Ribose

OSCCA Extensions For OpenPGP

draft-ribose-openpgp-oscca

SECDISPATCH, IETF 100 Singapore

16th November 2017

Ronald Tse Wai Kit Wong

Jack Lloyd Daniel Wyatt Erick Borsboom

Enables OpenPGP (RFC4880) to be used within China

Why, and how?

- The **Office of State Commercial Cipher Administration (OSCCA)** governs usage of cryptography in China
- Non-approved cryptographic algorithms are **disallowed especially in hardware**
- Only **3 OSCCA-approved** algorithms
  - SM2: ECC (draft-shen-sm2-ecdsa)
  - SM3: Hash (draft-oscca-cfrg-sm3)
  - SM4: Blockcipher (draft-ribose-cfrg-sm4)

This document defines

- Their usage in OpenPGP
  - Public Key Algorithm **SM2**
  - Hash Algorithm **SM3**
  - Symmetric Key Algorithm **SM4**
- An OSCCA-compliant profile
  - "**OSCCA-SM234**" (as an alternative to B-Suite)

SM2 Elliptic Curve Cryptosystem (ECC) (GB/T 32918.{1-5} -2016)

Algorithm

- SM2 is an **ECC that contains 3 algorithms (DSA, Key Exchange, PKE)** and **a curve**
- *512-bit public key, 256-bit private key*
- See **draft-shen-sm2-ecdsa-02**
- History
  - 2010 First published by OSCCA
  - 2012 Standardized GM/T 0003-2012
  - 2015 Included in ISO/IEC 11889
  - 2016 Published in GB/T 32918.X-2016
  - 2017 Included in ISO/IEC.14888-3

Application in OpenPGP

- **SM2DSA (GB/T 32918.2)** as **OpenPGP "Public Key Algorithm"** (e.g., ECDSA)
- **SM2PKE (GB/T 32918.4)** as **OpenPGP "Public Key Algorithm"** (e.g., RSA)
- SM2KEP (GB/T 32918.3) unused – 2/3-pass and vulnerable to MITM
- **Adheres to GM/T 0009-2012** ("SM2 Application Specification") for interop
- **Uses "SM2 Recommended" EC (GB/T 32918.5-2017)**
- No known feasible attacks today

SM3 Cryptographic Hash Algorithm (GB/T 32905-2016)

Algorithm

- SM3 is a **256-bit digest algorithm**
- See: **draft-oscca-cfrg-sm3**
- Designed by Xiaoyun Wang (SHA-1…)
- Merkel-Damgård, with **strengthened step function and message dependency**
- History
  - 2010: First published by OSCCA
  - 2012: Standardized GM/T 0004-2012
  - 2016: Published as GB/T 32905-2016
  - 2017: Included in ISO/IEC 10118-3

Application in OpenPGP

- **SM3** as an **OpenPGP "Hash Algorithm"**
- Can be used in conjunction with other public key algorithms, including RSA and SM2

- No know feasible attacks today
- Excellent hardware realization and performance, software performance slightly ahead of SHA-256

SM4 Blockcipher (GB/T 32907-2016)

Algorithm

- SM4 is a **128-bit blockcipher**: **8-bit S-box, 32 rounds**
- See **draft-ribose-cfrg-sm4**
- Designed by Shuwang Lu
- History
  - 2003 in GB 15629.11-2003 (WLAN)
  - 2006 Published as “SMS4” by OSCCA
  - 2012 Standardized GM/T 0002-2012
  - 2016 Published as GB/T 32907-2016
  - 2017 in ISO/IEC 18033-3.AMD2

Application in OpenPGP

- **SM4** as an **OpenPGP “Symmetric Encryption Algorithm”**
- As an alternative to AES-128

- Excellent hardware realization
- No known feasible attacks today, latest attack 24-rounds out of 32
- (always beware of side channels)

Implementation details and moving forward

Available for implementers and users

- **SM2/3/4** already available in **Botan, OpenSSL**. Support in **mbedtls / LibreSSL** coming.
- Ribose's **RNP** [1] OpenPGP tool already supports these algorithms
- To implementers: some additional **algorithm-specific fields** required as described in document
- No feasible attacks against SM2, SM3, SM4 today

What's next

- **AD-sponsorship needed**
- Request **codepoints in the IANA PGP registry** (RFC8126)
  - SM2: "Public Key Algorithms"
  - SM3: "Hash Algorithms"
  - SM4: "Symmetric Key Algorithms"
- More examples
- **Feedback / reviews welcome!**

[1] RNP: https://github.com/riboseinc/rnp

*The source of this **Internet-Draft** can be seen at*
https://github.com/riboseinc/rfc-openpgp-oscca/

T H A N K Y O U

*And… this Internet-Draft was created in **AsciiDoc** using **asciidoctor-rfc**. Try it out!*
https://github.com/riboseinc/asciidoctor-rfc/