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 26 June 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
   1.3. Prior Work

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
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-----
MIIDLTCCAhWgAwIBAgIULXcNXGI2bZp38sV7Cf6VcQfKnKDwD0YJKoZIhvcNAQEN
BQAwLTEMcAc4SIExkezjTc8aFfj/BE0AwGvZ3IE+CjRoIUwvLh6+4gsH1qQgu+
3NvKuieABJuJl+iCk3bZl4f2HTGMQGqj1vb9gp94YeMnq08qGEA
63mhUqZpnmN1FE-e+qf/tkTji189/eXYbdkXzYldUeTl3oCi65IL
EExzejtC8aFfj/BE0AwGvZ3IE+CjRoIUwvLh6+4gsH1qQgu+
3NvKuieABJuJl+iCk3bZl4f2HTGMQGqj1vb9gp94YeMnq08qGEA
63mhUqZpnmN1FE-e+qf/tkTji189/eXYbdkXzYldUeTl3oCi65IL

-----END CERTIFICATE-----

3.2. Certificate Authority Secret Key

-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxR9nz41hKhqfHrNBxGjkHjp+JwBewVn/dovHI3x8HCzd4e/x
oNFDZ48m8mCRUzfJph3r878/Mj35UMXl1k2qtqXH6DscmCiraHE16Lil7+n
a/O+9vN2v90MCM/b4Pa5GraPUOXL/981UUiKGRVLesdB6r58jy0kcdIf1l
Zph3r4A/R4Z7Ld0INdIpByv/hDyM0yYbbCCPW+5vScIlhgey2qY0iOQdreYBRNm
yE3UGUsXdU8ukZ72x47X7p/+2ROLOz395dgF0pbJIR1MNmgqij/rkgsRRF7ONnX0
0W/n/wtpYZVh8009KUu9y67+zzxu9fg/jv4qIDQABAoBAQc6LuWfU1KZPDEA
/7Ldv/hguNXpU6b7rLe8lpJ7L8219gwPdBPCRlohpY3uVYLT94AM5SejITxRv
Ig6Fp7wSj58kkXkO+G71Mzji163m4ndNIG5vSu7DxEnGhcrD7t5qJdV++p+p2r9
7uA0oL99gclw/NJVq3f2p6SfHdjeFrULPq59roYsvt/ECCxso5W2ozbM
OsygJ0A8psvBhf1MFq0+er/dFFr49oaBasP0RksbETRWNK7ld2I1q9hru2K7Nz1l
lxrHpryRCHknMBN8IVZvoBIScmBmio/5yp5p3PVPB93zw5XdS/A9YNs56bhuPEX54
mHgDaq/AjoG00A0ydxrL0C8nj8af3wMwazXetU8udJ0YeEYMYCNI+RdxbTSI
KAy77c0ad0d7DwXmjdBDqEBqUH03ou3iuXitG6r3wMNeZvyR3vO97f9R00MQs1K
WkqroM7S8j14J/JPuruFqqua+VSTXN22zb7ULj9yu0edlgxqBncNkbbaOAwj0
3r2tQNGBta2Tvkpl5jflvyy90000FaydpqdMujskbili/gfW2UliW8h8t19jyjSdeAhv7
j8LBilFyxpy/fc+IcEov79uq5x44LV/KiP4Fc3KGRMYmrd2ld+wJqogTkDh
ZKVZw65a0nxqIybgCTny+DRxCTBGczpCQzCk2JhiBzoaBAJpzd1jzRU2fC600ueZQ
