Workgroup:	openpgp		
Internet-Draft:	draft-bre-openpgp-samples-01		
Published:	20 December 2019		
Intended Status:	Informational		
Expires:	22 June 2020		
Authors:	B.R. Einarsson	. juga	D.K. Gillmor
	Mailpile ehf	*Independent*	*ACLU*

OpenPGP Example Keys and Certificates

Abstract

The OpenPGP development community benefits from sharing samples of signed or encrypted data. This document facilitates such collaboration by defining a small set of OpenPGP 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 22 June 2020.

Copyright Notice

Table of Contents

1. Introduction
   1.1. Requirements Language
   1.2. Terminology
2. Alice's Ed25519 Samples
   2.1. Alice's OpenPGP Certificate
   2.2. Alice's OpenPGP Secret Key Material
   2.3. Alice's Revocation Certificate
3. Bob's RSA-3072 Samples
   3.1. Bob's OpenPGP Certificate
   3.2. Bob's OpenPGP Secret Key Material
   3.3. Bob's Revocation Certificate
4. Security Considerations
5. IANA Considerations
6. Document Considerations
   6.1. Document History
7. Acknowledgements
8. References
   8.1. Normative References
   8.2. Informative References

Authors' Addresses

1. Introduction

The OpenPGP 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 OpenPGP certificates and secret keys for use when generating or operating on such samples.

Samples are provided for two "personas", Alice and Bob. Alice uses keys based on the Ed25519 elliptic curve algorithm, but Bob is a bit behind the times and has a 3072-bit RSA key.

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

This document makes use of the terminology section from [I-D.draft-dkg-openpgp-abuse-resistant-keystore-04].

2. Alice's Ed25519 Samples

Properties:

- OpenPGP Version: 4
- Fingerprint: EB85 BB5F A33A 75E1 5E94 4E63 F231 550C 4F47 E38E
- Primary key algorithm: Ed25519 [I-D.ietf-openpgp-rfc4880bis]
- Primary key creation date: Tue Jan 22 11:56:25 GMT 2019
- Primary key capabilities: certify, sign
- User ID: `Alice Lovelace <alice@openpgp.example>`
- Symmetric algorithm preferences: AES-256, AES-192, AES-128, 3DES
- Hash algorithm preferences: SHA512, SHA384, SHA256, SHA224, SHA1
- Compresson algorithm preferences: ZLIB, BZip2, ZIP
- Subkey algorithm: Curve25519
- Subkey capabilities: encrypt
- Subkey creation date: Tue Jan 22 11:56:25 GMT 2019
- There are no expiration dates in the entire certificate

- The secret key material is in the clear (no password)
- All OpenPGP signature packets contain a hashed Issuer Fingerprint subpacket (see [I-D.ietf-openpgp-rfc4880bis]

2.1. Alice's OpenPGP Certificate

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: Alice's OpenPGP certificate
Comment: https://www.ietf.org/id/draft-bre-openpgp-samples-01.html

