openpgp
Internet-Draft
Intended status: Informational
Expires: 9 November 2025

B. R. Einarsson
Mailpile ehf
juga
Independent
D. K. Gillmor
ACLU

8 May 2025

OpenPGP Example Keys and Certificates
draft-bre-openpgp-samples-03

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.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://openpgp-wg.gitlab.io/openpgp-samples/. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/.

Discussion of this document takes place on the OpenPGP Working Group mailing list (mailto:openpgp@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/openpgp/. Subscribe at https://www.ietf.org/mailman/listinfo/openpgp/.

Source for this draft and an issue tracker can be found at https://gitlab.com/openpgp-wg/openpgp-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/.

Copyright Notice

Table of Contents

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 four "personas", Alice, Bob, Carol, and David. Alice has two certificates currently active: a version 4 certificate, using legacy framing for the Ed25519 elliptic curve algorithm (for compatibility with legacy implementations), and a modern v6 certificate using standard mandatory-to-implement (MTI) algorithms from [RFC9580]. Bob also uses a version 4 certificate, but he fears a potential quantum computer that might attack 256-bit ECC security, and has a 3072-bit RSA key which he thinks might force an adversary with a quantum computer to spend more resources attacking. Carol is a bit behind the times and has a DSA/ElGamal key, which is deprecated in [RFC9580]. David is a minimalist, and uses version 6 certificate offering mainly MTI algorithms from [RFC9580].

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 terminology from [RFC9580]. For subtle terminology changes from older versions of OpenPGP, see Appendix B.1 of [RFC9580].

2. Alice’s Certificates

Alice has two certificates in operation at once, as she is trying to transition from her old certificate to a more up-to-date version.

2.1. Alice’s Ed25519Legacy Version 4 Certificate

Properties:

* OpenPGP Version: 4
* Fingerprint: EB85 BB5F A33A 75E1 5E94 4E63 F231 550C 4F47 E38E
* Primary key algorithm: EdDSALegacy(Ed25519Legacy) (Section 5.5.5.5 of [RFC9580])
* 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 for SEIPDv1: AES-256, AES-192, AES-128, 3DES
* Hash algorithm preferences: SHA512, SHA384, SHA256, SHA224, SHA1
* Compresson algorithm preferences: ZLIB, BZip2, ZIP
* Subkey algorithm: ECDH (Curve25519Legacy)
* 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 Section 5.2.3.35 of [RFC9580])

2.1.1. Alice’s Version 4 OpenPGP Certificate

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: Alice’s v4 OpenPGP certificate
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

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

2.1.2. Alice’s Version 4 OpenPGP Secret Key Material

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Comment: Alice’s v4 OpenPGP Transferable Secret Key
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