U8T0GNR+hPfRgGgwv9umzdpO79a9G3+UEDFp6D5JmCaPitmX5p6s57SToDhK
peh51lPtj/477M2tbNcKcsh1hvMynRuItKTY4NeShxM5spX0I20L+iKMXZC/OXk
ktj33ayl1CfCfKfXtwMx5B71aPaOACGvItm0OxTy9RhGN5VBBaA16844+YdItfW9NGh
yA60RoaCoy90JY75H0Oba50UddMrLaC0iwC1dcdru2E56yp0571p1ucy94p9qG36
mFgD7B81hAa4J8+uFeWoldrVY8340vFnuIs0QI8ksqipk1BjylzjLD928wMdf
5Wqagh+cKygEYajqKzyFyD7dO2s5kwPzoBv8nmmWn5n3U0F50/Mf/sufTty
FohYU5e/YiHbPrYry8Zs50swujGvN26RjIQ4i4wCvd2ZZOxw1Dqnu0AQleY93n5
YDg6U+BjPw9O54LAc+f/BkwW0Q8Nwdxj5855F6QMvC04l1uZB0yao=
-----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-----
MIIDbjCCAlagAwIBAgIUZ4K0WXNSS8H0cUcZavD9EYqqTAswDQYJKoZIhvcaNAQEN
BQAwLTErMckGA1UEAxmiU2FtcGxlIExBTVBTIENlcnRpZmljYXRlIEF1dGhvcml0
7q35ZdG2JazzJGNZDZ9sV7Akh0hlRfoFjTZa5m4RegQAYSyaqg43ouWi1xRN0avf0
UTYrwjK04qRvdTV2gCATC0EGq/xiNU0sfjJXzbCublN3fZMOXshKKBqThlK7SJSa9
Czax7efGoiY/idk0e9ineK30SCCAIkJlNzf2UZrP73IPZmekx0Tatff9hW9dDA+
/H1lypTn/aG0Q/s9icFxr6y2ZQXsuQPmjZmgj10aD9caZWgRYCGfhlhmA0V1uQ
l1wobYU8DAxVn+GgbqbyjGQMoYthIK0Gn5+wofwXXUM/zbu+g6+1I5doxxRXFqtg
2GzbIqkAHZQm+bBnFrhAgMBAAgjZcwqZw0DAYFQVTAQH/BAIwADAEeBqNHREE
FzAvqRhnbhGjZUBzwltZ5IeGfcG6lRBMGAA1UdJQ0MAoGCGsGQUFBBwMEMA8G
A1udDwEw/qWFAGwHoAhAQVYDVR0BBYEFKwVFqk/yUVry7oZkQ46SXR1wB5MB8G
A1udIwQYMBAAFdSTXPAID2yw3paoDPU9/eAonfnMA0GCSqGISb3DQEBDOUAAo41B
AQ7B6o4yZ7yrVScpPc0lRc6gtdI4q93aKXECQczNQLp4yesh6brqaZhNJuwYcJ5T
qbUym9hJ701JE4JGNH+yAZR1Itte6HFKYIBM4EJum6++2hqbUaLz4tL06BHqOQC
v/9NiNY7q9R9c/b5UsYHwhqKwht2a+Atg4J8kpg+q+MmZMQV/A07RuLFJK91UW
LBMEXFcpIJONH0PaSTQnEI/MvtuSu+8RnClAI3yFfyTkTb+8rD7VxyUtqDZ6duU/
9/iqD/5S70Q1iywtd343mACz3B1RIfxMHSAsdQAf2btGumqR0KiAp3KkYRAePoa
JqYkB7Zad0ngFl0G0FHON+7
-----END CERTIFICATE-----
```
4.2. Alice's Private Key Material

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAw+6t+xWXRt10MB8yRjWQ2fbFkwCodIZUX68Y02Te2EuEXoEAGEs
