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

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

9. Acknowledgements
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/2XJM79WIQ370WPRVDomvz8wPQYJKoZIhvcNAQEEK
MDcGDTALBglghkgBZQMEAgGhGjAYBgkqhkiG9w0BAQgwwCyYIZIAYUDBAIBogMC
ASAwLTErMCKgaA1UEAxMii2Ftcg6xIExETBVTIEElcnRzZmljXVRlIEFIdGhvcml0
eTAxFw0xOTExMDEwNDQyOTMwMDkyNTExNTQ0NTQ0MiowLTErMCKgaA1UEAxMi
U2Ftcg6xIExETBVTIEElcnRzZmljXVRlIEFIdGhvcml0eTECASMwCwYJKoZIhvcN
AQEKA4IBdwAwggEKoIBAoCAQxI2hvhIJP+TubAqJkGkG77h7h2FuPU/zkJJcPxlCy
psclxsnKzEbcq+mW0Mrnx5dPvBUaOHiIj6Gvaf+Gbd4r/GHKr0s0l8aby5
KQ+4QwOwDrd0AKQa6G3v4XxXG7G5qfLZ2IjytGtznkV10INOVQ317zb5/qrqsy0Kdq
z4FFpOw6jEoUrnc1Wajf90Mw0I/8TdpWdabt980HLGCLV/jbbI+juwoLdihBG
GeovOxY3VXlSImeXCa+e1KmW4LGlU1v1bbLopAEVl2qKrrSpzhnkD7y1C4
491Xux8tOCaUYAPjk+HgQb4UIxbINzqRF4kqoAw9AgMBAAAGjQzBA8GA1Ud
EwEB/wFMABAf8wDwYDVR0PAQH/BAUDAwcGADAdBgNVHQQ4EFguYRe9Q6FjJCCQn
4uurncQIbjo0EwPQYJKoZIhvcNAQEKEMcgCTALBglghkgBZQMEAgGhGjAYBgkqhkiG9w0
BAQgwwCBiYIZIAYUDBAIBogMCASADgEgBSAAZviK0N77fodh22PS9Xy7m
/WPU1mX7bPhN13kDrV1we+o/ITL+zLwmgGwW6/GO3a4gF0r4FjHoAhplUdhC0F
/VY7c7tfo/0sr0E2vbh7eXmvJTDKlcPs0qgym55TmswHAmC11tV16aDmU1u
T1tRDv8gvBzmi8FvbLWEtW6S+2632QLwM0KkmDg07Eq0E6AHvA0+d9X75j5rVVo
mq1d1hDMLiLMsW5kgRd1so695qZJNt0F9Y3r3FcrK6vH3BUwhppJzmn3EPSEE42s0
rscjzQqPhYBz9/7t757r+56jwhich+nsbbcKg3UVHufuiB1hMNiNjMaoTJ4=
-----END CERTIFICATE-----
3.2. Certificate Authority Secret Key

-----BEGIN PRIVATE KEY-----
MIIeAIBADALgkqZkd8JG9w6BAoOeQg5MIEpABABAQCAEAsZdoYbyCT/K7mwaCa
hZBpl+5yakhbjIP8SXD80C3QKbHNbCJ+iC18xG6nPt1tDK8Z9b8z8WvGjh4CmPy
O1hmm/hm3ek/xwhZkzrpGm8uSkPuHkMA0XdxAJE0hr91b1v1120Ahn5WRt1F17Rr
Z5K15DgVdd+82+f6d6q7Mjxn+snBRaTsAeoxKLq5tVmgI3/TjJfjt/E3avWm7m7f
fEByxnfZ4fWvPo7sKcW3y2hxqnL7swN1vW15bcJnIwnmrBCpluCxtbLB9W2y6
KaABLy9qKk4qkc4Z5A+4rWmuw0PFZv17kLtmkWLGAD45Nh4Eg+FN2v4ijQ04EX+C