lFgEXEcE6RYJKwYBBAHaRw8BAQdArjWwk3FAqyiFbFBKT4TzXcVBqPTB3gmzlC/U
b7O1u10AAP9XBeW6lzGOLx7zHH9AsUDUTb2pggYGMzd0P3ulJ2AfvQ4RtCZBbGlj
ZSBMb3ZlbGFjZSA8YWxpY2VAb3BlbnBncC5leGFtcGxlPoiQBBMWCAA4AhsDBQsJ
CAcCBhUKCQgLAgQWAgMBAh4BAheAFiEE64W7X6M6deFelE5j8jFVDE9H444FAl2l
nzoACgkQ8jFVDE9H447pKwD6A5xwUqIDprBzrHfahrImaYEZzncqb25vkLV2arYf
a78A/R3AwtLQvjxwLDuzk4dUtUwvUYibL2sAHwj2kGaHnfICnF0EXEcE6RIKKwYB
BAGXVQEFAQEHQEL/BiGtq0k84Km1wqQw2DIikVYrQrMttN8d7BPfnr4iAwEIBwAA
/3/xFPG6U17rhTuq+07gmEvaFYKfxRB6sgAYiW6TMTpQEK6IeAQYFggAIBYhBOuF
u1+jOnXhXpROY/IxVQxPR+OOBQJcRwTpAhsMAAoJEPIxVQxPR+OOWdABAMUdSzpM
hzGs1O0RkWNQWbUzQ8nUOeD9wNbjE3zR+yfRAQDbYqvtWQKN4AQLTxVJN5X5AWyb
Pnn+We1aTBhaGa86AQ==
=n8OM
-----END PGP PRIVATE KEY BLOCK-----
```

2.1.3. Alice’s Version 4 Revocation Certificate

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: Alice’s v4 revocation certificate
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

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

2.2. Alice’s Version 6 Certificate

Properties:

* OpenPGP Version: 6
* Fingerprint:
* Primary key algorithm: Ed25519 (Section 5.5.5.9 of [RFC9580])
* Primary key creation date: 2025-05-08
* Primary key capabilities: certify, sign
* User ID: Alice Lovelace <alice@openpgp.example>
* Symmetric algorithm preferences for SEIPDv1: AES-256, AES-128
* Ciphersuite preferences for SEIPDv2: AES-256+OCB, AES-128+OCB
* Hash algorithm preferences: SHA512, SHA256
* Compresson algorithm preferences: Uncompressed, Zlib
* Subkey algorithm: X25519 (Section 5.5.5.7 of [RFC9580])
* Subkey capabilities: encrypt
* Subkey creation date: 2025-05-08
* 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 Section 5.2.3.35 of [RFC9580])

2.2.1. Alice’s Version 6 OpenPGP Certificate

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: Alice’s v6 OpenPGP certificate
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

xioGaBzZBhsAAAAgaJvdqiQPPe0mLXXurqTUwVdBb29n/way5Q8Nx9GCnDfCsAYf
GwoAAABBBYJoHNkGAwsJBwMVCggDFgACApsDAh4JIqEG5GpHmgZCqlNv9TW7HEOX
s16IEj9OAWVn0u91E6MEEfIFJwkCBwIAAAAjAAgwA02wiFFCT07l+Yr84wJWANg
4OYkV+eGU1OWOO9OOdxNgGQhsHEW6AgOb7Sj0fRUskcqgSAsfMI2oqzzD1XG/typ
uYLHAKAHnqGyzRydg9+SVe9eQR1FPjI2xH62T38KzSZBbGljZSBMb3ZlbGFjZSA8
YWxpY2VAb3BlbnBncC5leGFtcGxlPsKbBhMbCgAAACwFgmgc2QYCGQEioQbkakea
BkKqU2/1NbscQ5ezXogSP04BZWfS73UTowQR8gAAAAC//CAXohjgLPyA9tF0ycnt
CnOCjmxGDUHsaXGOCLKuMqTgWcidu2ja+MJD+Ji8aW5/T3cptP0VgPlVIUO2WOfp
R696NBW9+9QWY0PIUNe76Eb6ZVM6hAIDvKi8o+rUeJdxOwfOKgZoHNkGGQAAACDQ
N8/qc1weHlL/3EEQUeHu86A5m9UzFdtoD+yZAmN1ccKbBhgbCgAAACwFgmgc2QYC
mwwioQbkakeaBkKqU2/1NbscQ5ezXogSP04BZWfS73UTowQR8gAAAADGtyDzQG3f
Evv23p56q981flET9fBxXbK4SGdxt/UH4Rr88vmXU6h8brN7gg1JgvEjbkefwsbY
rMj17ndS3u/YcWGEyz9oNFSKlecpUT9QR3EIab2onDv74NDe5rJGd868bgY=
-----END PGP PUBLIC KEY BLOCK-----
```

2.2.2. Alice’s Version 6 OpenPGP Secret Key Material

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Comment: Alice’s v6 OpenPGP Transferable Secret Key
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