mo0N6L0tcuTdGr39F2EkB8y1t0KkXexswqAgBCqv8yjVDr13yV82wrms5Td32TDL
7I+Sigak4ZSu+uwP0s8Y03cxqlmp4onZNHvdZ3it9EggmQyUzX0dmQ6z509yDzH
plMaE2zxxYcPXQwpv4xtccbfT2htEP77YnPbaa+sts0F717KDsozGYI9ddq/XGs
lyEWAoH5YZgFNdKbdJ3dKCG2FPAvcCVZ/hog6msoxKdKwBqY3CtBp+fhq8MW11DP82
1P0oOvt5EaF8UJRbaths2yKpA2WbUjvqW5x4aQIDAQABAA0BAA71wvruI4Gi1DLwGq
EHJfdRXJXSX5o+dejeMTHKxAI1MBvSL3NCp1s0fCF6b+pmmYRkX1qg3qfpszS2/zR
pp2DUel9+8ZK6h0nTDWrsJb/mY6S6wCMhW3WTWL19oCkY4ryEksH4HzHfo6t8
DpTwAdr7PcrmHClXM15413HksCIB95trPrKsGyhHyFLOThReOog2Nsm7e5hmv
7WkMuESFku5OHFLUw5FyELeZhhJarl8RZ17qYbtT6X6IamX0f9aTMDPA1qAcix+4K0a
zf3cN1xqg/yIVtvs6oyknTStswi3i46PWzMwf845Eayunrg8e6F3hW7zndjxw
Jg/qAEaeqYEA35LL02tGdb5gWHwzzZAnTzBMo1Z3toEN25LettU4MY7mxkJMTRDAi
5V0dpSXRvFa5r8qwU9yEFm+0uB6k52CVbTE1Fp96JlbzYjZnKaLm50G8+HSLdtn
1vj1XyCGRDJKJ8GazPzPw+Wfp6449wWspguXMD1OM8jfekgTeh6rGECyEA4tKM
Da3tFEEyV9ZSxZV9ep9dhE7kmVqr2pvt2YfJTknSo2kkj/qkoMi2PhS8ZOJQ
J90bDngq15s1O/qi+hwYRmcKCrvfnfJUEq3v+3BFQYPDfwkgtgiBu5TDGnImFA2t
l+23SwCwpjfPh5rkJk8GTQ0Ts1rHxYX3djNPhhhb0ECgYAOjsegN9HZalVUKFntRtIO
kXrcURtu4MbexbLkVTDot+UKuhfEBCNtmPWEAGceuZtm1rM5YZx3MTazMUsJgs1
zEp7ow8RTMyg6/0LIA5awmEaZATY5+0o3mQsQTKd+uLiW3xm55pTZNE82PpqVmn
/G94Vgs+BA5m4nC9q3XGQ2vBrD35et+9Yf7KYT5jqtSpt6kp6m+ql5HUJTDv/t
rKl3bB6v4MkBXmRZB/EjDiN/9vln5w+yl6s/iKyucXjFDFV4T1QzAn5nJAbraC0FF
iMkKvn5V5N3fIdAm+Z9mJNY8t/vbZiQoronam6yTwHU5s5kJNIEdcrQ5pJbU1
7s3BAnOgAxqDE0K1sw/e05p0th97fBNrIqUuemSuctUia1vI1mwiKul1wuxYV8D82z92xh
q0dsZHfSiVzwzhrFvQpEGh1mDNVfuSHG1q74qDyP5p30enrK4bloBhX1t2Z
pUSp7jME4rNqAXfdVUPq4U7Tyq951DmaFLClmUZ0DnUay19dc=
-----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 ---

