmlXqL5jkENc+F589pTh89SrX
3W08AySMhR3+ebkgrT8cIcTRTT/2q1XesxX56hFEmFUZqUB3uuuI3ET6qbtlQYOx
dwsX3ZHH9rxzYnL7OiAfn26u8LHpGwjzPDfvFVX6rV4GAdCKSG+uySEFDm4kGRcL
Hyn0mwc5tPL/MEsatWv0tiqBx1KLM4qdiZZYsoftAocqo/W7NPiPd/AAyCzafl9n
g5+bSk4WAxn8y/QXMVvCcUhRTg2dRCZvbzyzCyUCgYEAxTXVfdEMiy9Vzq0DIjuj
pJJsaqO6PlWfvcJWKNXBAS36bsH8Y2RtYu7rNzw8u6YctfjyW4/6WYVJ3viGVEAC
jCzsywTvJqELkjWngGnMCi+AXlWcjgGsZq5yRC3HaJyD7Z7Glk6/kgQpBqfnSt9Q
OFb/go3rK36dA9gTPbHllk8CgYEA5oha1VmTNnR63J03On1XkqCPdfccFTiR/6kp
fKMiuMd41C/Wrtjcb1ODz8+K23qrOOlUSMMnKfcw+O0GOaFGgKaQ5BOwKvQVmL5F
Ix8bpRUcOCyoaROu92T8ayya9AZFhne7oaZj2tsB/t7vOpKn6oU5nukhwQ3EcGCO
0PafHbMCgYEAqcB5EF/NiFEqb0iFlgX4CkTvhauBOP7DDbgmKeg0xispkgTwly1u
6uX1GgqDzJJjzE+Jbj80o7ITsBYEqqieiMJy4R5SLNIa/7OnhuWKeIoC2TCgHaxb
Fde7C+zL5MQ022j8T41hYPKrzcrhUJWAm75nGZ3HfBz0Usa/aS+kDAkCgYEAgvXH
FBhUxsSY3yb4ruNxkjxgAxWkAHIojmIczU8ndGzsuS2L+bv8TcnVwYIXUeN3zVbP
qJ4ka3Sff2m29ZomoQL+oHKGy3/pnOHKCM+tNrStWUQVT8v8w1G9C21FgYbmjCMM
liId68AqfA1NPar+dP3F4/5wTGlzxJs1xoOzlH0CgYBWYkSXnbohU41XYyRfEz6T
dUhTyQNTR2kH4hEPsSvi/7jCaMe5ApLyqO6hwDMewVT3p8uUYx5hfUqoZtaWlQo7
jUzJsSgzmMiJ5raecCzSsae6f/BwsxRpgu5+Ca/5F5X840kGMjxbMN/2gBPdeBWq
hZndvqWgc41kEMuIVKdV2A==
-----END 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-----
MIIDzDCCAoSgAwIBAgIUaM19lySPCQyh61J7nYsAARDm+TswPQYJKoZIhvcNAQEK
MDCgDTALBglghkgBZQMEAgGhGjAYBgkqhkiG9w0BAQgwCwYJYIZIAWUDBAIBogMC
ASAwLTErMCkGA1UEAxMiU2FtcGxlIExBTVBTIENlcnRpZmljYXRlIEF1dGhvcml0
eTAgFw0xOTExMTgxODU0NDNaGA8yMDUyMDkyNTE4NTQ0M1owGTEXMBUGA1UEAxMO
QWxpY2UgTG92ZWxhY2UwggEgMAsGCSqGSIb3DQEBCgOCAQ8AMIIBCgKCAQEA04zK
35E5NSXLMjy1RwBKrerfEBISXze1KfRRhFXVoGudB4d+2a82IiNrZ9xGjiM8eihw
MnssK89PrrMZTxPqOpvS20MSfECtOV+v7EXxVqDHLdWd+OhTMbzxl0eL0Lf7NKFf
e7B1PfghwDSy/ti+vwfUEOZZqMem870ygrEbOrEBIg7OVe0snFXhlvqoVXzi5Gxz
MgNi6fUMiegeuJPMOWWfmwVC2xsvvMHr4X3EVUZ7UcMsTA7imtZv+5Ubxgh+0abK
tCLL5Tir9yvdlQplpHFZLiiJq7EiB7hYNY0SFB6kMuoYkp7TCBc1Yi7CfohVh+rk
ip8jgjI3MK7bdQE2zQIDAQABo4GXMIGUMAwGA1UdEwEB/wQCMAAwHgYDVR0RBBcw
FYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAPBgNV
HQ8BAf8EBQMDB5AAMB0GA1UdDgQWBBT/Quy1JKgeDOfjF2KMSbJlvPEjLTAfBgNV
HSMEGDAWgBTJ71DoWMkJCyfi66tyc5AhuiPQ4TA9BgkqhkiG9w0BAQowMKANMAsG
CWCGSAFlAwQCAaEaMBgGCSqGSIb3DQEBCDALBglghkgBZQMEAgGiAwIBIAOCAQEA