xUsGaBzZBhsAAAAgaJvdqiQPPe0mLXXurqTUwVdBb29n/way5Q8Nx9GCnDcARFLH
px8+g7SoDwUCBTh1VJVqZVN2dNTtC1zc+mhMkqfCsAYfGwoAAABBBYJoHNkGAwsJ
BwMVCggDFgACApsDAh4JIqEG5GpHmgZCqlNv9TW7HEOXs16IEj9OAWVn0u91E6ME
EfIFJwkCBwIAAAAjAAgwA02wiFFCT07l+Yr84wJWANg4OYkV+eGU1OWOO9OOdxN
gGQhsHEW6AgOb7Sj0fRUskcqgSAsfMI2oqzzD1XG/typuYLHAKAHnqGyzRydg9+S
Ve9eQR1FPjI2xH62T38KzSZBbGljZSBMb3ZlbGFjZSA8YWxpY2VAb3BlbnBncC5l
eGFtcGxlPsKbBhMbCgAAACwFgmgc2QYCGQEioQbkakeaBkKqU2/1NbscQ5ezXogS
P04BZWfS73UTowQR8gAAAAC//CAXohjgLPyA9tF0ycntCnOCjmxGDUHsaXGOCLKu
MqTgWcidu2ja+MJD+Ji8aW5/T3cptP0VgPlVIUO2WOfpR696NBW9+9QWY0PIUNe7
6Eb6ZVM6hAIDvKi8o+rUeJdxOwfHSwZoHNkGGQAAACDQN8/qc1weHlL/3EEQUeHu
86A5m9UzFdtoD+yZAmN1cQCJHOx++DEy+WW72TrVnUUPhD7Rbdqe2cixtp0WnzDo
PcKbBhgbCgAAACwFgmgc2QYCmwwioQbkakeaBkKqU2/1NbscQ5ezXogSP04BZWfS
73UTowQR8gAAAADGtyDzQG3fEvv23p56q981flET9fBxXbK4SGdxt/UH4Rr88vmX
U6h8brN7gg1JgvEjbkefwsbYrMj17ndS3u/YcWGEyz9oNFSKlecpUT9QR3EIab2o
nDv74NDe5rJGd868bgY=
-----END PGP PRIVATE KEY BLOCK-----
```

2.2.3. Alice’s Version 6 Revocation Certificate

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: Alice's v6 revocation certificate
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

xioGaBzZBhsAAAAgaJvdqiQPPe0mLXXurqTUwVdBb29n/way5Q8Nx9GCnDfCpgYg
GwoAAAA3BYJoHNlyDR0AdW5zcGVjaWZpZWQiIQbkakeaBkKqU2/1NbscQ5ezXogS
P04BZWfS73UTowQR8gAAAAD2xiAY2Be2UdkRKDkl/dgsqXGqUFYMPGmr70NN05mr
yDY0wGDKu7RlQ6V2EHRJTdh44lMh44Eh73JIVy9PvT08a+C287zH8JT2PMLnsz35
1HmbrkUmgAdHthtv4VdWL/pjIw8=
-----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 (Section 5.5.5.1 of [RFC9580])
* 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 for SEIPDv1: 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 Section 5.2.3.35 of [RFC9580])

3.1. Bob’s OpenPGP Certificate

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: Bob’s OpenPGP certificate
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

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://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

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://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

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. Carol's DSA/ElGamal Samples

Properties:

* OpenPGP Version: 4
* Fingerprint: 71FF DA00 4409 E5DD B0C3 E8F1 9BA7 89DC 76D6 849A