MIINxQ1BAzCDV0GcsqG51b3DQHEAaCCDu4EgkKMIINrjCCBC8GcsqG51b3DQHE BqC7CBAwqGCaEAMIEEFQYKoZIhvcNAQcBMWBCGqS51b3DQEMqMDqDgOIsxMo cGNg7NdMACnG3qII6LIPoswM0sYjwWTaxiUEtKmgTV7g7g79g73AlKhrW6sVb N+Ji8BejrjQ2Q3d6ayE89b1Ubdxqx59g9QIDkctF1HEwtywsp6B9dL t0YoWljrj7c20sJOWMEL5fNeA+Xi7Im2KR6dDxtFw/pwAzaw7jnaBGlci2K0NqgL 9qY050uHk0BoaSAOA9KUJc3CIHFMqf41jvgyPRdzcXozEy7EnjAeF3smdsFUc hdi3ZqwpFDk1aJjttt0vKh1cHLSMqG98j0My7vPSFHVMOVMUvHj351nkWy 2A4Fxceo50C0Xk5wNn5aiMmRy0U6vHeZKft6Tcyi6BArfrLA18BaIu7As4qae EQPjH7A6ENs9vd8fzBST0ULj9k8B0Lh7v2ymCNDuVLrj6BvridFAgycRvLquvq oIQO4wPEqMKF5V/UMC9HUYLVPXILzJ96GAI5JEi6gAPvSFD5ZsbYs95PAXA2831 zJeg51XIePe4yac1hEurpy9q3M5jzP9l8eiyYgyaXGUrZPr4tJ3nJin55E2Zd A1sze8FWh0oHy0wawfgw2fne5eU83qfKfjzj/9HDWqoEPQGvJrLSMaizidCiL1Jg jgaAGPCCvZW7uq01s/ys1U1IqGaeZMNUj+hq23as0OPKzp3r3eFevlseUl0dCZOQA zSp4Uldh4p4rSUaZn2AIhHrpr7V7yJlTpsx2ycbb8OkPGvmVw5px4v7fFwvj CWhfsA0yKLC8FXNluCsaWyu0HgHNe8teM3Awb3vGQGqM1btqj896qgsbcysAr +049Y5L80b876A3ZNkK89q0ByqGyn7+B3V25kbhkbkozPJl/BaMY4nuauA sLc6peraI/fjv5jTcaHNfL3ip3v6nhK6ap6rL21u8AU7XiK8Las2BiCY92 VtqUpffppBq6s3gB4ZG1J51wi4E0Q6FASVvXtKmP0wA55XZ/S5DhJn8j0Ww3 xpyBvzvdeerbYyULbvn/Uwdgj6vXvcuv3MGw/oak0kx/d70CpatjnFmka7k1 KS050F4xZygLY46Lu45b5Vr+cstne3FjgWXJTGUtoBecyueXKdWExEUL/oUoc pt80ReGFX3pDpnHcn9RTWnGxtF6d6rBmtuUFHrQys2msMVX7/805q11N7Lt7H1400 7wT73CgwK5snwagAY5ncrRxyLapmjqVt+O+R+F542w30yctlimbo0Ajz5821 q10UeqvK7Qw7lgCq116etE216vXvBdcLr42hrnRZynsHjgkXg6uz7cataKhS+ qu153djqwv0gbvqXkq1K9G9wBwawagq0qMIIinA1BADBC45UC5qGsqG51b3DQHEATAc BgoqkFgk9g9wBADEAAMA4E92Bz56G16BfA5f1uYCBaqzMr1pbeerGQCQBD-x+lGh Pu5ZC81jLMQJU/UruWZmN88zaZEMypr7tH1ycvB1yLRACFwQQatDahd3RpgFp Gk7r00539JOHcUbB6J36dKcDdyNuYidWuhKtcbxhX7D0VauUF75VMG7Yn9wOj jw700y3NkaD2jZvJ1HxKACwEn4q8B8C5T6j4FZja0f2jvtQ3VdqtghjFmUVSbYFz+akY l2c0x3xgeP0df3hNt0r0YxU7yleIIsyEdeq5tQ5C5KcntBxOEPsVbHlzOx1 XoFa0v15Nzz41v00AqGWhhO0i1albUtTt/ej/PKJZw6taw3lp5RlvwVWTX7FWbqy NA899qu06Ox8qmqPaCw4h3jEi4l93uc0i169Hkhkqy9Tni/42jxurTr4m0hbixn4 bQHt0510oC0eHstY0em4yD382bxeq0luE361yC2x1s9An8cQntV/3jw3wF0ujw7j