mDMEXEcE6RYJKwYBBAHaRw8BAQdArjWwk3FAqyiFbFBKT4TzXcVBqPTB3gmzlC/U
b7O1u120JkFsaWNlIExvdmVsYWNlIDxhbGljZUBvcGVucGdwLmV4YW1wbGU+iJAE
ExYIADgCGwMFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AWIQTrhbtfozp14V6UTmPy
MVUMT0fjjgUCXaWfOgAKCRDyMVUMT0fjjukrAPoDnHBSogOmsHOsd9qGsiZpgRnO
dypvbm+QtXZqth9rvwD9HcDC0tC+PHAsO7OTh1S1TC9RiJsvawAfCPaQZoed8gK4
OARcRwTpEgorBgEEAZdVAQUBAQdAQv8GIa2rSTzgqbXCpDDYMiKRVitCsy203x3s
E9+eviIDAQgHiHgEGBYIACAWIQTrhbtfozp14V6UTmPyMVUMT0fjjgUCXEcE6QIb
DAAKCRDyMVUMT0fjjlnQAQDFHUs6TIcxrNTtEZFjUFm1M0PJ1Dng/cDW4xN80fsn
0QEA22Kr7VkCjeAEC08VSTeV+QFsmz55/lntWkwYWhmvOgE=
=iIGO
-----END PGP PUBLIC KEY BLOCK-----
```

2.2. Alice's OpenPGP Secret Key Material

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Comment: Alice's OpenPGP Transferable Secret Key
Comment: https://www.ietf.org/id/draft-bre-openpgp-samples-01.html

lFgEXEcE6RYJKwYBBAHaRw8BAQdArjWwk3FAqyiFbFBKT4TzXcVBqPTB3gmzlC/U
b7O1u10AAP9XBeW6lzGOLx7zHH9AsUDUTb2pggYGMzd0P3ulJ2AfvQ4RtCZBbGlj
ZSBMb3ZlbGFjZSA8YWxpY2VAb3BlbnBncC5leGFtcGxlPoiQBBMWCAA4AhsDBQsJ
CAcCBhUKCQgLAgQWAgMBAh4BAheAFiEE64W7X6M6deFelE5j8jFVDE9H444FAl2l
nzoACgkQ8jFVDE9H447pKwD6A5xwUqIDprBzrHfahrImaYEZzncqb25vkLV2arYf
a78A/R3AwtLQvjxwLDuzk4dUtUwvUYibL2sAHwj2kGaHnfICnF0EXEcE6RIKKwYB
BAGXVQEFAQEHQEL/BiGtq0k84Km1wqQw2DIikVYrQrMttN8d7BPfnr4iAwEIBwAA
/3/xFPG6U17rhTuq+07gmEvaFYKfxRB6sgAYiW6TMTpQEK6IeAQYFggAIBYhBOuF
ul+jOnXhXpROY/IxVQxPR+OOBQJcRwTpAhsMAAoJEPIxVQxPR+OOWdABAMUdSzpM
hzGs1O0RkWNQWbUzQ8nUOeD9wNbjE3zR+yfRAQDbYqvtWQKN4AQLTxVJN5X5AWyb
Pnn+We1aTBhaGa86AQ==
=n8OM
-----END PGP PRIVATE KEY BLOCK-----
```

2.3. Alice's Revocation Certificate

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: Alice's revocation certificate
Comment: https://www.ietf.org/id/draft-bre-openpgp-samples-01.html