* Primary key algorithm: DSA 3072/256 (Section 5.5.5.2 of [RFC9580])
* Primary key creation date: Sat Dec 21 2019
* Primary key capabilities: certify, sign
* User ID: Carol Oldstyle <carol@openpgp.example>
* Symmetric algorithm preferences for SEIPDv1: AES-256, AES-192, AES-128
* Hash algorithm preferences: SHA512, SHA384, SHA256
* Compresson algorithm preferences: ZIP
* Subkey algorithm: ElGamal 3072/256
* Subkey capabilities: encrypt
* Subkey creation date: Sat Dec 21 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 Section 5.2.3.35 of [RFC9580])

4.1. Carol’s OpenPGP Certificate


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: Carol’s OpenPGP certificate
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

xsPuBF3+CmgRDADZhdKTM3ms3XpXnQke83FgaIBtP1g1qhqpCfg50WiPS0kjiMC0
OJz2vh59nusbBLzgI//Y1VMhKfIWYbqMcIY+lWbseHjl52rqW6AaJ0TH4NgVt7vh
yVeJt0k/NnxvNhMd0587KXmfpDxrwBqc/l5cVB+p0rL8vs8kxojHXAi5V3koM0Uj
REWs5Jpj/XU9LhEoyXZkeJC/pes1u6UKoFYn7dFIP49Kkd1kb+1bNfdPYtA0JpcG
zYgeMNOvdWJwn43dNhxoeuXfmAEhA8LdzT0C0O+7akXOKWrfhXJ8MTBqvPgWZYx7
MNuQx/ejIMZHl+Iaf7hG976ILH+NCGiKkhidd9GIuA/WteHiQbXLyfiQ4n8P12q9
+4dq6ybUM65tnozRyyN+1m3rU2a/+Ly3JCh4TeO27w+cxMWkaeHyTQaJVMbMbDpX
duVd32MA33UVNH5/KXMVczVi5asVjuKDSojJDV1QwX8izZNl1t+AI0L3balCabV0
SFhlfnBEUj1my1sBAMOSO/I67BvBS3IPHZWXHjgclhs26mPzRlZLryAUWR2DDACH
5fx+yUAdZ8Vu/2zWTHxwWJ/X6gGTLqa9CmfDq5UDqYFFzuWwN4HJ+ryOuak1CGwS
KJUBSA75HExbv0naWg+suy+pEDvF0VALPU9VUkSQtHyR10YO2FWOe3AEtpbYDRwp
dr1ZwEbb3L6IGQ5i/4CNHbJ2u3yUeXsDNAvrpVSEcIjA01RPCOKmf58SDZp4yDdP
xGhM8w6a18+fdQr22f2cJ0xgfPlbzFbO+FUsEgKvn6QTLhbaYw4zs7rdQDejWHV8
2hP4K+rb9FwknYdV9uo4m77MgGlU+4yvJnGEYaL3jwjI3bH9aooNOl6XbvVAzNzo
mYmaTO7mp6xFAu43yuGyd9K+1E4k7CQTROxTZ+RdtQjV95hSsEmMg792nQvDSBW4
xwfOQ7pf3kC7r9fm8u9nBlEN12HsbQ8Yvux/ld5q5RaIlD19jzfVR6+hJzbj2ZnU
yQs4ksAfIHTzTdLttRxS9lTRTkVx2vbUnoSBy6TYF1mf6nRPpSm1riZxnkR4+BQL
/0rUAxwegTNIG/5M612s2a45QvYK1turZ7spI1RGitJUIjBXUuR76jIsyqagIhBl
5nEsQ4HLv8OQ3EgJ5T9gldLFpHNczLxBQnnNwfPoD2e0kC/iy0rfiNX8HWpTgQpb
zAosLj5/E0iNlildynIhuqBosyRWFqGva0O6qioL90srlzlfKCloe9R9w3HizjCb
f59yEspuJt9iHVNOPOW2Wj5ub0KTiJPp9vBmrFaB79/IlgojpQoYvQ77Hx5A9CJq
paMCHGOW6Uz9euN1ozzETEkIPtL8XAxcogfpe2JKE1uS7ugxsKEGEDfxOQFKAGV0
XFtIx50vFCr2vQro0WB858CGN47dCxChhNUxNtGc11JNEkNv/X7hKtRf/5VCmnaz
GWwNK47cqZ7GJfEBnElD7s/tQvTC5Qp7lg9gEt47TUX0bjzUTCxNvLosuKL9+J1W