bcGCz+qLDHbmZGkVD+TDqqw+HTEeKDcp4nBRd+AJIxNBRMnhaaaVR1E7lriQZJxE
mpLW/EUWoXi8xUxMzQlo2o/8srypMQCdmBa9ADaUXchSzaW5G9eSWxCIRsZI+/r1
PzBcgXrNyIb/rVV/hCt22/oidcJfCfXNNlgik8Ec5amGadOY8OlgXU69W7o1brHZ
dIV7FhtfIsQVvtJ0VZwr77CU64X6FkSQUpgJ2iu60tGmR5ZPfl/77SzZx87/BTOL
55LFgp4oaLv07hkjUTxLa2aakqgSHDJwdy4THdHQokJJqX69rSzLup4i/bzAyn1S
2O/BpKwh+84PtgHvSN7Cjg==
-----END CERTIFICATE-----
```

4.2. Alice's Private Key Material

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADALBgkqhkiG9w0BAQoEggSoMIIEpAIBAAKCAQEA04zK35E5NSXLMjy1
RwBKrerfEBISXze1KfRRhFXVoGudB4d+2a82IiNrZ9xGjiM8eihwMnssK89PrrMZ
TxPqOpvS20MSfECtOV+v7EXxVqDHLdWd+OhTMbzxl0eL0Lf7NKFfe7B1PfghwDSy
/ti+vwfUEOZZqMem870ygrEbOrEBIg7OVe0snFXhlvqoVXzi5GxzMgNi6fUMiege
uJPMOWWfmwVC2xsvvMHr4X3EVUZ7UcMsTA7imtZv+5Ubxgh+0abKtCLL5Tir9yvd
lQplpHFZLiiJq7EiB7hYNY0SFB6kMuoYkp7TCBc1Yi7CfohVh+rkip8jgjI3MK7b
dQE2zQIDAQABAoIBAQDFqqRVSaielHXMtxTbBtbAstlCduBbv/2y+erBMEKv5l2P
j3djh2eZdmcBYL08SohTzD0prhWTyd22avqW/RC7OqZG4eD/4J77IQGMT741J310
wkkdLlet/dHvfJaTq5U5lB9Xv4WNJbDDm3o0zelNLc9lCxdzsTm6PWpY24uJxe7J
iwOyz8tLXgjLX/yQJOZOkXMbTC6jj0ZZHHdpslgPH0hIEMlLZ1HULG3Nxk9Fh1Yx
OM0Pk3/6FzmeZ6sBE2srH7cwaeJ3v3cOGeo37ww0eVw2ETdPlo0P0fBqC1RnkFU+
upt9OXaBDhT7T8hXWHuIHt1w213pgxY4RDYhnxKBAoGBAN06U8LQwMJZhZyzArQg
1xKVwn4GjdCY/2dVgFePmMkrHq8KgyXpe6drVrElq4b9RF7Nstt4tqiJr2+vMsy6
9ihIgSIfyaPCa0/WtVP9youzF+H9nHotNKs+Q8yMpTl4yk5DaHXk08J89e4Zma97
C4YBYOolK4DKU+mfvyW8DUIlAoGBAPTNDRzAzpP8ggZ6NtRh/f8MS2dHY2c1IDZI
6Wf8LKccbUT7F02BGNSBpydLFGvy/s0zP+XEvmsBllr+IrEQzBZLkF6u/7svHkze
n6w2+XeRcPDQAQJ/YaOPHZ9kXMp244H4EZqvtljSron7hfV4Gso0ktFPoDjc9DoW
Zxikrj2JAoGAWDtdEMPlPR4rNdYHbAP1A0qLaWv/v4RlyLbHGyUAUKtL75AHwmUe
liUvTDOz94CndhAgF3xLjWhseeSsJA8lAef46L041IFD/3GonDkKQTFKgy187RV+
fhW1QK2PcB6GwTQNQ4fiFR11kGLRcrVmYSnHl1r/wLvxP6oguFIKD6kCgYEAo6EE
KLn/2w8nYmkCiUfO3VI8fJZNLUlndKGb0jPPLQxlRXyIgPfPvwvCzRL0XYuZIVQm
W9D8bs4q0DuauLw/jo+HuqJCsb23BS6xkA1XBsMiuPRwGFlIzGj3JfmRxItfWxqT
uc/FlO2OWRDU49UaIxqtIFeXAys93C3pT6GUDfECgYBn3KLqvGmCHvTpWzGOH6lv
ABpux3YQFKxI0KtNg8U5lJMtVSTd1dHHwosQNiO6jrr+06N1EKB1w12DUWhTNb9r
GEiPX1h7KPZocVNYm8xdaynNu2UFNyjvdnPewv5uXz/PW1BEvfT1vWA9nZEpZzZE
WkfjBtiQpGhkOuVgrj1x3Q==
-----END 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-----
MIIOVQIBAzCCDh0GCSqGSIb3DQEHAaCCDg4Egg4KMIIOBjCCBI8GCSqGSIb3DQEH