iHgEIBYIACAWIQTrhbtfozp14V6UTmPyMVUMT0fjjgUCXaWkOwIdAAAKCRDyMVUM
T0fjjoBlAQDA9ukZFKRFGCooVcVoDVmxTaHLUXlIg9TPh2f7zzI9KgD/SLNXUOaH
O6TozOS7C9lwIHwwdHdAxgf5BzuhLT9iuAM=
=Tm8h
-----END PGP PUBLIC KEY BLOCK-----
```

3. Bob's RSA-3072 Samples

Properties:

- OpenPGP Version: 4
- Fingerprint: D1A6 6E1A 23B1 82C9 980F 788C FBFC C82A 015E 7330
- Primary key algorithm: RSA 3072 [RFC4880]
- Primary key creation date: Tue Oct 15 10:18:26 GMT 2019
- Primary key capabilities: certify, sign
- User ID: `Bob Babbage <bob@openpgp.example>`
- Symmetric algorithm preferences: AES-256, AES-192, AES-128, 3DES
- Hash algorithm preferences: SHA512, SHA384, SHA256, SHA224, SHA1
- Compresson algorithm preferences: ZLIB, BZip2, ZIP
- Subkey algorithm: RSA 3072
- Subkey capabilities: encrypt
- Subkey creation date: Tue Oct 15 10:18:26 GMT 2019
- There are no expiration dates in the entire certificate
- The secret key material is in the clear (no password)
- All OpenPGP signature packets contain a hashed Issuer Fingerprint subpacket (see [I-D.ietf-openpgp-rfc4880bis]

3.1. Bob's OpenPGP Certificate

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: Bob's OpenPGP certificate
Comment: https://www.ietf.org/id/draft-bre-openpgp-samples-01.html

mQGNBF2lnPIBDAC5cL9PQoQLTMuhjbYvb4Ncuuo0bfmgPRFywX53jPhoFf4Zg6mv
/seOXpgecTdOcVttfzC8ycIKrt3aQTiwOG/ctaR4Bk/t6ayNFfdUNxHWk4WCKzdz
/56fW2O0F23qIRd8UUJp5IIlN4RDdRCtdhVQIAuzvp2oVy/LaS2kxQoKvph/5pQ/
5whqsyroEWDJoSV0yOb25B/iwk/pLUFoyhDG9bj0kIzDxrEqW+7Ba8nocQlecMF3
X5KMN5kp2zraLv9dlBBpWW43XktjcCZgMy20SouraVma8Je/ECwUWYUiAZxLIlMv
9CurEOtxUw6N3RdOtLmYZS9uEnn5y1UkF88o8Nku890uk6BrewFzJyLAx5wRZ4F0
qV/yq36UWQ0JB/AUGhHVPdFf6pl6eaxBwT5GXvbBUibtf8YI2og5RsgTWtXfU7eb
SGXrl5ZMpbA6mbfhd0R8aPxWfmDWiIOhBufhMCvUHh1sApMKVZnvIff9/0Dca3wb
vLIwa3T4CyshfT0AEQEAAbQhQm9iIEJhYmJhZ2UgPGJvYkBvcGVucGdwLmV4YW1w
bGU+iQHOBBMBCgA4AhsDBQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAFiEE0aZuGiOx
gsmYD3iM+/zIKgFeczAFAl2lnvoACgkQ+/zIKgFeczBvbAv/VNk90a6hG8Od9xTz
XxH5YRFUSGfIA1yjPIVOnKqhMwps2U+sWE3urL+MvjyQRlyRV8oY9IOhQ5Esm6DO
ZYrTnE7qVETm1ajIAP2OFChEc55uH88x/anpPOXOJY7S8jbn3naC9qad75BrZ+3g
9EBUWiy5p8TykP05WSnSxNRt7vFKLfEB4nGkehpwHXOVF0CRNwYle42bg8lpmdXF
DcCZCi+qEbafmTQzkAqyzS3nCh3IAqq6Y0kBuaKLm2tSNUOlZbD+OHYQNZ5Jix7c
ZUzs6Xh4+I55NRWl5smrLq66yOQoFPy9jot/Qxikx/wP3MsAzeGaZSEPc0fHp5G1
6rlGbxQ3vl8/usUV7W+TMEMljgwd5x8POR6HC8EaCDfVnUBCPi/Gv+egLjsIbPJZ
ZEroiE40e6/UoCiQtlpQB5exPJYSd1Q1txCwueih99PHepsDhmUQKiACszNU+RRo
zAYau2VdHqnRJ7QYdxHDiH49jPK4NTMyb/tJh2TiIwcmsIpGuQGNBF2lnPIBDADW
ML9cbGMrp12CtF9b2P6z9TTT74S8iyBOzaSvdGDQY/sUtZXRg21HWamXnn9sSXvI
DEINOQ6A9QxdxoqWdCHrOuW3ofneYXoG+zeKc4dC86wa1TR2q9vW+RMXSO4uImA+
Uzula/6k1DogDf28qhCxMwG/i/m9g1c/0aApuDyKdQ1PXsHHNlgd/Dn6rrd5y2AO
baifV7wIhEJnvqgFXDN2RXGjLeCOHV4Q2WTYPg/S4k1nMXVDwZXrvIsA0YwIMgIT
86Rafp1qKlgPNbiIlC1g9RY/iFaGN2b4Ir6GDohBQSfZW2+LXoPZuVE/wGlQ01rh
827KVZW4lXvqsge+wtnWlszcselGATyzqOK9LdHPdZGzROZYI2e8c+paLNDdVPL6
vdRBUnkCaEkOtl1mr2JpQi5nTU+gTX4IeInC7E+1a9UDF/Y85ybUz8XV8rUnR76U
qVC7KidNepdHbZjjXCt8/Zo+Tec9JNbYNQB/e9ExmDntmlHEsSEQzFwzj8sxH48A
EQEAAYkBtgQYAQoAIBYhBNGmbhojsYLJmA94jPv8yCoBXnMwBQJdpZzyAhsMAAoJ
EPv8yCoBXnMw6f8L/26C34dkjBffTzMj5Bdzm8MtF67OYneJ4TQMw7+41IL4rVcS
KhIhk/3Ud5knaRtP2ef1+5F66h9/RPQOJ5+tvBwhBAcUWSupKnUrdVaZQanYmtSx
cVV2PL9+QEiNN3tzluhaWO//rACxJ+K/ZXQlIzwQVTpNhfGzAaMVV9zpf3u0k14i
tcv6alKY8+rLZvO1wIIeRZLmU0tZDD5HtWDvUV7rIFI1WuoLb+KZgbYn3OWjCPHV
dTrdZ2CqnZbG3SXw6awH9bzRLV9EXkbhIMez0deCVdeo+wFFklh8/5VK2b0vk/+w
qMJxfpa1lHvJLobzOP9fvrswsr92MA2+k901WeISR7qEzcI0Fdg8AyFAExaEK6Vy
jP7SXGLwvfisw34OxuZr3qmx1Sufu4toH3XrB7QJN8XyqqbsGxUCBqWif9RSK4xj
zRTe56iPeiSJJOIciMP9i2ldI+KgLycyeDvGoBj0HCLO3gVaBe4ubVrj5KjhX2PV
NEJd3XZRzaXZE2aAMQ==
=NXei
-----END PGP PUBLIC KEY BLOCK-----
```