ln1myRpff/5ZOAnZTPHR+AbX4bRB4sK5zijQe4139Dn2oRYK+EIYoBAxFxSOzehP
IcKKBB8RCAA8BQJd/gppAwsJCgkQm6eJ3HbWhJoEFQoJCAIWAQIXgAIbAwIeARYh
BHH/2gBECeXdsMPo8Zunidx21oSaAABihQD/VWnF1HbBhP+kLwWsqxuYjEslEsM2
UQPeKGK9an8HZ78BAJPaiL3OpuOmsIoCfOghhMZOKXjIV+Z57LwaMw7FQfPgzSZD
YXJvbCBPbGRzdHlsZSA8Y2Fyb2xAb3BlbnBncC5leGFtcGxlPsKKBBMRCAA8BQJd
/gppAwsJCgkQm6eJ3HbWhJoEFQoJCAIWAQIXgAIbAwIeARYhBHH/2gBECeXdsMPo
8Zunidx21oSaAABQTAD/ZMXAvSbKaMJJpAfwp1C7KAj6K2k2CAz5jwUXyGf1+jUA
/2iAMiX1XcLy3n0L8ytzge8/UAFHafBl4rn4DmUugfhjzsPMBF3+CmgQDADZhdKT
M3ms3XpXnQke83FgaIBtP1g1qhqpCfg50WiPS0kjiMC0OJz2vh59nusbBLzgI//Y
1VMhKfIWYbqMcIY+lWbseHjl52rqW6AaJ0TH4NgVt7vhyVeJt0k/NnxvNhMd0587
KXmfpDxrwBqc/l5cVB+p0rL8vs8kxojHXAi5V3koM0UjREWs5Jpj/XU9LhEoyXZk
eJC/pes1u6UKoFYn7dFIP49Kkd1kb+1bNfdPYtA0JpcGzYgeMNOvdWJwn43dNhxo
euXfmAEhA8LdzT0C0O+7akXOKWrfhXJ8MTBqvPgWZYx7MNuQx/ejIMZHl+Iaf7hG
```

```
976ILH+NCGiKkhidd9GIuA/WteHiQbXLyfiQ4n8P12q9+4dq6ybUM65tnozRyyN+
1m3rU2a/+Ly3JCh4TeO27w+cxMWkaeHyTQaJVMbMbDpXduVd32MA33UVNH5/KXMV
czVi5asVjuKDSojJDV1QwX8izZNl1t+AI0L3balCabV0SFhlfnBEUj1my1sMAIfl
/H7JQB1nxW7/bNZMfHBYn9fqAZMupr0KZ8OrlQOpgUXO5bA3gcn6vI65qTUIbBIo
lQFIDvkcTFu/SdpaD6y7L6kQO8XRUAs9T1VSRJC0fJHXRg7YVY57cAS2ltgNHCl2
vVnARtvcvogZDmL/gI0dsna7fJR5ewM0C+ulVIRwiMDTVE8I4qZ/nxINmnjIN0/E
aEzzDprXz591CvbZ/ZwnTGB8+VvMVs74VSwSAq+fpBMuFtpjDjOzut1AN6NYdXza
E/gr6tv0XCSdh1X26jibvsyAaVT7jK8mcYRhovePCMjdsf1qig06Xpdu9UDM3OiZ
iZpM7uanrEUC7jfK4bJ30r7UTiTsJBNE7FNn5F21CNX3mFKwSYyDv3adC8NIFbjH
B85Dul/eQLuv1+by72cGUQ3XYextDxi+7H+V3mrlFoiUPX2PN9VHr6EnNuPZmdTJ
CziSwB8gdPNN0u21HFL2VNFORXHa9tSehIHLpNgXWZ/qdE+lKbWuJnGeRHj4FAv+
MQaafW0uHF+N8MDm8UWPvf4Vd0UJ0UpIjRWl2hTV+BHkNfvZlBRhhQIphNiKRe/W
ap0f/lW2Gm2uS0KgByjjNXEzTiwrte2GX65M6F6Lz8N31kt1Iig1xGOuv+6HmxTN
R8gL2K5PdJeJn8PTJWrRS7+BY8Hdkgb+wVpzE5cCvpFiG/P0yqfBdLWxVPlPI7dc
hDkmx4iAhHJX9J/gX/hC6L3AzPNJqNPAKy20wYp/ruTbbwBolW/4ikWij460JrvB
sm6Sp81A3ebaiN9XkJygLOyhGyhMieGulCYz6AahAFcECtPXGTcordV1mJth8yjF
4gZfDQyg0nMW4Yr49yeFXcRMUw1yzN3Q9v2zzqDuFi2lGYTXYmVqLYzM9KbLO2Wx
E/21xnBjLsl09l/FdA/bhdZq3t4/apbFOeQQ/j/AphvzWbsJnhG9Q7+d3VoDlz0g
FiSduCYIAAq8dUOJNjrUTkZsL1pOIjhYjCMi2uiKS6RQkT6nvuumPF/D/VTnUGeZ
wooEGBEIADwFAl3+CmkDCwkKCRCbp4ncdtaEmgQVCgkIAhYBAheAAhsMAh4BFiEE
cf/aAEQJ5d2ww+jxm6eJ3HbWhJoAAEEpAP91hFqmcb2ZqVcaRDMSVmhkEcFIRmpH
vDoQtVn8sArWqwEAi8HwbMhL+YwRItRZDknpC4vFjTHVMd1zMrz/JyeuT9k=
=pa/S
-----END PGP PUBLIC KEY BLOCK-----
```