YcAB1XsoK5dow59RlILVj2vRRhcUlw1v+vQ5v40G0GsdVZVG01r1H10c5ep0jWj7hPW 7LrLYNIJn+kkfPafFdojbRBl7LaUkqokmBnhAt4xPxfm0FBoDQ7PffpbN9yd USFskQv0ALSsCNbdes2hB2BT3x0s01uLx2zw2rw2oAfKx/Duy+jTlW07047ArVr t4+kZomLsy+BlHWBSw8v42HrPleTjRhGHC5LytGdyknpyHmop0e9fG141cEn1B3K q9ubAdClS0y+Kr+ldRzFaQjEMKLfWkYPWnmo2NjLkKnd44)HLo1hRwee9gk NbnZurX0oE5BkqN9z0B+DfA5qB3pxDP3XKlQ0GveMVv7 8az3LpFmukD0W0fwxzq8u/DAgewfRLERBAm36ayxe6901c660wF61dt 3bBpaNy2K+hrryqz+VNBp5Ai5eB0+U94HDq7xCL6D4psK5L1RJXQWnnKytYd2sji KECQ1IC1EQjVWNNWFPE9/Mw5TutLjPK5E1NCzkOJtueGxY315LcEB4hنزFHLsgK RA725sV3d6TBEQy9b3f+o/b+E66ZU1JRb+9N9mrMqR02w6d9s9i815Ntwwu TkMhClj/7dv2kPTTD1DgksvN5H9sEps07nI4L5F2P04SvsvsVUC4UJzCCWBvCsGQg S1b3DQHEAaACCBuBEgqVMUFLRTCCBUECGyqG51b3DQHEMcCe0IIE7Jcm0woAYK 2iZIhiVcNAoBZA0BAeMEvWJxpqjzFQICFpsEqgTTKrmizjeneN/0J7nBm1FmpqFwFw KG5fa5Hh5kjkqoA5kOAssGUEstFvpx5sz/X/XwvqV4qxeHup+0D0ocD5eu6lWtg VB001e2439bhyRJC5MCqJbjeSm5sAB80qJNHIahUlJi19Mzv6r6fOsv7s7mr9w/wi wsf=0sca+xOlaNdltb+yXn7qcMq9c7U0NnmB56dijgyhplp2/zselWfswusX6c/8/s hO1qj+6/v0D0EvwYy7kq2dzlt2u1UItUr04wCvpPcKbo1bP+dXNWLQsY0rb9e hm0YjQm3eSzdLsaa9qom3y/sokT/tUtq1X0ln907Tz2aghAl24T2425NCQkgL ywmw91YuhKZt3HdPEFIPA7xq4v4tv3b2qkryBbY0ov+IBeWq81cl3Bq8kMw9E6BBm fkmqrqFYaXs5kULeM2QMWOUP4MTdmns9izVeUSAlaA3USGXEVeHev2rvj8McG81Rz qz8r/wqZlhoAouNo8rvCueAo+E95svFCFxsp+eoh+yxCExaqlLJn1E6+1R5l5s LuCiv35s/DjwvQ08061Jc0PZjSo8697TCPJy7htgzkKehG0HauP1X+4Kpr2ynsF sVxaz2bn2Uo/r/mdtxkjxspsCwO8hcQDlLGD3s1AIj7xQVv9Vzvqvb8U8LNl 1h5Q0lLSCGExs18pond+G5L5q+TWH7TBRBpGhTcsyHMPLO1ri4Qwo805evx0k6bk
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-----
MIIDaTCCAlGgAwIBAgIUIlPuMG0CCx8CzfXJwT46333mmG81wQYJKoZIhvcNAQEN
BQAwLTERcMGA1EAUEwPzA/GxLIEBTBVIENcnRzmljYXRlIEF1dGhvcml0eTAg
TAgwDQYJKoZIhvcNAQEBBQAwHg0MB0GA1UdDgQWBBQDrAKQ6Dj0kN4Z7pXzMnThZgAopzAf
-----END CERTIFICATE-----
```