3.2. Bob's OpenPGP Secret Key Material

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Comment: Bob's OpenPGP Transferable Secret Key
Comment: https://www.ietf.org/id/draft-bre-openpgp-samples-01.html

lQVYBF2lnPIBDAC5cL9PQoQLTMuhjbYvb4Ncuuo0bfmgPRFywX53jPhoFf4Zg6mv
/seOXpgecTdOcVttfzC8ycIKrt3aQTiwOG/ctaR4Bk/t6ayNFfdUNxHWk4WCKzdz
/56fW2O0F23qIRd8UUJp5IIlN4RDdRCtdhVQIAuzvp2oVy/LaS2kxQoKvph/5pQ/
5whqsyroEWDJoSV0yOb25B/iwk/pLUFoyhDG9bj0kIzDxrEqW+7Ba8nocQlecMF3
X5KMN5kp2zraLv9dlBBpWW43XktjcCZgMy20SouraVma8Je/ECwUWYUiAZxLIlMv
9CurEOtxUw6N3RdOtLmYZS9uEnn5y1UkF88o8Nku890uk6BrewFzJyLAx5wRZ4F0
qV/yq36UWQ0JB/AUGhHVPdFf6pl6eaxBwT5GXvbBUibtf8YI2og5RsgTWtXfU7eb
SGXrl5ZMpbA6mbfhd0R8aPxWfmDWiIOhBufhMCvUHh1sApMKVZnvIff9/0Dca3wb
vLIwa3T4CyshfT0AEQEAAQAL/RZqbJW2IqQDCnJi4Ozm++gPqBPiX1RhTWSjwxfM
cJKUZfzLj414rMKm6Jh1cwwGY9jekROhB9WmwaaKT8HtcIgrZNAlYzANGRCM4TLK
3VskxfSwKKna8l+s+mZglqbAjUg3wmFuf9Tj2xcUZYmyRm1DEmcN2ZzpvRtHgX7z
Wn1mAKUlSDJZSQks0zjuMNbupcpyJokdlkUg2+wBznBOTKzgMxVNC9b2g5/tMPUs
hGGWmF1UH+7AHMTaS6dlmr2ZBIyogdnfUqdNg5sZwsxSNrbglKP4sqe7X61uEAIQ
bD7rT3LonLbhkrj3I8wilUD8usIwt5IecoHhd9HziqZjRCc1BUBkboUEoyedbDV4
i4qfsFZ6CEWoLuD5pW7dEp0M+WeuHXO164Rc+LnH6i1VQrpb1Okl4qO6ejIpIjBI
1t3GshtUu/mwGBBxs60KBX5g77mFQ9lLCRj8lSYqOsHRKBhUp4qM869VA+fD0BRP
fqPT0I9IH4Oa/A3jYJcg622GwQYA1LhnP208Waf6PkQSJ6kyr8ymY1yVh9VBE/g6
fRDYA+pkqKnw9wfH2Qho3ysAA+OmVOX8Hldg+Pc0Zs0e5pCavb0En8iFLvTA0Q2E
LR5rLue9uD7aFuKFU/VdcddY9Ww/vo4k5p/tVGp7F8RYCFn9rSjIWbfvvZi1q5Tx
+akoZbga+4qQ4WYzB/obdX6SCmi6BndcQ1QdjCCQU6gpYx0MddVERbIp9+2SXDyL
hpxjSyz+RGsZi/9UAshT4txP4+MZBgDfK3ZqtW+h2/eMRxkANqOJpxSjMyLO/FXN
WxzTDYeWtHNYiAlOwlQZEPOydZFty9IVzzNFQCIUCGjQ/nNyhw7adSgUk3+BXEx/
MyJPYY0BYuhLxLYcrfQ9nrhaVKxRJj25SVHj2ASsiwGJRZW4CC3uw40OYxfKEvNC
mer/VxM3kg8qqGf9KUzJ1dVdAvjyx2Hz6jY2qWCyRQ6IMjWHyd43C4r3jxooYKUC
YnstRQyb/gCSKahveSEjo07CiXMr88UGALwzEr3npFAsPW3osGaFLj49y1oRe11E