BqCCBIAwggR8AgEAMIIEdQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIpDrb
dCxhKlICAhQAgIIESB1zFYAxN8dSKVt4GIHWL4QgzrstGxhClCrdgWt8FY6GYjXw
/WQCgyleTcCfws05fv3rkWMpItBcuzkK8be6xAjssRZXR0bhBBvjKbCw+62tLtkq
uiRA7oxwaZO+2ZYebhSkc7AyQkkzLE8aY277ckIlNda774RH6qxxmbw78drgoEMx
ssp93wSwiG40tBpX1tCP0EIK7RyFfpTYhJeIFPujLIJ46Lib8k5TobdWXBXF1Leh
yswtxLt4tItjcS0fQeSc9zsXrUDLVglUauj4HckHl6WO7qp2A4sV7u6Qq+F+m5cf
7nhOs8qiZlMsDnwV7dw90yePmFn8qmIlm6d7/ySuCHFZoK8HN6ye19UUwRF7nmsZ
FCtb5VdnC6KzsPYSmDDfFUTkUIw59L8SLQg63S8CWAcveGjKrpC8D1HghPFM7YgK
cY7xag8f3KIUVVlfhW5LBEJuEw9f9r1tf3amLNJ0xEK8Z5dgQ13yoVTcqOoBDfD2
1+ubJsbj0y41jPLOQZoRqmnAnoIIapqiBsljqLhKjT6W6Jd5Vw/wi8CESxbYFO6d
fkx8tEilQgp/OgIWA44tTxotuezWxyUPrqvT2hOn9kle9H9iPN5hz4QEFtzOQbhF
5L2S65E092RYD+kbqdnNRpptVjbcZLj/z8ZjYnktGZgFILha7skVih/GhFNrqDgm
KE0x9v0e1MTbiGuthYh5YOGQK3z+zI68qRopalpTm49kf49Hn0oA1/Qyr8k5ucO7
0RnN4979Dr+hARd4W9eibQoxhcITqnZ/AFkJKn3t1BiEAPBvTuu0FpY+jQOs9cQz
wjSsClw8e8NUbLyxW5o7VyrjIK66IUMFKoXtq+G20qm2xob7XrEO5HH/+Q/7uoyy
Hs1ld1GdZhq2RptndYWNpkcdHlREXCBTbDrK3UAyjHTm2qPm73JuMeprVzjJyg0a
Iw63evt085gUlrygZhYT00xvBp3TM911+2CEseNRh6I4tn5R64x9R60z0OH4+WpL
Nqimcj0pEB1DPkdvntLB3yWFuSc4rAOYtmvlxJlUuZSQZKU4dIVY2Jwygz6B/Ioi
7GH7R0KPfYqs+qewPtQ7DvukR77SGFaTnrUKbmIx7yfzWC6a6NgsLEB/+Zk4MNXc
+1S1JKHf7nkT1m+0gkJXkk7LimO+n4S8cymbJtXcDo2ShfsUqg4Nh/5h/vdobv3z
VsXSvgB7UC5PfupnSyAX51OINBu1rWLlJj6gaH4FfqzSkeH2otD3zZ+zeQ71zd4/
h37fRKuoC41d8RKcl/DTU3cv+8ACKm088agL8PChRBIwT2Y8pS1zg5JO+Pxf+Xwn
4fKzI+T8PIOiG/XAgBfgGmA1vmpEK4frfn2JamBtcNgkf5LF6UbR/KuOb2t0Joju
lFMHEwHL8CXvSJJpLqZhlg14pDK7kEpTpVmqW95coyq4JCIC0OdBhPHFiOAIP7VN
/cyPjrkwggQPBgkqhkiG9w0BBwagggQAMIID/AIBADCCA/UGCSqGSIb3DQEHATAc
BgoqhkiG9w0BDAEDMA4ECJ87XKiG3ZH+AgIU8YCCA8iVK1z4QGnBk99uWB7qh+Rs
aTPEpuJfDU+yfQPq+2u3gHMU8iUfR8jyDuAdp8rUE5InxVd/rlGPUKqg3/E+DBt0
uwL4wQHvT3PfPZT304xpGxirktZgoJc+fA969OQoOvc6cJqe5m6fxvCGwBLFRluI
xThRfvyouoSLZoSoqaKUU7nszFNXTva773hvkdyf6P7297HCL8co0WvLikvS31dL
+snz/AenqtOmVj3AVpekYGA7o5ce6xJT6HK0HiSPaL1Y7C2w9auh0ZPfNT0eeb1Q
v96Wk6x9p5DTXcgrxGtz52laGS2OU36zVMyMFrHDBSBjrHbVx+SADIVStVghYOLk
dOiY8vCtB1MKWUg4eJf4MlCcOrj0kD5PAMjOZ75/2iZBlJocE7xCUYJv/IfiK8ku
tEtDhnfNKKFbcbdZP1WatHZ9Z5xQibUBtsKTttf7O/NtStuJwywqLF2mygAhNFdS
v9LQsrbTB9vam22J+wiUlnY/XhPCPgsu97N7djKhdXH3JfQjNj7qM1YZbw5sP5Ib