qqAMPOQDAQAOA0BAAHs9dbd2HtppCMEpTawv23+oZ6HvloVI44fYv0Qp7DZc58
wZWTd491l9l1/jxSoSbYArIj9kcdXXGPypp/wF/UmIXQ5jJkENc+F589pT8h9R3X
3W088ySHM3+ebkgRT8cTcRTT/2q1Qsxx56hFEmFUZqUB3uuuI3ET6qbt1Q0yQ
dw3X2ZHHR9xznL70iaFm2eubHLHwp6zPDPvFX6rV4GAdCKSG+uySEFDm4KGRCL
Hyn0mwc5tPL/MEsatWv0tiq8x1KL4qdiZZYsoftAocqo/W7NfPiPd/AAYCzafil9n
g5+bSk4Wxnx8y/QXMVVcUHtRqg2dRCZvbyzCyUCqYEAXTXVfdEMyi9Vzq0DIjuj
pJJsao6PlWfvcJWkN8AS36sbsH82RtylVo7rZw8u6Yctfjyw4/6WYV3viGVEAC
cZsyoTwJqELkJwGngNmcI+AXLIwjcGjQsQy5cR3HajYD7Z7Glk6/kgQbpQfnt9Q
0FB/go3rK3d6A9gTPbHliKb8CqYE5ohaILmNnR63J030n1XqxCpdccFTR/6k
fkMiuMd41C/brjcb10Dz8/K23qro01USMMnkfcwao8G0afFggKao5B0wKvQvM5F
IxbpRUC0CyoaRUO9U78ayya9AZFhne70az2jtsB/t7vOpKn6uo5nkuwhQ3EcGCO
OPahMbcYEqc5B5EF/NfIEqbo9FlGx4CKTvhaubOP7DGBmg0xispkgTwly1u
6uX1lGqdDzJjzEyeJb8007TsYEqQieIMJy4R5SLN1a/70nuhWKeloC2TCgHxb
Fde7c+2L5MQ022j8T4lyHPKrcrhuJWam75nG3HFBz0Usa/a5+kDACKqYEAGvXH
FHbUnxs5Y3ybr4ruNkxkxgAxWAekHlo1mLcZU8n6g2u5L+4v8TcnwVlYUXeN3V4v
pJk4a35f2m29zomoQL+C0HyCq3/pnH0CM+ntRsTwUQVT8v8w10GCr21FgYbmjCNM
lii6d8qAqINAPr+ap3Df4/5W1LgzJs1xo02lH8CgBYWyk5XnbhU41YYyrRfe2ET
dUHtYQTRk2H46hEPsV/j+jCa5Me5pLqy0whDMevWt3p8uUXy5hUq04taWvL0q7
jUZjsQgzmJSraeC5CeSaaf6/BwsxRpgu5+Ca/5F5X840kGMjjxbMN/2gBPdeBWo
hZndvoWg41kEMUIYKvD2A==
-----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-----
MIIDzDCCAoSgAwIBAgIUaM19lySPCyh611J7nYSAAAdm+TswPQYJKoZIhvcNAQEK
MDcgDTAkBgghkzBQMEAgGhjJAYBgkgqkhikGiw6BAgqMCwLYZIswDBAIBogMC
ASAwLTErMCAIGA1UEAxMili2FtcGxli1ExBTBVBTIENcnRpZmljYXRlIEF1dGhvcm0
ETAgFw0xOTExMTgyIwIwMDIwMDIwMDIwMDIwMDIgZjAwMjAwMjAwMjAwMjAw
MWNmMjAyMjAyMjAyMjAyMjAy
MnssK89PrMzTIPqdpvS2OMFECT0v+v7EXxVqDHLdWd+0hTMbzl0eLGLf7NKFf
e7B1PfgxhDSy/ti+wvUEOZzqMemh570ygrEb0rEB1g70Fe0sFnhhwvOvXzi5Gxz
MqNisfMuieejuJPW0wfwuVC2xsvvMVHR4X3EVUZ7LCMsTA7rjSv5+U5bgh+8abK
tCL5ti8yl0plpHFZLiijQ7EhiYNY0SFB6kmYoYuKyp7TCBc1Yi7CfOvHv+rk
