Upcoming MTI choices, and what is left before "done"

Cryptographic algorithms in OpenPGP, the crypto refresh, and beyond

IETF 112

Cryptographic algorithms in RFC 4880

MUST implement

- DSA
- ElGamal
- SHA-1
- TripleDES
- CFB
- Modification Detection Code (MDC) using SHA-1
- V4 keys use SHA-1 for fingerprints

SHOULD implement

- RSA
- AES-128 and CAST5
- ZIP (and is the default)
- Salted+Iterated hashing for “string-to-key” (S2K) key derivation

Deprecations in RFC 4880

MUST NOT

- Use MD5 when signing
- (but MAY verify)

- Use a symmetric algorithm that is not in the recipient's preference list (except TripleDES is implicitly included since it’s MTI)

SHOULD NOT

- Implement keys of <1024 bits (for DSA, ElGamal, RSA)

Cryptographic algorithms in RFC 6637 (ECC in OpenPGP)

MUST implement

- ECDSA and ECDH
- NIST curve P-256
- SHA2-256
- AES-128
- Bonus: SHA-1 MUST NOT be used with ECC

SHOULD implement

- NIST curve P-521
- SHA2-384 and SHA2-512
- AES-256

Cryptographic algorithms in the crypto refresh

Tentative

MUST implement

- EdDSA and ECDH
- Curve25519
- SHA2-256
- AES-128
- AEAD (probably OCB?)
- V5 keys use SHA2-256 for fingerprints

SHOULD implement

- Curve448
- SHA2-384 and SHA2-512
- AES-256
- ZLIB (but uncompressed is the default)
- Argon2 for key derivation

Tentative

Deprecations in the crypto refresh (part 1)

MUST NOT

- Generate <2048 bit RSA keys
- Encrypt, sign, or verify using <1024 bit RSA keys
- Implement DSA or ElGamal

SHOULD NOT

- Encrypt, sign, or verify using <2048 bit RSA keys
- Decrypt using <1024 bit RSA keys

Tentative

Deprecations in the crypto refresh (part 2)

MUST NOT

- Use MD5, SHA-1 or RIPE-MD/160 when signing, and
- Use MD5, SHA-1 or RIPE-MD/160 when verifying “new” signatures
- Encrypt data with IDEA, TripleDES, or CAST5 (but MAY decrypt)
- Use Simple (unsalted) S2K

SHOULD NOT

- Use MD5, SHA-1 or RIPE-MD/160 when verifying “old” signatures
- Use Salted (non-iterated) S2K

Very Tentative

What’s left for the crypto refresh?

- Brainpool curves? → Not a CFRG recommendation
- FIPS compliant MTI algorithms? → NIST Draft SP 800-186 and FIPS 186-5 contain Curve25519 and Curve448
- AES-256 as MTI?

What’s next after this crypto refresh?

Extremely Tentative

- Post-quantum cryptography
- Perfect forward secrecy?

Questions?