+XXJPe6i7oJwAtLD1Y/Yb8OKZAF6xeaQqrDk5Ebfl5/WqAgUYKC4Fbuu19HVnXRZ
Z6DlwGUFydvOGXxAIQAXJKzYIaCJsR4LnbD910YBRvsJ8X/O3Ms9t9rxX+Ub1aJp
9gLO2fgj2zMQJ5LLEVbe43bpdd+1/Buo2vMT012T3qC9GcTKfu7AXPTn24zuXkq0
Oj3MP4i954FqWKcnBSffSsQ2L1LhpqGWGZagX2Y+na4VU1MZMw2hKtJNF+g1nvGH
I00nqgo3m+4iP3vQWJgZ9dNU3qnYhTRKUbbZGQdwBxLYiT2chKa4AEdrQucH4pmW
CaK9dlXBRbbGCTFlWE6ziC78u2+PE/nkwX6Jb7/9jJ4dQ6GxEfZjVWngdjrJfVCF
rhp9efCtYOoiNb4DfXcaVZagVRYh2fjKOFiileelNegRd/yAlSl30cZuSt59inpH
nwg/jPzmrbhSZ1kv6XV4f9nZ5uoZEghFl2ZkWJyv9wYwGouHQzV4Oqo5qRXO/EIP
E1N03KnuCwB5efJdiRRuTUHlaMF6MaSxOhkTLedwzHk0eNWGC+0dCf6RZ20nd/OD
jcL7bQtcWXohWXxuO+v9Iidvesg8NCm9+8hu7IRhx7nmD39uB0uFiPZXvUzQ1j+b
4Zo5oc6NiMxRKuguuBODVN107RhSeG1fRWGwJ+xx7GimT6tKQ1AsRP/9U/lJ+rk4
CAIrcaLCFdAcNnnvEUBU7He6Ull4Qr6Pmx7auGcpM2b/YDxQN+3oZTCCBVwGCSqG
SIb3DQEHAaCCBU0EggVJMIIFRTCCBUEGCyqGSIb3DQEMCgECoIIE7jCCBOowHAYK
KoZIhvcNAQwBAzAOBAjd2iv64ENk/AICFC4EggTIDGMDlVUkL/IQJrAhyHFDX426
h7uzqUfzkDIJ3nGMZawga2QgCy+viuyYIvMkz9i8ikKOLjyg3IP+ZuLk0Velh5id
Fj6ivGExReWvjhkeHs+YODRN6I+83p3Al4bi/bIgM/I6qmcpzIAPhZNJgQwByDC/
1c9gCRwERX3ge8g5Rc9V6KKyy6rlJpdpvi5xX7kw+FUBMIf9xP18wed76UXtYm/H
8ggTe9g0qPPfKyRytkgYhP8qZLgXU3jmbc1OvgsO3cX+zJPc3nR1ZTIk/hn1s49j
mzZnvzTHmk719SRViO3arG/WBT72Y1TTdYI8gP0c9uYIJ+fp8JNLZdgOaqHMDw/l
Om+MCMLivRgry8TrpwO6N5KaktNO5cpVeBxiHMuHuXGDeHoG86om3Mp3WCMqsDo7
b+tIxIaz2aylubjJC6zxp5ADOgrbywewrVN64EgnxsnBYA01zM74TTRJMtRns+LX
```

```
+uaXNzPVHkLGPTcfhc/+nMIB5XnFwxanSaiGnguZyjdLnPyXI5aT9Zkcfx86X0QZ
PJXJ3lnLJf8f1vrNMEXUmBNPDQOhXZlsqZR8Nuznn+8Q5Tiecuoz+HfAy549BNNP
GKFw8WDUOSLDXOrRO+jvEt6J2GX7WTwO5YeBgb1f/XWwLBb6qFGhndQyQC5Upa8i
yT0h3YlAQm8GgNbj0PXGxg/0czUc+fi6xFJsrsGWS++IwEYEdu7xFEM1+kgw7OvY
KDXE298BAu1zW0ZVcS0U9S/D2QrZzt6Bpij7vIL0gSThQ6rvjbO4PHuJuLSdV6gK
+xzahqAKzO6qN+TBrGzIHindNLYcsOXm2NRZoheTAPvhJzY1qlELlW71dcXDSNFK
So81ZxSpBAYK5O676QpP3JU6/ruWaW6KgToOlZCHJG6YPV6LEG56AFrSQdgyklJc
Bpb8V51cB97pWp3N3C/gVqkr71F+hrM+T5ygRTxakMdMBLTvG7B3febGT5SuXrPM
RuPPsQV+DbgCIZKDDoEinRbnER0VZE4iox2ZHOxBrbO9uTDkKlhVNWvSJNDA1eJW
oItNQcqiKQkREdbkSGWA8tYUzgn5MbyJ6yQ5raeYh40zvqvSaYFWxV3WMnEEstcY
Z9GgdjQkxf+RonMy2g8vqtsHm5ryRgoRKLauaEHC059mGhhc5JgziJghuucUMZN4
zsezVQGpzwbqrX+x6UXbRBzRwBr5YGXah0Lescuui691tyKlPybDl1cZ0duofox2
MxKpQ4gzJidwm8iYeyE3fNbr93JOS1NneXhQ7gnBYxFyD4ALNVDtM61WIkWpf2FL