5.2. Bob's Private Key Material

---- BEGIN RSA PRIVATE KEY -----
MIIeApAIBAAKCAQEAwv5b14tnK6aArKtPeh6m/dUDZ+w3X832iYPxztZRr2IR2rwF/C2ZbsjMDzxQdKs+FdsK5v+XYNjErCh/PSWu0f+faT51/KC5s1xKj5sMaKnype5uZjpAaw70j+eY+jz8fjytjMI0ULQ0IlGLmt0ff0AjlX/w+h4svw/sNtb0k5sxVRpnk6scRzjW3dszq0mKq/w+yWwh4vFfprY/UPtpy1xEBSpPr0r2Zzd18inevnQM7aRZduyK5mXG5+NKK9agc6a8ap7ZP1idz/dJ8KziEqXZCDc9e9Q35s3f3h0qkmRt45h8EJ1J459Km97gbpE+90FvFuy2gZ/DMD0AIU0BEw1DAQABAo1BAEv1KcAmXC99N9D4KQP87726zhC53s3jli/NVs5BvJ1JsvVa22ocZ7nk7FP0ttPzTA0DDLJ7V7WCKSDLnNiphLN0X/LM0It75KVpxym5fRIoW03zomDkgfZy/L2kCnaogPfF19zTu/T5SU
r1J4dkRFQ0fWr3Fkg9FDcWksUsUt5fNS52Cv0ndQWiGt8EnsZIwX9H8rnn5rSTroDsk9C0jyjMcc7iX7304KDvUalVJ1Rtx+y1lbPTyuKF2nbNjWhsYhuIOGT4Gm6Tirda
z6bWjuxH7nNrkGr0t14aE8Xv5jesC+J5ulwaji/6V+eDZvFpVqiXyq6oa6JioPw7v
rX7cICQEcYEA09ovqo1/YdDN0TJXb4LNMt51wLxgrpzE/SNPEV5XknQ5yf6rrkZ3
+l/r6w2opor4Y+3/igM0BZcN7YqIM9Drkg6bDLzrs354A9dZLDBNAgCnDR0yY87
U3f2ljppA2zzRahYKhskFxt2w3cUs2990YgjNwLal7LrXvpAeECgYEadypv
f+wzdeC0xsbGG1Lb4xiiFpJY2s604auZ3/s/y9W3v8LSKrytHHopQ0g3GALvQ9i/Ay
LWRB1ajTzEue6lIYINZI2+wvK2zP2GB21/XJ5MI3x7AcRr//1/muyhw3GfypGpg
6zRE45dZPfm9nkylw14/y147ubdOnyxifBmDxMCGyA0HB16HIZ0jsjBh3iS06W
kaJ6r/Wx9FY8j864h+45juDNeINc1m19T26s7wrcikXyytidHi+zdjg+orEuke2
UMpq4EPFkgkfoahPXi1hCQ0mfw4YMCECEdMMyypJwJjs6luiEdx/LPfC1CL
r1fHLQ0j4Mrfn0ZQnyA0KBQc6WTrypv8MyynA1j4jD32bTayQ0ZK98CU7o
YGRBfwmw9R8/qC3FJR3qGupW9Me4+n54ZC1w12ncn6XMLj1P8wdrLrNtvGv5hV
yVzsbZsgq9ZcnhtiyxHrpkG2hYQdG/HSB79Ge6aBV6vz9p74X6Qo1lnQe2cx6
EzgTmWkBGQdJwmtDK85G0juJB70OB+CxB39j8a780wypx+XY1bqm+n3aD1yJB
8VVTlhWvq3wM51edjxVvaykKd31KjpnBt1W1jFwEqDxMB0wwRDBdpvff3jh4
Jjk+Ltvnhhww09ktCvZGPzLYsFSc1tLuodBMNjxU9u0bqTyqx/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.
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


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