ip8jgj13MK7bd0E2z0IDAQABo4GXMIGUMAwGA1udEmEwL/wQGMAAwHgYfVQR0RBbcw
FYETYXwp2VAC2i1pW0uZKhbX8sZTATBqNVHSUDDAKBqrgBqEFBoCDBADPBqNV
HQ8BAf8EBQMBDB5AAMBOGA1udDgBWBTFQ/IJKqgeOdfjF2KMsBjvPjELTAFBqNV
HSMEGDAwQgBTJ71DoMWtkyci66tyc5AhuiP0qTAT9BqgkhiGiw6BAqwMKANMASG
bcGtWdFLaAwQCAeAmGgC8qGSih3QEBCDALBglhkgBZQMEAgGiAwIBIA0CAQEA
beCcw+qLDhbmZGkVd+TDQwMTHEEFDcp4nBDrd+AJIgNBRMnhaavaVR171riQ2JEsc
mpLW/EUWoX18UXxMzQlo2oB8sryfMQQcmdBa9ADuxgZw59g5ewwXCRsZI+/r1
PzBcgXRyItb/rVH/hCt22/oidcJfcXXNLigk8Ec5amGdOY80lxU69N70ibrHZ
dIV77FhftIsQVv8j0VZw77CUB4X6FkJq3QpJ2i6U6O6GmRZPF/-775Zx87/BD0L
55Lcpp4oaLv07hjJbUTxa2aakgqS0DHJwP4THdHqokJqX69r8Lup4I/bAy1N5
20/BpKw+84PthvSmNCjg==
-----END CERTIFICATE-----
4.2. Alice's Private Key Material

-----BEGIN PRIVATE KEY-----
MIIeVABADALBgkqhkiG9w0BAQoEggSoMIIeEpABAAKCAQAEhK35E5NSXLMjy1RW8rKerfEB1SXe1KrRfXVoGudB4d+za8Z211rZ9xgj1MBeihwMnsskB99PrRmZTxPqOpvS20M5FECTOv+V3EXxvDHlDwd+OhTMBzxn0elE0L8fN3KFe7B1PfghyDSy/kt+wvUE02ZDqMm870ygrEb0rEB1g70Ve8snFxhdbqvoXvix60xMqNi6fuM1egeuJPM0WqfvmCVzszvMhr4X3EUUZ7ucMsTA7imtZv+5ubxgh+0akTClLL5tiryr9yvdLqplpHFZLiiJq7eIb7hYNy05BF6kmUoYKp777C1i17fOhVh+hrikp8jgji3MK7bdOEZzQlDQABao1BAQDFqgRVSaielHXMxtsTbBtbAst1cDuBby/zy+erBMEKvSl2Pj3djh2ZdcmyL6B8zoHtT2DprHRytd22avw/MRC7jiZ0Z4eD/4J77l1QMT74ji3Lrwwkdk6/let/dHvfaJaTq5U5iB9xv4WNjbbDcmz0zeINLc91CdxzTs6WPy24u1xej1iw0y2tLXgjLX/yjOZ0kXMbT6ji02ZHdpzspjPH0HEMLL1HIULG3Nk099h1YXOM0P3k/6FzymeZ6sBEsrH7cwaeV3c090e07w0eVw2ETdPlo08p0fBc1rNkFpU+upt90XaBdhT77h8XhHuHIt1w213gapxY4RDKYnxkBAoGBAN06U8LQwMJHzYyzAr0q1xKvWn4jgCjY/2dVgFePmMKrHqg8KgyXpe6servkGlq4bR7F7Nstt4qji8r2m+vsy69ihIgSIfyaPCao/WVPVpoyzuf+H9nhotNks+Q8ymTPy4k5sAhXk08j89e4Zma97C4YB000k4DKU+mvfyyW8DUIa0oGBAPTNRdzAzug26NtRh/f8MS2HDY2c1IDZI6Wf8LkccbUT7F02BNSBydpLFgv/s0zP+XEvmsBllr+IrEqzBZK6F6u/7svHkze5nw2+XeRcPDAQJY/YaOHPZH9KXmp244hH4EzqvtljSron7hfV4Gso0ktPofDj9cOWZx1krjZJaogAwDtdEMpLp4rNydHyAbPA0qLawv/v4RlyLbhgyUAkLtL75AHWmUeliUV1D294CndhAgF3xhrwhseesSjA8lAef46L84IFD/3GONDK7QTFKgy187Rv+fH1QK2pBC6gwTQ0Q1fRI1kGLRcrVnhsNhlr/lwVxcP6oqUGK6DcyEAOeeEEKL/n/2w8hYmKCIUO3V18f2JZLNUlindKGBbPJpPLQxLsXyIgFpPVwVcZRL0XyZ1VQmW9D8bsq6DuaLw/j6jHqu1Csb23BS6KxAIBsMuPRwC6FlzJ3jfnxItf9xqTuce/FL02WURdU49uAIqxt7FexAys93c3T6GUDfEcgyBn3KLyvm3CHvVpxG0H1LveApux3YQFXIOKtN8U5J1MvtdhpHwosQ1Ni06jrrr+06N1EKb1L2D0UwhTNb9rGEIPX1h7KPZCOCVNYM8xdaynu2UFNeyjvdmPewv5uXz/PW1BEvfT1WVA9nZEPZzZWEKfjbt1hOPkG0uVgrjr1q30==
-----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.
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+gAwIBAgIUCS2CS7BZTYaT2CSLDN0yBRF/PYwPQyJKoZIhvcNAQEK
MDcgDTAqBgkgBZMEbAgGhGjAYBkgkqhkiG9w0BAQgwCwYJYIZAIwUDBAIBogMC
ASAwLTErMCKGa1UEAxMiU2FtcGxlIEBTBETaIncnRzIEF1IEBdGhvcmQe
aTAgfw0x0TEtMThrODU0MDAbMDUyMDkzY2EtMTE4NTQ0M1owFjEUMBIGA1UEAxML
Qm9iI3JhYmJhZ2UwLwQgEwcgMAsGCSqGSIb3DQEBCgAwIBAgIUDa2C59uT3+xV
3/9aFTRs2dUK1iQPmFLZf1nA1fiDH39Mw6VwqADAsnM3gH5NOZjA7+pfLS/Eq2hMx
GoKXmg4WDXBYGn8rtdfKvqgj09Cydf1pFBWlyL5oIdzrsfchbeKEqGz+YAIINDh5q
VgswcWefc/FV0nvOx23DwAKiG9sElwxWLjCpCbaVCCGdlFBh1WUNLj05R6AbFbnh3
EC7qBko6DkttH/Vzs/nZ421GntmnjqSEH9Cw6BK/wbnp4+RtlpsuEVxxR5leRHot
uTo/QL8dLG3XwIDAQABo4GVMIGSMMAwGA1udEwEB/wQCMAwHAYDRV08BBuweE4ER
Ym9iOHNTawWllmY4WlwbGUsyqYVY4RBOHh1KvGUNHgAwOwCyYDVVR0PAQh/BAUDAWwQADAdBDgNVHQ4EFgQU6A7CAjF9FUMyO4G0V+kni1rZKnpqswHwYDRV0jBBgq
FoAyu9eQ06FJcQsn4uucrQ1boj00EwPQYJKoZIhvcNAQEKMDcGDTAqBglghkBQ
ZMDAQjGAJBkgkqhkiG9s0BAQgwCwYJYIZAIwUDBAIBogMCASADggEBAK0s11Y
t1Ac52MhMO+Hn4ExpIjmykg+i3R0EQqtOCngOCsmR0b6i+j65a221yCTyqmqnp
S/SrEwKXxv5U/1q1bBFvRlqkEypf1u82UBwKUb3g6t9/12XsfKl4u0wCm1ZcS5n3m
lwn3Ah1n1/cHjZqgdD2D9AcSHgCue3NjJ/287poNMFcyWhMU13M1c6ow7R1Rod
qTfRCBmP9qQ6Gr20T15ZMay1w+ZgAm5SNL+U/YV/uznT5mi+EvFgb8WtQAzZcmfa
Y1eHaCmfn3w8KKNjZwpWFS6w2H6lclAYLY734tqmsji12tmDVxGd6eLJNTd3p2g
+pJAwTPUXBcG4U=
-----END CERTIFICATE-----