bBCZcbiIi4MaWSGhAgChS6AVS+vMvPKoQ2zGVP0bR2moduxGBSHWUp4PrcE47m/K
Eq0esce2dr3suzKrJVDKZgBeO4KRTR+UIVV0NH0gr3rYH2IKMgIIY7KIwR7z2+rw
YymRekxfQW7zIxHAPYoC33pHHRWEXzbI3vTbpIp0/AkQ3iK1FUx1iVsG5dCvuvNJ
ivgZM68SRNREshdV9tazQ6ea1eNkXIt1VCleK+alKAI6fsaBG1+qr4yPxBu7wNUi
GoXz5vs5w7FWcv3sNJT2TlSOjWSdRiC8LvAagaxA1e+p5ChA5eNRlqpM9LYvpMH3
3NQonqX3MUAwGQYJKoZIhvcNAQkUMQweCgBhAGwAaQBjAGUwIwYJKoZIhvcNAQkV
MRYEFP9C7LUkqB4M5+MXYoxJsmW88SMtMC8wHzAHBgUrDgMCGgQUx4ffmsHbTzUu
5I38Gmcq7ODXLQ0ECIDP5r/x8XxSAgIoAA==
-----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-----
MIIDxzCCAn+gAwIBAgIUCS2CS7BZT/YaT2CSLDN0yBRF/PYwPQYJKoZIhvcNAQEK
MDCgDTALBglghkgBZQMEAgGhGjAYBgkqhkiG9w0BAQgwCwYJYIZIAWUDBAIBogMC
ASAwLTErMCkGA1UEAxMiU2FtcGxlIExBTVBTIENlcnRpZmljYXRlIEF1dGhvcml0
eTAgFw0xOTExMTgxODU0NDNaGA8yMDUyMDkyNTE4NTQ0M1owFjEUMBIGA1UEAxML
Qm9iIEJhYmJhZ2UwggEgMAsGCSqGSIb3DQEBCgOCAQ8AMIIBCgKCAQEA4SwN1/lH
1IyS1ceZTQtBWpP9mdnO0Ww/UJaOvkfqC25ef7QhjLyOXzUbl5IGXtcqP77YGBOW
3/9aFTBSZdURKIwQPmFLZf1nAIlDH39Mw6VWqADAsnM3gH5NOZA7+pflS/Eq2hMx
GoKXmg4WDXBYGnQrwdtfKvguf09ycDp1fBWyLG0IDzrsChcebKEqCg2+YAINDh5q
VgsWewcf/FVOnv02x3ZEaKiGElmWXWLjcQpCbawCGCdLfBh1UWNLj05R6AbFbnh3
Ec7qKbo6DkttH/Vzs/nZ42l6NtmnjqSEH9CwbBK/wbnp+RtlaPSuEVvxR5leRHot
uTo+QL8DlGJ5XwIDAQABo4GVMIGSMAwGA1UdEwEB/wQCMAAwHAYDVR0RBBUwE4ER
Ym9iQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDwYDVR0PAQH/
BAUDAweQADAdBgNVHQ4EFgQUa7CAjF9FUMyO4G0V+kn1rZKNppswHwYDVR0jBBgw
FoAUye9Q6FjJCQsn4uurcnOQIboj0OEwPQYJKoZIhvcNAQEKMDCgDTALBglghkgB
ZQMEAgGhGjAYBgkqhkiG9w0BAQgwCwYJYIZIAWUDBAIBogMCASADggEBAK0s11zY
t1Ac52MnHMO+HPen4EXpxmgy+gi3ROEQqtQCngOCSmROb6ijnP65a221yCTqymqp
S/SEqVkXv5lU/1qbBFvRlqkEypl8U28WVKUb3gGt90/12XSFlk45u0wrmVZcSn5m
lwoNv3Ahni/cHZjQqgD29AhgSCue3NjJ/287oPoNMFcYwhMUf13MIcJ6ow7RiPOd
qTfRCBknPfQqGrz0T15ZMayiW+ZgAm5NL+U/YV/uznT5mirE+VfGbz8WtQAzZcma
YIeHaCmff3wq8kRJZpWFSb6w2H6lclAYYLG734tqmsj1i2tmDVxGd6+lJNTd3p2g
+pjAwTPUXBXGP4U=
-----END CERTIFICATE-----
```

5.2. Bob's Private Key Material

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADALBgkqhkiG9w0BAQoEggSoMIIEpAIBAAKCAQEA4SwN1/lH1IyS1ceZ
TQtBWpP9mdnO0Ww/UJaOvkfqC25ef7QhjLyOXzUbl5IGXtcqP77YGBOW3/9aFTBS
ZdURKIwQPmFLZf1nAIlDH39Mw6VWqADAsnM3gH5NOZA7+pflS/Eq2hMxGoKXmg4W
DXBYGnQrwdtfKvguf09ycDp1fBWyLG0IDzrsChcebKEqCg2+YAINDh5qVgsWewcf
