Cryptography for IETF protocols

A proposal for discussion by the SEC ADs

Paul Wouters & Deb Cooley
IETF 120 Vancouver
25 July 2024

Streams involved with cryptography

- Internet Engineering Task Force (IETF)
  - Internet Engineering Steering Group (IESG)
    - Security Area Directors (SEC ADs)
  - Working Groups (SEC, OPS, ROUTING, etc)
- Internet Architecture Board (IAB)
- Independent Stream Editor (ISE)
- Internet Research Task Force (IRTF)
  - Crypto Forum Research Group (CFRG)
    - Crypto Panel

History of formal IETF statements related to cryptography

No statements on how we select cryptographic algorithms

- **1996** RFC 1984
  - IAB & IESG Statement on Cryptographic Technology and the Internet
- **2000** RFC 2804
  - IAB & IESG statement on IETF Policy on Wiretapping
- **2003** RFC 3552
  - Guidelines for Writing RFC Text on Security Considerations
- **2013** RFC 6973
  - Privacy Considerations for Internet Protocols
- **2014** RFC 7258
  - Pervasive Monitoring is an Attack
- **2015** IESG Statement
  - Maximizing Encrypted Access To IETF Information

The IETF sometimes specifies or defines cryptographic algorithms

- **MD5** RFC1321
  - The MD5 Message-Digest Algorithm
- **SHA1** RFC3174
  - US Secure Hash Algorithm 1 (SHA1)
- **SHA2** RFC6234
  - US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)
- **AES**
  - Various RFCs
- **ShangMi (SM)** draft-oscca-cfrg-sm3
  - RFC8998 ShangMi (SM) Cipher Suites for TLS 1.3
- **GOST** RFC 4357 / RFC5830 / RFC5832 / RFC7091 / RFC7836
  - Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms
  - GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms
  - GOST R 34.10-2001: Digital Signature Algorithm
  - GOST R 34.10-2012: Digital Signature Algorithm
  - Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012
- **CHACHA20POLY1305** RFC7539
  - ChaCha20 and Poly1305 for IETF Protocols
- **CAMELLIA** RFC3713
  - A Description of the Camellia Encryption Algorithm

The IETF has in the past defined cryptographic suites or profiles

- **Suite B**
  - RFC5430 / RFC6460 / RFC6379 / RFC4869 / RFC8423
  - via AD sponsoring
- **CNSA**
  - RFC8603 / RFC8755 / RFC8756 / RFC9151 / RFC9206 / RFC9212
  - via Independent Stream Editor (ISE)
- **GOST**
  - combined profiles and definitions into one RFC
- **SM**
  - combined profiles and definitions into one draft

Common IANA registration policies

- **Specification Required**
  - Specification on any URL anywhere, preferably stable
  - Can be RFC, draft, expired draft, random website, FTP site
- **Expert Review**
  - Reviewed by Designated Experts
  - Can be 1 of N experts, or N of N experts
- **Standards Action RFC**
  - Standard Track RFC produced by WG
  - Or (unlikely) Area Director sponsored Standard Track RFC
- **(Any) RFC Required**
  - Standards Track, Experimental, Informational or ISE
  - Working Group or AD Sponsored or ISE
- **First Come, First Serve (FCFS)**
  - Usually have a basic validation check by Designated Expert

Sometimes the IANA registry is split with different parts having different policies, sometimes the policy is a mix of the above.

IANA registries for core crypto protocols and their registration policies

• TLS	Specification Required
• IKEv2/IPsec	Expert Review
• PKIX	Use OID ARC. Sometimes uses an RFC
• BGPSEC	(Use TLS or IPsec)
• RPKI	Standards Track RFC
• SSH	Expert Review
• DNSSEC	Any RFC (standards, experimental, ISE)
• Kerberos	Standards Track RFC *or* Expert Review
• CMS / SMIME	Use OID ARC. Sometimes uses an RFC.
• OpenPGP	Specification Required
• MLS	Specification Required

Current and previous SEC ADs have been working on changing registration policies to not require an RFC for cryptographic parameters (where no other constraints apply)

Let SEC ADs know if you know of more relevant registries[*]

[*] by email

IETF

Role of the CFRG

- New cryptographic primitives and algorithms are recommended by Crypto Forum Research Group (CFRG) at the IRTF
- CFRG is the “IETF interest group” towards the public cryptographic community at large. CFRG does not analyse or evaluate cryptography itself.
- Crypto Panel acts as a “directorate”.

Informal IETF policies on cryptography

- Cryptography not recommended by CFRG:
  - Preferably does not get an RFC number
  - Should get a code point if they want one.
  - Do not get RECOMMENDED / SHOULD / MUST status.

Why do people want an RFC ?

- They don't know they don't need one
- An RFC is a status symbol
- No other well known place to publish cryptographic specification that gets implemented
- Vendors won’t implement without an RFC
- Vanity Crypto

SEC AD Proposal

- **Limit publication of crypto RFCs to:**
  - Vetted by public cryptographic community outside the IETF
  - Recommended by CFRG
  - Only crypto that needs IANA “RECOMMENDED YES”
- **Update IANA registries to not require RFC for crypto**
  - Only use Specification Required
  - Except registries that have other limitations
    - eg DNSKEY only has 256 code points
- **No limits on code points (where possible)**
  - Specification Required is enough
  - Maybe some basic Expert Review checks (eg anti-spam)
- **Crypto Profiles / Suites published via ISE**

Next steps

- Those interested should also attend ISOPEN:
  - **Independent Stream Open Meeting**
  - Friday 9.30 - 11.30 in Regency C/D

- Formalize proposal in document(s) for the streams?
- Questions / Comments ?