5.2. Bob’s Private Key Material

-----BEGIN PRIVATE KEY-----
MIIeVBADALBGkghikiG9w0BAPoEggSoMIEpABAAKCAQEA4SwNI/HLIySiIeZ
TQT/Bwp9mndn0Ww/U0a0vkfcfC25ef7Qjly0Xzub151GtxcP777YGB0W3/9aFfTS
2dURk1wQfPmFLzfnA1lDH9MW6WqADAsmH3HNqZCA7+pfsl/Eq2hMxGoXmg4W
DXBYGnOqvdfkVqYuF90ycDp1fbWlyG0IDrzscHeebKEqG2+yAIYNdH5q9gSweWCf
/FV0nVq2x32EaaKIGELmXWLjEcPcbawCCDdLflBhi1uWNLj05R6A6Fbnh3Ec7qKbo6
DKtt/HVz/nZ4216Ntmmj/qSEH9CwbBK/wbnp+RtlapSuEvxVxsR5leRHotuTo+QLD
lGj35xvdQQABoa8nBdkeX0q7BvG3aW497fdNUqZaA6H+X2xgFfCdbDB3hglyZ7MPXsCfQa
8ic79B3F20nWJBbTXcf11KnW0/njnmRGIz0p+yI6Kg4t39k08c96G1k1Rclx/EGjF
5akbw8wZIjOMDIjMUB73K2d1+PZZM+vMHEayMmbF1su0flIjmemrxs+k/1LyS2d
TXV3b2d7vxGPKNYfEmq75Qg2xsZsQRX2s+0RYTQDDEF4uctCULtNrRkuy2UJUWZ
LUZstkjjMI3ztJ46wpL4Ny02kTEhMavoSmIXdHgtXwzoBnFySzJwYqg260vsTZ
CV0HyThiALm0ma+7Vas9MFyRnFKq2d2ajruxqEcqYEA+Z3H1ioZDDF+qavmxPeg
gyg/C90MYHPGbHq2f hxVLM2ZPdCbTYV8eYNnBK7dX1o4BA/A0/SQ5MbF50sAJ
8PeqeeF6fJ319S+DfGTLj6EIzhp4K8ysqrgQGga14RutAaFIHmEsoIG1x+2HJJ
cT8k5VtelU1kyXLuPebBjweCgYEAs5u49aUpfSEDBV0KJPrZXR0i6J+XKKTwAE
ImRc+5csf6HSdocCS0sgaqZq0f8tWma0SpEcxb94loNHRni084DKd3hij9h9n4
+g+PQaU3q0xpFDXvXrS6pBQDndhd9tt3izNe2v7wc8YKhvqsz50HwmoNOHdQG
O4mpAF8CqYAF1xVrjOjz+RdCytdHc+EqtgrerezoiOiuUPxfUAZ0/NK8P+ZIO99
Lb65QzprAtu9pec0wPVITnh80tZClyehaZK+M417g94w0rlri1XoterCSHkPe
kG6C6Wvyk92uAbA7q2oDKCW0htExFFyM00YUHh23J6tchA1wlpfKAQkBGocbowse
kDjBVus3LS+kzWbnFPAp/bmxtdtMFV5v95a0P/5PXnmx9mJL2keVsh8nohHvkxzyt
1r6mB31Cuspdq9d1j0s8tmsUqtGZRY1ZdkvTEK5se61V65Qv+U83LAH6qO12A87
pMRkH2zBqUn9ma9H10P6iA1X8ABQ2MZX3daTkBcOZCTEvDr+QLOpCSnvxGrjiciVY
OK4umtukoVJQ04o3Qr2obdRzhFWfOBFhDev8yPXwUM5/yYjM3yHyKaq9r3Xum
2qNHvRCXbvo1pa8A0Z1ukfUCapwosj+598vNq74D+8i5gkQzhsM/NeH2G+wXQ
mLvzkd23FtLxKnOaC0APA==
-----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.
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


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