/FVOnv02x3ZEaKiGElmWXWLjcQpCbawCGCdLfBh1UWNLj05R6AbFbnh3Ec7qKbo6
DkttH/Vzs/nZ42l6NtmnjqSEH9CwbBK/wbnp+RtlaPSuEVvxR5leRHotuTo+QL8D
lGJ5XwIDAQABAoIBABKeXOqtzxWxJfcNUQzA0H+X2xFcpDBG3hlgyZ7MPXsCfkfa
8ic79B3FO2nWBjbTXcf1lNKw0/njmGRGIZoP+yI6KqGt09k0Ec9GiklRclx/EGJF
5akbw8wZJXOMDJmU873KzDtJ+PZzM+vmHEayMmbFklSuOflImjemrxS+kLZYwS2d
TXW3b2d7vxGPKNfYEmg7SSg2xsZsORX2S+ORyTQDQEF4utCU1tNrmRJkuy2UIUWZ
LUZstkgjMI3ztJ46wpL4NyO2kTEhMawoSmIxDgHztXWzoB8nFyuSzJwYg26OvsTZ
CVOhyTGhiALm0ma+7Vas9MFyRnFKkQd2ajruxgECgYEA+Z3Hi1oZDDF+qavmxPeg
gyqC9OMyH6pGbHqZhfxVLm2ZPdhCbTYV8e7YNnBK7dX1o04BAA/OS/Q5MbF50sAJ
8Peqeef6FzJ319S+DGfTlJ6EIZhp4K8ysgrQgSGaI4RUtAaFIHm1EsoIG1X+2HJJ
cT0k5VteU/1kyXLuPeBbJwECgYEA5u49aUpfSEDBV0KJPrZDXR0ib6J+XKkTWAeL
ImRC+5csf6HSdocCSOsgaZxqOf8TWmaOSpEQcxb9m4ioNHRniQ84Dk3dhdJIh9n4
g+PQUa3QxpXFdXVxrSp6bQJdNqdhd9tt3izNe2v7cw8YKhvqSz50HwnwoU0NhDQG
Q4mPAF8CgYAf1XVrWjQzj+RdcyTdHc+EqtlErezoiOiuUPxfUAz0/Nk8P+ZI00r9
Lb65QpzrtAu9pecOwPVITn80zTOCIyehaZR+M417g94w0lribiNXoterCSsHkpBe
kG6C6Wwk921uAB7eQ2dKXCWohtEXfYvMO0YHUh23jGtcHaIwlfpKAQKBgQCbowse
kDJBVus3LS+kZWBnPAB+bmxtdMIFvSfHaP0/5PXnmx9mJL2keVsh8nohVkkrzxyt
IrGMb31Cuspqd91joS8tbMsUqtGZRY1ZDkvTEKs5e61V6W5Qv+U83LAH6q0lA207
pMRkHzWbqRunHaM9TP0kAiX8ABtQ82MZV3daTwKBgQC2TVr+qLQPaCnvxGrticVY
OK4mtuveWJP04gO3mQZwbhDRzhWFpoFBHDev0yPxWUMM5/yYjm5xyHKa9gr3xmum
2qMHvRCXbvo0IpaxA8QZiukfUCapwojs+598VnQ74D+81gSkQzh8sM/NeHG2+WXd
mLVzkdz3FTLWyKnAQcA0PA==
-----END 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-----
MIIOSQIBAzCCDhEGCSqGSIb3DQEHAaCCDgIEgg3+MIIN+jCCBIcGCSqGSIb3DQEH
BqCCBHgwggR0AgEAMIIEbQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQICyQi
BIYtsOMCAhQagIIEQAvzXw/1WcnliaVunfrC1lE938KEKEQ8Z04VwolOliHO2gG0
RypRv45m0A+se3fWDaEJ1nQeAGP9A3qHGYlQSwIDNkUGvk4CqHv0NXOxjdXemhHu
IYs4OxYePflGpdjiqx4dtI41bowOATL/f3/X3Oqu3m81y8W++HN53aIzoWDkT7HB
PGFebll4q461WqRxs/on2I763xR4iqqj5RDgLfE1K+pBdpzCqWTnjCYLbakJVz2k
dvmADPEIEs8RDjl8P86VlyIN4sIVy6LoTFg2Mr662IEz71DoF+87wI9GTTQS7xbw
kuUfH7Rc1QkmFDZ5ppFZLx/sGG+j96w+5+4ZbP/rxyIye3O6yEufHw7KztqSyjEh
CVMG2wB4IEZyb1pNhBpTk6hk+5vso944l2XKRRQdz3hupS57SR3fMA9kBxnV4K3o
H5Ju7+Gj0rfOEV/0XJiH1j5o1iZPIZ8bGHFSzkoJyUj3aXYdx9ajZUOShBmuKQpF
jemi1daVgyWTUXCj+4BKr7qayCVi/a870bdZzGnbedfbXWYnFLu23ympw/yuT/Ez