he9gCHFm+fuzbXrWmdPjYU5/ZdqdojzDqfu4ThfnipknpVUM1o6MQqkjM896FHm8
zbKVFSMhEP6DPHSCexMFrrSgN03PdwHTO6iBaIBBFqmGY01tmJ03SxvSpiBPON9P
NVvy/6UZFedTq8A07OUAxO62YUSNtT5pmK2vzs3SAZJmbFbMh+NN204TRI72GlqT
t5hcfkuv8hrmwPS/ZR6q312mKQ6w/1pqO9qitCFCb2IgQmFiYmFnZSA8Ym9iQG9w
ZW5wZ3AuZXhhbXBsZT6JAc4EEwEKADgCGwMFCwkIBwIGFQoJCAsCBBYCAwECHgEC
F4AWIQTRpm4aI7GCyZgPeIz7/MgqAV5zMAUCXaWe+gAKCRD7/MgqAV5zMG9sC/9U
2T3RrqEbw533FPNfEflhEVRIZ8gDXKM8hU6cqqEzCmzZT6xYTe6sv4y+PJBGXJFX
yhj0g6FDkSyboM5litOcTupURObVqMgA/Y4UKERznm4fzzH9qek85c4ljtLyNufe
doL2pp3vkGtn7eD0QFRaLLmnxPKQ/TlZKdLE1G3u8Uot8QHicaR6GnAdc5UXQJE3
BiV7jZuDyWmZ1cUNwJkKL6oRtp+ZNDOQCrLNLecKHcgCqrpjSQG5oouba1I1Q6Vl
sP44dhA1nkmLHtxlTOzpeHj4jnk1FaXmyasurrrI5CgU/L2Oi39DGKTH/A/cywDN
4ZplIQ9zR8enkbXquUZvFDe+Xz+6xRXtb5MwQyWODB3nHw85HocLwRoIN9WdQEI+
L8a/56AuOwhs8llkSuiITjR7r9SgKJC2WlAHl7E8lhJ3VDW3ELC56KH308d6mwOG
ZRAqIAKzM1T5FGjMBhq7ZV0eqdEntBh3EcOIfj2M8rg1MzJv+0mHZOIjByawikad
BVgEXaWc8gEMANYwv1xsYyunXYK0X1vY/rP1NNPvhLyLIE7NpK90YNBj+xS1ldGD
bUdZqZeef2xJe8gMQg05DoD1DF3GipZ0Ies65beh+d5hegb7N4pzh0LzrBrVNHar
29b5ExdI7i4iYD5TO6Vr/qTUOiAN/byqELEzAb+L+b2DVz/RoCm4PIp1DU9ewcc2
WB38Ofqut3nLYA5tqJ9XvAiEQme+qAVcM3ZFcaMt4I4dXhDZZNg+D9LiTWcxdUPB
leu8iwDRjAgyAhPzpFp+nWoqWA81uIiULWD1Fj+IVoY3ZvgivoYOiEFBJ9lbb4te
g9m5UT/AaVDTWuHzbspVlbiVe+qyB77C2daWzNyx6UYBPLOo4r0t0c91kbNE5lgj
Z7xz6los0N1U8vq91EFSeQJoSQ62XWavYmlCLmdNT6BNfgh4icLsT7Vr1QMX9jzn
JtTPxdXytSdHvpSpULsqJ016l0dtmONcK3z9mj5N5z0k1tg1AH970TGYOe2aUcSx
IRDMXDOPyzEfjwARAQABAAv9F2CwsjS+Sjh1M1vegJbZjei4gF1HHpEM0K0PSXsp
SfVvpR4AoSJ4He6CXSMWg0ot8XKtDuZoV9jnJaES5UL9pMAD7JwIOqZm/DYVJM5h
OASCh1c356/wSbFbzRHPtUdZO9Q30WFNJM5pHbCJPjtNoRmRGkf71RxtvHBzy7np
Ga+W6U/NVKHw0i0CYwMI0YlKDakYW3Pm+QL+gHZFvngGweTod0f9l2VLLAmeQR/c
+EZs7lNumhuZ8mXcwhUc9JQIhOkpO+wreDysEFkAcsKbkQP3UDUsA1gFx9pbMzT0
tr1oZq2a4QBtxShHzP/ph7KLpN+6qtjks3xB/yjTgaGmtrwM8tSe0wD1RwXS+/1o
```

