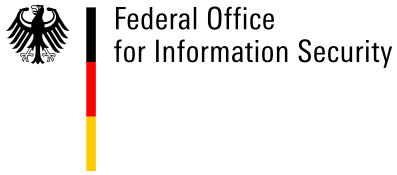
Common Criteria Crypto Working Group

International Cryptographic Module Conference 2017

Fritz Bollmann (BSI)

Mary Baish (NIAP)



Federal Office
for Information Security

Federal Office
for Information Security

Crypto in Common Criteria

Cryptography is ubiquitous in Common Criteria Protection Profiles

- Primarily defined using CC class ‘FCS’
- PPs and SDs specify SFRs and evaluation activities to verify cryptographic security functionality
- Consistency in specification and verification is difficult to achieve

Goal: *Harmonization of the specification and evaluation of crypto mechanisms in collaborative Protection Profiles (cPPs) and product evaluations within CCRA*

Overview

- WG Established in 2015

- Chairpersons
  - Federal Office for Information Security, BSI
  - National Information Assurance Partnership (NIAP)

- The tasks of the WG are to:
  - Assist the iTCs in terms of crypto SFRs and evaluation activities
  - Collate and harmonize crypto evaluation for recognition in the CCRA
  - Develop and maintain crypto Supporting Documents

Challenges

- Coverage of all possible ‘FCS’ components
  - Technology dependent?
  - Guidance needed for iTCs?
- Algorithm agreement
  - 27 nations
  - Clarity in SFRs
- Security strength
  - Not addressed

Covering ‘FCS’ for iTCs

- Piloting Agreed Crypto SFRs
  - USB Portable Storage Device cPP
  - SFR definition complete and delivered to iTC
  - Evaluation activities nearly finished (2-3 outstanding)

Algorithm Agreement

- Approach –
  - provide a means to express all CCRA Participants' needs regarding cryptography – both in the specification of cryptographic functions and the evaluation methodology used to determine TOE compliance with the SFRs
  - tables capture all alternatives
  - Nations specify preferences (or mandates) via position/endorsement statements

Example – Key Generation

FCS_CKM.1.1/Asymm The TSF shall generate **asymmetric** cryptographic keys **[selection: *key name*]** ~~in accordance with a specified cryptographic key generation algorithm [selection: *cryptographic key generation algorithm*] and~~ **with** specified cryptographic key sizes [selection: *key sizes*] that meet the following: [selection: *list of standards*].

The following table provides the allowed choices for completion of the selection operations of FCS_CKM.1.1/Asymm.

Identifier	key name	key sizes	list of standards
AKG1	RSA	[selection: 2048 bit, 3072 bit]	FIPS PUB 186-4 (Section B.3)
AKG2	ECC	[selection: 256 (P-256), 384 (P-384), 512 (P-521)]	FIPS PUB 186-4 (Section B.4 & D.1.2)
AKG3	ECC	[selection: 256 (brainpoolP256r1), 384 (brainpoolP384r1), 512 (brainpoolP512r1)]	RFC5639 (Section 3) [Brainpool Curves] FIPS PUB 186-4 (Section B.4)

Example – User Data Encryption

FCS_COP.1.1/UDE The TSF shall perform *user data encryption/decryption* in accordance with a specified cryptographic algorithm [selection: *cryptographic algorithm*] and cryptographic key sizes [selection: *cryptographic key sizes*] that meet the following: [selection: *list of standards*]

The following table provides the allowed choices for completion of the selection operations of FCS_COP.1/UDE.

Identifier	cryptographic algorithm	key sizes	list of standards
UDE1	AES in CBC mode with non-repeating and unpredictable IVs	[selection: 128 bits, 256 bits]	ISO 18033-3 (AES) ISO 10116 (CBC)
UDE2	AES in CCM mode with unpredictable, non-repeating nonce, minimum size of 64 bits	[selection: 128 bits, 256 bits]	ISO 18033-3 (AES) ISO 19772, sec. 8 (CCM) NIST SP800-38C
UDE3	AES in GCM mode with non-repeating IVs IV length must be equal to 96 bits; the deterministic IV construction method [SP800-38D, Section 8.2.1] must be used; the MAC length t must be one of the values 96, 104, 112, 120, and 128 bits.	[selection: 128 bits, 256 bits]	ISO 18033-3 (AES) ISO 19772, sec.11 (GCM) NIST SP800-38D
UDE4	AES in XTS mode with unique [selection: consecutive non-negative integers starting at an arbitrary non-negative integer, data unit sequence numbers] tweak values	[selection: 256 bits, 512 bits]	ISO 18033-3 (AES) [selection: IEEE 1619, NIST SP800-38E] (XTS)
UDE5	Camellia in CBC mode with non-repeating and unpredictable IVs	[selection: 128 bits, 256 bits]	ISO 18033-3 (Camellia) ISO 10116 (CBC)
UDE6	Camellia in CCM mode with unpredictable, non-repeating nonce, minimum size of 64 bits	[selection: 128 bits, 256 bits]	ISO 18033-3 (Camellia) ISO 19772, sec. 8 (CCM) SP800-38C
UDE7	Camellia in GCM mode with non-repeating IVs the IV length must be equal to 96 bits; the deterministic IV construction method [SP800-38D, Section 8.2.1] must be used; the MAC length t must be one of the values 96, 104, 112, 120, and 128 bits.	[selection: 128 bits, 256 bits]	ISO 18033-3 (Camellia) ISO 19772, sec.11 (GCM) NIST SP800-38D
UDE8	Camellia in XTS mode with unique [selection: consecutive non-negative integers starting at an arbitrary non-negative integer, data unit sequence numbers] tweak values	[selection: 256 bits, 512 bits]	ISO 18033-3 (Camellia) [selection: IEEE 1619, SP800-38E] (XTS)

Next Steps

- Expand set of SFRs for general use in cPPs/iTCs
  - Deliverables:
    - Cryptographic Definitions
    - Specification of Security Functional Requirements for Cryptography
    - Evaluation methodology of Cryptographic Functional Requirements

- Further engage CCUF Crypto WG
  - Protocol specification?
  - Maintenance of SFR and EA documentation?

Questions or concerns? Contact

zertifizierung@bsi.bund.de
niap@niap-ccevs.org