9gVfZMiwZQGPdkH+oHgaZ4L+wmDY79L2ezY2vsD75ig9P8BRwiNV1I/2G+18CeCE
cOBuIBDyCiB1BfxeQo6HxrytUWmDO1B0HwJcEtUD4lOf6ntmKv7UEE5wD9Kp6AAX
jmV7Zb6lCI/fApJwhqoJ6P7zJhgURzb8/buYYfuDzJuEiwdpR+SLRVrrRZGkDRRL
dCJEltu6VKiUgCE1jggOi/aX6cLCkejCl0uoQHCGxRRa8F03COq0aBlq2FjmwJ4S
OWQYig0V44AShXpb+B3IuqfEaLcn8C6CM18l8XzZSixwmlrFsfmVZnEFN7DnBcIc
mf+nhBXeBezVaK6q1KMedsUTbMXtSY1WKZFseN2euzQutA682LQly6MO9sp2skSZ
WchX6NaL3/43frdcMWShEWRGBlOHL2DRxj8WrfpEEO7U1SLoK6MAPrZRwj/+hTSU
zz6nYrCxnGBedTnknnHswTvllxN+YviwiByLKykH6ZRml4I9lZYIlZUiwC6wGq2E
AQas3B75bLGhnj+zRQOvw+KwmTWuiFPUyYnpBJnwthxeS3PMAoUcoB7ybGg1FtSo
C26PxhgNMCIa7XZ8e/wlM5QRDE7jemgjaGIh001shhxiUW7c9Z+rTIZsxV+DJa99
UGGwjRPurlAjQE0qLtuA+iIMx64IsM4kAnhX13mR2yxvEBw/loZjxfvRHdq4zgPr
ypHVKZWMdGxxDDHDamc9wjNm57fR6TeBnJLJujliV/H/Fy/sYKtV5Rf1pf1dfL/7
bmY/gU33jW79CTF7Dc9e56edrgP3c101Fhy7TqSFQdgRTdKwthi3mGanH3kPPwMD
ZsO9mVpeh4Cr2DCURIzOW+a7XtkKINsnFgk6xbrs/ORPjsS9IYbf2FcauAlhMIIE
DwYJKoZIhvcNAQcGoIIEADCCA/wCAQAwggP1BgkqhkiG9w0BBwEwHAYKKoZIhvcN
AQwBAzAOBAgg+R/Oxgf1jwICFLiAggPISORX68GniJPLQGdtk1jleW+1U3SiginW
SHaDNyhBHah1xaq5PXfRkISW2PW/mTn18Jiu2Ww0FJEG46VLBEn2XxcxoTqybhxK
oq/r8AW1SAYnycs2pMKZLs56nBA05w03YGuX3mpUrG2I1BWklwXVl2pjgBAb1EEC
i9FdBGOpifo7Azjnddi3o6QAmu1q2dJlwHWTyWkpLdzFWTQWSwrbN5QEQAIDefEB
ABAYGHkYK7r7IVevIoUBIT+8onUd5z3AjA81+60hMaEE/4n9m4X+iZfZD8ieUhHs
jP/IcRc6S5Jzc2Dyl6k84zO5bD5od2GFAUVeOdSlxaN7R737wgHatlLG1yUqHW+Q
TLCDrOzxM9/By51BnXocFhkFWWqs4Lrj4quwV5lqpBoyyrfo4ssHzB/PkG7iHrci
Vh8RUvey6piheLn8KAqxR1dTXx+FdY7E2aPXwdaOVZ8ZqQLqC1lh4YIk7HIuEfqW
1JW6EYmD/8SiqTXW15cMhNuZJw7ho7v/pw17i5lBz5l9tJYRwq4ODIxU7XwvydIB
qV+paYBXwqWdL98H5sYC2WCp73jj2ROD2IZUd+RL7JxlM6t/Ilf01GQWar4xl3Rc
Nzw4CeWPqrAOsjOOWxjgz4nAJkCI0zoRIzUc3BRDkwhg/Tb5YbjyPxTJvDwtyhy0
x9punubjChjMckIyJ7uxYcYkWXE7U1GCz6Cj7vJmOx/CSX1C0KXBZoyqHqDaie1d
wcSDbiufy9FOkS7fjx5G+865rcbjCAnSZRhdnHjnKG3d8zTKKcP7aQu4DV2orzr1
G1vaEtLjqi602dg0FkeEyLjvZOnLeMhj5pyyBHQp6OW+rlLSoY1jqeMhLbIubPqi
OEAPBNOP3ntMo0T950W7xm/MEEqUlgcm8vnbhlPjEagCaQNHnZwnc+A1WS24DVk0
xaCeyNdUd9OuvIvM+b7mgR/tD3LFB/EwG11plgDD3lg39GZxo6ioClsu88amzC9E
EZ5uN/kZUT9ISqvgCXp7IvrwXWuNqJcQg8kAJnkq3UP0nSYpWAq3XliaXNzzN16P
uG8d5zZQDVWaQAQeYSdNd4A3S2CXSEQZpuR76Rb0mQ5d9UlweFwZXwOqfk/0l+Br
Y0WpJnlOVpHfuaC/Lq1o8UkYfktfruR+8HcOBW94YqjktoQ4JnzDKB6NuLiD7gPZ