4.2. Carol’s OpenPGP Secret Key Material

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Comment: Carol’s OpenPGP Transferable Secret Key
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

xcQTBF3+CmgRDADZhdKTM3ms3XpXnQke83FgaIBtP1g1qhqpCfg50WiPS0kjiMC0
OJz2vh59nusbBLzgI//Y1VMhKfIWYbqMcIY+lWbseHjl52rqW6AaJ0TH4NgVt7vh
yVeJt0k/NnxvNhMd0587KXmfpDxrwBqc/l5cVB+p0rL8vs8kxojHXAi5V3koM0Uj
REWs5Jpj/XU9LhEoyXZkeJC/pes1u6UKoFYn7dFIP49Kkd1kb+1bNfdPYtA0JpcG
zYgeMNOvdWJwn43dNhxoeuXfmAEhA8LdzT0C0O+7akXOKWrfhXJ8MTBqvPgWZYx7
MNuQx/ejIMZHl+Iaf7hG976ILH+NCGiKkhidd9GIuA/WteHiQbXLyfiQ4n8P12q9
+4dq6ybUM65tnozRyyN+1m3rU2a/+Ly3JCh4TeO27w+cxMWkaeHyTQaJVMbMbDpX
duVd32MA33UVNH5/KXMVczVi5asVjuKDSojJDV1QwX8izZNl1t+AI0L3balCabV0
SFhlfnBEUj1my1sBAMOSO/I67BvBS3IPHZWXHjgclhs26mPzRlZLryAUWR2DDACH
5fx+yUAdZ8Vu/2zWTHxwWJ/X6gGTLqa9CmfDq5UDqYFFzuWwN4HJ+ryOuak1CGwS
KJUBSA75HExbv0naWg+suy+pEDvF0VALPU9VUkSQtHyR10YO2FWOe3AEtpbYDRwp
dr1ZwEbb3L6IGQ5i/4CNHbJ2u3yUeXsDNAvrpVSEcIjA01RPCOKmf58SDZp4yDdP
xGhM8w6a18+fdQr22f2cJ0xgfPlbzFbO+FUsEgKvn6QTLhbaYw4zs7rdQDejWHV8
2hP4K+rb9FwknYdV9uo4m77MgGlU+4yvJnGEYaL3jwjI3bH9aooNOl6XbvVAzNzo
mYmaTO7mp6xFAu43yuGyd9K+1E4k7CQTROxTZ+RdtQjV95hSsEmMg792nQvDSBW4
xwfOQ7pf3kC7r9fm8u9nBlEN12HsbQ8Yvux/ld5q5RaIlD19jzfVR6+hJzbj2ZnU
yQs4ksAfIHTzTdLttRxS9lTRTkVx2vbUnoSBy6TYF1mf6nRPpSm1riZxnkR4+BQL
```