```
BHpXTnQ7TfeOGUAu4KCoOQLv6ELpKWbRBLWuiPwMdbGpvVFALO8+kvKAg9/r+/ny
zM2GQHY+J3Jh5JxPiJnHfXNZjIKLbFbIPdSKNyJBuazXW8xIa//mEHMI5OcvsZBK
clAIp7LXzjEjKXIwHwDcTn9pBgDpdOKTHOtJ3JUKx0rWVsDH6wq6iKV/FTVSY5jl
zN+puOEsskF1Lfxn9JsJihAVO3yNsp6RvkKtyNlFazaCVKtDAmkjoh60XNxcNRqr
gCnwdpbgdHP6v/hvZY54ZaJjz6L2e8unNEkYLxDt8cmAyGPgH2XgL7giHIp9jrsQ
aS381gnYwNX6wE1aEikgtY91nqJjwPlibF9avSyYQoMtEqM/1UjTjB2KdD/MitK5
fP0VpvuXpNYZedmyq4UOMwdkiNMGAOrfmOeT0olgLrTMT5H97Cn3Yxbk13uXHNu/
ZUZZNe8s+QtuLfUlKAJtLEUutN33TlWQY522FV0m17S+b80xJib3yZVJteVurrh5
HSWHAM+zghQAvCesg5CLXa2dNMkTCmZKgCBvfDLZuZbjFwnwCI6u/NhOY9egKuUf
SA/je/RXaT8m5VxLYMxwqQXKApzD87fv0tLPlVIEvjEsaf992tFEFSNPcG1l/jpd
5AVXw6kKuf85UkJtYR1x2MkQDrqY1QX/XMw00kt8y9kMZUre19aCArcmor+hDhRJ
E3Gt4QJrD9z/bICESw4b4z2DbgD/Xz9IXsA/r9cKiM1h5QMtXvuhyfVeM01enhxM
GbOH3gjqqGNKysx0UODGEwr6AV9hAd8RWXMchJLaExK9J5SRawSg671ObAU24SdY
vMQ9Z4kAQ2+1ReUZzf3ogSMRZtMT+d18gT6L90/y+APZIaoArLPhebIAGq39HLmJ
26x3z0WAgrpA1kNsjXEXkoiZGPLKIGoe3hqJAbYEGAEKACAWIQTRpm4aI7GCyZgP
eIz7/MgqAV5zMAUCXaWc8gIbDAAKCRD7/MgqAV5zMOn/C/9ugt+HZIwX308zI+QX
c5vDLReuzmJ3ieE0DMO/uNSC+K1XEioSIZP91HeZJ2kbT9nn9fuReuoff0T0Dief
rbwcIQQHFFkrqSp1K3VWmUGp2JrUsXFVdjy/fkBIjTd7c5boWljv/6wAsSfiv2V0
JSM8EFU6TYXxswGjFVfc6X97tJNeIrXL+mpSmPPqy2bztcCCHkWS5lNLWQw+R7Vg
71Fe6yBSNVrqC2/imYG2J9zlowjx1XU63Wdgqp2Wxt0l8OmsB/W80S1fRF5G4SDH
s9HXglXXqPsBRZJYfP+VStm9L5P/sKjCcX6WtZR7yS6G8zj/X767MLK/djANvpPd
NVniEke6hM3CNBXYPAMhQBMWhCulcoz+0lxi8L34rMN+Dsbma96psdUrn7uLaB91
6we0CTfF8qqm7BsVAgalon/UUiuMY80U3ueoj3okiSTiHIjD/YtpXSPioC8nMng7
xqAY9Bwizt4FWgXuLm1a4+So4V9j1TRCXd12Uc2l2RNmgDE=
=miES
-----END PGP PRIVATE KEY BLOCK-----
```

3.3. Bob's Revocation Certificate

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: Bob's revocation certificate
Comment: https://www.ietf.org/id/draft-bre-openpgp-samples-01.html

iQG2BCABCgAgFiEE0aZuGiOxgsmYD3iM+/zIKgFeczAFAl2lnQQCHQAACgkQ+/zI
KgFeczAIHAv/RrlGlPFKsW0BShC8sVtPfbT1N9lUqyrsgBhrUryM/i+rBtkbnSjp
28R5araupt0og1g2L5VsCRM+ql0jf0zrZXOorKfAO70HCP3X+MlEquvztMUZGJRZ
7TSMgIY1MeFgLmOw9pDKf3tSoouBOpPe5eVfXviEDDo2zOfdntjPyCMlxHgAcjZo
XqMaurV+nKWoIx0zbdpNLsRy4JZcmnOSFdPw37R8U2miPi2qNyVwcyCxQy0LjN7Y
AWadrs9vE0DrneSVP2OpBhl7g+Dj2uXJQRPVXcq6w9g5Fir6DnlhekTLsa78T5cD
n8q7aRusMlALPAOosENOgINgsVcjuILkPN1eD+zGAgHgdiKaep1+P3pbo5n0CLki
UCAsLnCEo8eBV9DCb/n1FlI5yhQhgQyMYlp/49H0JSc3IY9KHhv6f0zIaRWs0JuD
ajcXTJ9AyB+SA6GBb9Q+XsNXjZ1gj75ekUD1sQ3ezTvVfovgP5bD+vPvILhSImKB
aU6V3zld/x/1
=mMwU
-----END PGP PUBLIC KEY BLOCK-----
```