cIa8em1hCb6G46Hed3DA3CP9FBkwvIFQotvXkanXwlCtFIty+BLaR3WkCo+XnTPJ
wcCnsNj1fUT3A5jxJcaNqZ50nqSpUDpywqBH2OnjxWswggVYBgkqhkiG9w0BBwGg
ggVJBIIFRTCCBUEwggU9BgsqhkiG9w0BDAoBAqCCBO4wggTqMBwGCiqGSIb3DQEM
AQMwDgQIa1JMn8WZhDUCAhQJBIIEyG6S+HEHperIXKg4B7Wd6qDHvbpphQjYAcxo
aROYpZV+JI7OtMXZgcMIFQUvR3aV6XvAX6jDMSav4SDEwq9PEGErDgnQ326mmcl0
+69++sFFgYw7QRDeTzKbm46XEght5syUT/4/qHGse3nUw6dSn1gvKV1U1QME/diq
Hz2SO7bDuPYYhQZe5JboOrW2o+OZptc/QYh0a+4qJSi8/+eCFnknSZV4fiKHpU0+
a1BpwnbHeQHLN18VsQhIIujHqLAssPYKyTExXk5fqsiKs235Xn6DdCpMznHtjbSv
abeMVRhKKHxwvFpCz/3NdHKZPzPXu253/24IxiEkbGCI3HtwLIup2gQ2T1M5wMSF
Gv1qn5nPK4PO+ryfFUKwIYbRcZRTXRXYVqYtGT7bO3fsp3hGXbI2W3L8C9JCqZuf
U4kH8lbzfHbasN4n4w/Odzw808iPK5pRji497gJUATGrCrWPkL8sTz5L3JTe+cql
```

```
kd30725f52e8oxBr1ztXP2dfCUHDiIcjNPgGHedR6T5p9f2St4MDXhqgDeVXJoTd
TmrIgo42SQZ/qo9LmUCmiNMjc54r0pLJAKJq4p2rBHXywEg/yVac7m3ZLvW8Tt6P
spe/mzwPGS/41ar5XB5SC06kDYfuH4mS1uq7671RjJR3f7W4L14ZbP6wpvHVkQxI
PsL2DfRMQ36SRiU/H/b4ndxweryKwh2OvXaNfay04xEJ5UNwJDBk6UePTiTfsKxa
OxFmOYHdO0IcdwvawwFbTcK5E/XVgtrjw/XUFMOqZgsouRTI0W1Q59vI2ftiz5fE
bnMN7mqhkRDJhzVuiEiqa64bIsMQb2WAqFlRfijpQ8YqW1JeY5LlwHuheU+MtWdm
XtKsi1IAlV3fGEuguUKvr//zvWi/N6lpHcjB1v9Z3377Ff4qxtPorFibh3mRwW79
mDGkJUOQD4tB634Mvy4VHQoPMo6FEi46T3+CcM+ZtCvE4T3o1sk696OFuhsBEUWS
mzRDuCo5Ju41XZmLET/PFLU/aldh1M+oDRDqSFAez5DhB4ryAeUIpbCHXNAOpONM
l7vOli9Gh3w8500j+y+oddCXy5iESfVfk82Rw0CSAwgta2JonuD/rZXXFJyifdl7
H2HKbbdCBXP3SfNRzMiSjAtzNDphNR3YzRwVBZqjbk0/5uNJGkAC7XFjwTk6jGkq
yZPPoLmpPeR21j0LjBlSKyREedAtMRPCp7sw/OwROnvAaJ1aP3Cc0Z8RDLsUOl0W
NJGPhpDno/zS/gLbsJiZZEnQTYc6zwa8iTcg3yabUjgnjFPimG4eYIgZlBHbpyFh
lL0jBG3D0bt4lhqb2p36FjminiAJrd3tE+/tyxn0rV9CAhnNVYL9bXGhFPMOmjhn
cpQkHkAy0g867AIDcw794wf8NfDagsp5lZx8pOf+UU0K62J+cE0KUUPAfs83rXiP
HTkAIjbSa0hzxMo3fpeY44v10JloigV8FTbjsj2k438o1bOU2fYFvkT2cD4f29iJ
O4g5bwiWs/Z0SCCaTjtH9BpQFzr0a4wc3stc7URnuEy096NjYbyevffIoH3r55Yl
zBxQqkOHZ+nZExy/VLQz6Zrxi/YXZu8Nn+X8bfa28NlJbRDJRcup1tFDzGs3+zE8
MBUGCSqGSIb3DQEJFDEIHgYAYgBvAGIwIwYJKoZIhvcNAQkVMRYEFGuwgIxfRVDM
juBtFfpJ9a2SjaabMC8wHzAHBgUrDgMCGgQUCBYj6taNz2Kbq1GVvRhDiwAr3goE
CC4G/pq+Uab4AgIoAA==
-----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

9. Acknowledgements

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

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