```
/0rUAxwegTNIG/5M612s2a45QvYK1turZ7spI1RGitJUIjBXUuR76jIsyqagIhBl
5nEsQ4HLv8OQ3EgJ5T9gldLFpHNczLxBQnnNwfPoD2e0kC/iy0rfiNX8HWpTgQpb
zAosLj5/E0iNlildynIhuqBosyRWFqGva0O6qioL90srlzlfKCloe9R9w3HizjCb
f59yEspuJt9iHVNOPOW2Wj5ub0KTiJPp9vBmrFaB79/IlgojpQoYvQ77Hx5A9CJq
paMCHGOW6Uz9euN1ozzETEkIPtL8XAxcogfpe2JKE1uS7ugxsKEGEDfxOQFKAGV0
XFtIx50vFCr2vQro0WB858CGN47dCxChhNUxNtGc11JNEkNv/X7hKtRf/5VCmnaz
GWwNK47cqZ7GJfEBnElD7s/tQvTC5Qp7lg9gEt47TUX0bjzUTCxNvLosuKL9+J1W
ln1myRpff/5ZOAnZTPHR+AbX4bRB4sK5zijQe4139Dn2oRYK+EIYoBAxFxSOzehP
IQAA/2BCN5HryGjVff2t7Q6fVrQQS9hsMisszZl5rWwUOO6zETHCigQfEQgAPAUC
Xf4KaQMLCQoJEJunidx21oSaBBUKCQgCFgECF4ACGwMCHgEWIQRx/9oARAnl3bDD
6PGbp4ncdtaEmgAAYoUA/1VpxdR2wYT/pC8FrKsbmIxLJRLDNlED3ihivWp/B2e/
AQCT2oi9zqbjprCKAnzoIYTGTil4yFfmeey8GjMOxUHz4M0mQ2Fyb2wgT2xkc3R5
bGUgPGNhcm9sQG9wZW5wZ3AuZXhhbXBsZT7CigQTEQgAPAUCXf4KaQMLCQoJEJun
idx21oSaBBUKCQgCFgECF4ACGwMCHgEWIQRx/9oARAnl3bDD6PGbp4ncdtaEmgAA
UEwA/2TFwL0mymjCSaQH8KdQuygI+itpNggM+Y8FF8hn9fo1AP9ogDIl9V3C8t59
C/Mrc4HvP1ABR2nwZeK5+A5lLoH4Y8fD8QRd/gpoEAwA2YXSkzN5rN16V50JHvNx
YGiAbT9YNaoaqQn4OdFoj0tJI4jAtDic9r4efZ7rGwS84CP/2NVTISnyFmG6jHCG
PpVm7Hh45edq6lugGidEx+DYFbe74clXibdJPzZ8bzYTHdOfOyl5n6Q8a8AanP5e
XFQfqdKy/L7PJMaIx1wIuVd5KDNFI0RFrOSaY/11PS4RKMl2ZHiQv6XrNbulCqBW
J+3RSD+PSpHdZG/tWzX3T2LQNCaXBs2IHjDTr3VicJ+N3TYcaHrl35gBIQPC3c09
AtDvu2pFzilq34VyfDEwarz4FmWMezDbkMf3oyDGR5fiGn+4Rve+iCx/jQhoipIY
nXfRiLgP1rXh4kG1y8n4kOJ/D9dqvfuHausm1DOubZ6M0csjftZt61Nmv/i8tyQo
eE3jtu8PnMTFpGnh8k0GiVTGzGw6V3blXd9jAN91FTR+fylzFXM1YuWrFY7ig0qI
yQ1dUMF/Is2TZdbfgCNC922pQmm1dEhYZX5wRFI9ZstbDACH5fx+yUAdZ8Vu/2zW
THxwWJ/X6gGTLqa9CmfDq5UDqYFFzuWwN4HJ+ryOuak1CGwSKJUBSA75HExbv0na
Wg+suy+pEDvF0VALPU9VUkSQtHyR10YO2FWOe3AEtpbYDRwpdr1ZwEbb3L6IGQ5i
/4CNHbJ2u3yUeXsDNAvrpVSEcIjA01RPCOKmf58SDZp4yDdPxGhM8w6a18+fdQr2
2f2cJ0xgfPlbzFbO+FUsEgKvn6QTLhbaYw4zs7rdQDejWHV82hP4K+rb9FwknYdV
9uo4m77MgGlU+4yvJnGEYaL3jwjI3bH9aooNOl6XbvVAzNzomYmaTO7mp6xFAu43
yuGyd9K+1E4k7CQTROxTZ+RdtQjV95hSsEmMg792nQvDSBW4xwfOQ7pf3kC7r9fm
8u9nBlEN12HsbQ8Yvux/ld5q5RaIlD19jzfVR6+hJzbj2ZnUyQs4ksAfIHTzTdLt
tRxS9lTRTkVx2vbUnoSBy6TYF1mf6nRPpSm1riZxnkR4+BQL/jEGmn1tLhxfjfDA
5vFFj73+FXdFCdFKSI0VpdoU1fgR5DX72ZQUYYUCKYTYikXv1mqdH/5VthptrktC
oAco4zVxM04sK7Xthl+uTOhei8/Dd9ZLdSIoNcRjrr/uh5sUzUfIC9iuT3SXiZ/D
0yVq0Uu/gWPB3ZIG/sFacxOXAr6RYhvz9MqnwXS1sVT5TyO3XIQ5JseIgIRyV/Sf
4F/4Qui9wMzzSajTwCsttMGKf67k228AaJVv+IpFoo+OtCa7wbJukqfNQN3m2ojf
V5CcoCzsoRsoTInhrpQmM+gGoQBXBArT1xk3KK3VdZibYfMoxeIGXw0MoNJzFuGK
+PcnhV3ETFMNcszd0Pb9s86g7hYtpRmE12Jlai2MzPSmyztlsRP9tcZwYy7JdPZf
xXQP24XWat7eP2qWxTnkEP4/wKYb81m7CZ4RvUO/nd1aA5c9IBYknbgmCAAKvHVD
iTY61E5GbC9aTiI4WIwjItroikukUJE+p77rpjxfw/1U51BnmQAA/ih5jIthn2ZE
r1YoOsUs8CBhylTsRZK6VS4ZCErcyl2tD2LCigQYEQgAPAUCXf4KaQMLCQoJEJun
idx21oSaBBUKCQgCFgECF4ACGwwCHgEWIQRx/9oARAnl3bDD6PGbp4ncdtaEmgAA
QSkA/3WEWqZxvZmpVxpEMxJWaGQRwUhGake8OhC1WfywCtarAQCLwfBsyEv5jBEi
1FkOSekLi8WNMdUx3XMyvP8nJ65P2Q==
=Xj8h
-----END PGP PRIVATE KEY BLOCK-----
```

4.3. Carol’s Revocation Certificate

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: Carol’s revocation certificate
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

iHsEIBEKAC0FAmf+z6EJEJunidx21oSaFiEEcf/aAEQJ5d2ww+jxm6eJ3HbWhJoC
hwACHQAAADDHAP9NuS1xgKIoaxxqo9Rh1pQqx/W72oIRTb6SxzORtpOI9gEAtg7d
Inkr6mSPRo5fMV3yPsscVn2TgxFgvV4Zat4j+g0=
=v8ah
-----END PGP PUBLIC KEY BLOCK-----
```