4. 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.

5. IANA Considerations

IANA has nothing to do for this document.

6. 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/openpgp-wg/openpgp-samples or by e-mail to the authors. Please direct all significant commentary to the public IETF OpenPGP mailing list: openpgp@ietf.org

6.1. Document History

Changes between -00 and -01:

- converted to XML2RFC v3
- added internal backreferences to sample material to spread awareness

7. Acknowledgements

The authors would like to acknowledge the help and input of the other participants at the OpenPGP e-mail summit 2019 [OpenPGP-Email-Summit-2019].

8. References

8.1. Normative References

[I-D.ietf-openpgp-rfc4880bis] Koch, W., carlson, b., Tse, R., Atkins, D., and D. Gillmor, "OpenPGP Message Format", Work in Progress, Internet-Draft, draft-ietf-openpgp-rfc4880bis-08, 6 September 2019, <http://www.ietf.org/internet-drafts/draft-ietf-openpgp-rfc4880bis-08.txt>.

[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>.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007, <https://www.rfc-editor.org/info/rfc4880>.

[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>.

8.2. Informative References

[I-D.draft-dkg-openpgp-abuse-resistant-keystore-04]
Gillmor, D., "Abuse-Resistant OpenPGP Keystores", Work in Progress, Internet-Draft, draft-dkg-openpgp-abuse-resistant-keystore-04, 22 August 2019, <http://www.ietf.org/internet-drafts/draft-dkg-openpgp-abuse-resistant-keystore-04.txt>.

[OpenPGP-Email-Summit-2019] "OpenPGP Email Summit 2019", October 2019, <https://wiki.gnupg.org/OpenPGPEmailSummit201910>.

Authors' Addresses

Bjarni Rúnar Einarsson
Mailpile ehf
Baronsstig
Iceland
Email: bre@mailpile.is

juga
Independent
Email: juga@riseup.net

Daniel Kahn Gillmor
American Civil Liberties Union
125 Broad St.
New York, NY, 10004
United States of America
Email: dkg@fifthhorseman.net