5. David’s v6 Ed25519/X25519 Sample

David Deluxe’s OpenPGP material is a minimalist example focusing on the mandatory-to-implement (MTI) aspects of [RFC9580].

Properties:

* OpenPGP Version: 6
* Fingerprint: 4199D9EAA6682A78D5A534F62BF76222A54E4DEBC785DBE6A6C5B34586026FE2
* Primary key algorithm: Ed25519 (Section 5.5.5.9 of [RFC9580])
* Primary key creation date: 2025-04-16
* Primary key capabilities: certify, sign
* User ID: David Deluxe <david@openpgp.example>
* Symmetric algorithm preferences for SEIPDv1: AES-256, AES-128
* Ciphersuite preferences for SEIPDv2: AES-256+OCB, AES-128+OCB
* Hash algorithm preferences: SHA512, SHA256
* Compresson algorithm preferences: Uncompressed, Zlib
* Subkey algorithm: X25519 (Section 5.5.5.7 of [RFC9580])
* Subkey capabilities: encrypt
* Subkey creation date: 2025-04-16
* 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 Section 5.2.3.35 of [RFC9580])

5.1. David’s OpenPGP Certificate

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: David’s OpenPGP Certificate
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

xioGZ/8j0xsAAAAgzrMRQzWvL9R2j8b0zCEMWYDSqxLVZ2JS2xC/Ug8+fKPCsAYf
GwoAAABBBYJn/yPTAwsJBwMVCggDFgACApsDAh4JIqEGQZnZ6qZoKnjVpTT2K/di
IqVOTevHhdvmpsWzRYYCb+IFJwkCBwIAAAAA698gckuZpqDL4TaSzOoe8YFTLe0g
q1ubFXhpvUY+f1GoNFaw96oz7ZyiQWFBWIhMsie7oLNxSHv1gKQC0Z+ftMbYPSWn
GGyMGEvMxmWjD+ybd2+Bj7uyNEBcX0TCyLYYrNgPzSREYXZpZCBEZWx1eGUgPGRh
dmlkQG9wZW5wZ3AuZXhhbXBsZT7CmwYTGwoAAAAsBYJn/yPTAhkBIqEGQZnZ6qZo
KnjVpTT2K/diIqVOTevHhdvmpsWzRYYCb+IAAAAA8/UgurmDFSbpSNPOjs2CaMoP
hD+wjuW/UxnfPfF/PU88CU+MkFaUB5Dr1OxJWgMHzBZIVzaO1QGY6AGIXmiT9u72
LkjPCpTSrrxKVipagOYn07VDnSBDbOQzGwoAvlInfJgKzioGZ/8j0xkAAAAgq3RT
z+ceY6yb7nSukwG6WSUfWMF7VHHAh1Jd45QpVzzCmwYYGwoAAAAsBYJn/yPTApsM
IqEGQZnZ6qZoKnjVpTT2K/diIqVOTevHhdvmpsWzRYYCb+IAAAAAockg36ZPi7Dp
wz63B7YXv4dlWWZqR5x6vabUAHpSUxuuS+1REOsZ4dSH7br2jLpZ39zSdloBdXSd
x/oP9jK8wYnrWhMykHxkUGy0HtI1jPxNF9b5XfZaRKBI7yObbr3TDocL
-----END PGP PUBLIC KEY BLOCK-----
```

5.2. David’s OpenPGP Secret Key Material

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Comment: David’s OpenPGP Transferable Secret Key
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

xUsGZ/8j0xsAAAAgzrMRQzWvL9R2j8b0zCEMWYDSqxLVZ2JS2xC/Ug8+fKMAsWVF
VyjYBj/6/wmEnerN2Feh1URrBlL6AEtiG3Oui6HCsAYfGwoAAABBBYJn/yPTAwsJ
BwMVCggDFgACApsDAh4JIqEGQZnZ6qZoKnjVpTT2K/diIqVOTevHhdvmpsWzRYYC
b+IFJwkCBwIAAAAA698gckuZpqDL4TaSzOoe8YFTLe0gq1ubFXhpvUY+f1GoNFaw
96oz7ZyiQWFBWIhMsie7oLNxSHv1gKQC0Z+ftMbYPSWnGGyMGEvMxmWjD+ybd2+B
j7uyNEBcX0TCyLYYrNgPzSREYXZpZCBEZWx1eGUgPGRhdmlkQG9wZW5wZ3AuZXhh
bXBsZT7CmwYTGwoAAAAsBYJn/yPTAhkBIqEGQZnZ6qZoKnjVpTT2K/diIqVOTevH
hdvmpsWzRYYCb+IAAAAA8/UgurmDFSbpSNPOjs2CaMoPhD+wjuW/UxnfPfF/PU88
CU+MkFaUB5Dr1OxJWgMHzBZIVzaO1QGY6AGIXmiT9u72LkjPCpTSrrxKVipagOYn
07VDnSBDbOQzGwoAvlInfJgKx0sGZ/8j0xkAAAAgq3RTz+ceY6yb7nSukwG6WSUf
WMF7VHHAh1Jd45QpVzwA7EvQ+nkOmhiM2nzkJtglKebTs+gukMlt5Yfx1HIn2qTC
mwYYGwoAAAAsBYJn/yPTApsMIqEGQZnZ6qZoKnjVpTT2K/diIqVOTevHhdvmpsWz
RYYCb+IAAAAAockg36ZPi7Dpwz63B7YXv4dlWWZqR5x6vabUAHpSUxuuS+1REOsZ
4dSH7br2jLpZ39zSdloBdXSdx/oP9jK8wYnrWhMykHxkUGy0HtI1jPxNF9b5XfZa
RKBI7yObbr3TDocL
-----END PGP PRIVATE KEY BLOCK-----
```

5.3. David’s Revocation Certificate

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: David’s revocation certificate
Comment: https://datatracker.ietf.org/doc/draft-bre-openpgp-samples/

xioGZ/8j0xsAAAAgzrMRQzWvL9R2j8b0zCEMWYDSqxLVZ2JS2xC/Ug8+fKPCoAYg
GwgAAABBBQJn/yR2CRBBmdnqpmgqeA0dAHVuc3BlY2lmaWVkIiEGQZnZ6qZoKnjV
pTT2K/diIqVOTevHhdvmpsWzRYYCb+IAAAAAqU8QckKWTMDfmM6mdwJtKAZf01tA
9Qf7YctkblvDD1fJQwcE4aVaQ3njaulLt6+w1iYpb+YvK4EUUbYeQ14AuMf2iW63
pAW/t62nlcghKDG4VAM=
-----END PGP PUBLIC KEY BLOCK-----
```

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]

8.1. Document History

Changes between -02 and -03: - added new v6 certificate for Alice in addition to the existing v4 cert (representing someone with both a compatibility-focused certificate and a modern certificate)

Changes between -01 and -02: - added Carol (DSA/Elgamal example) - added David (v6 MTI example)

Changes between -00 and -01:

* converted to XML2RFC v3

* added internal backreferences to sample material to spread awareness

9. Acknowledgements

The authors would like to acknowledge the help and input of the other participants at the [OpenPGP-Email-Summit-2019]. Heiko Stamer contributed Carol's OpenPGP material.

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/rfc/rfc2119>.

[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/rfc/rfc8174>.

[RFC9580] Wouters, P., Ed., Huigens, D., Winter, J., and Y. Niibe, "OpenPGP", RFC 9580, DOI 10.17487/RFC9580, July 2024, <https://www.rfc-editor.org/rfc/rfc9580>.

10.2. Informative References

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

Authors' Addresses

Bjarni R炭nar 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