CCDB Crypto Working Group

Presentation of Crypto SFR Catalogue

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

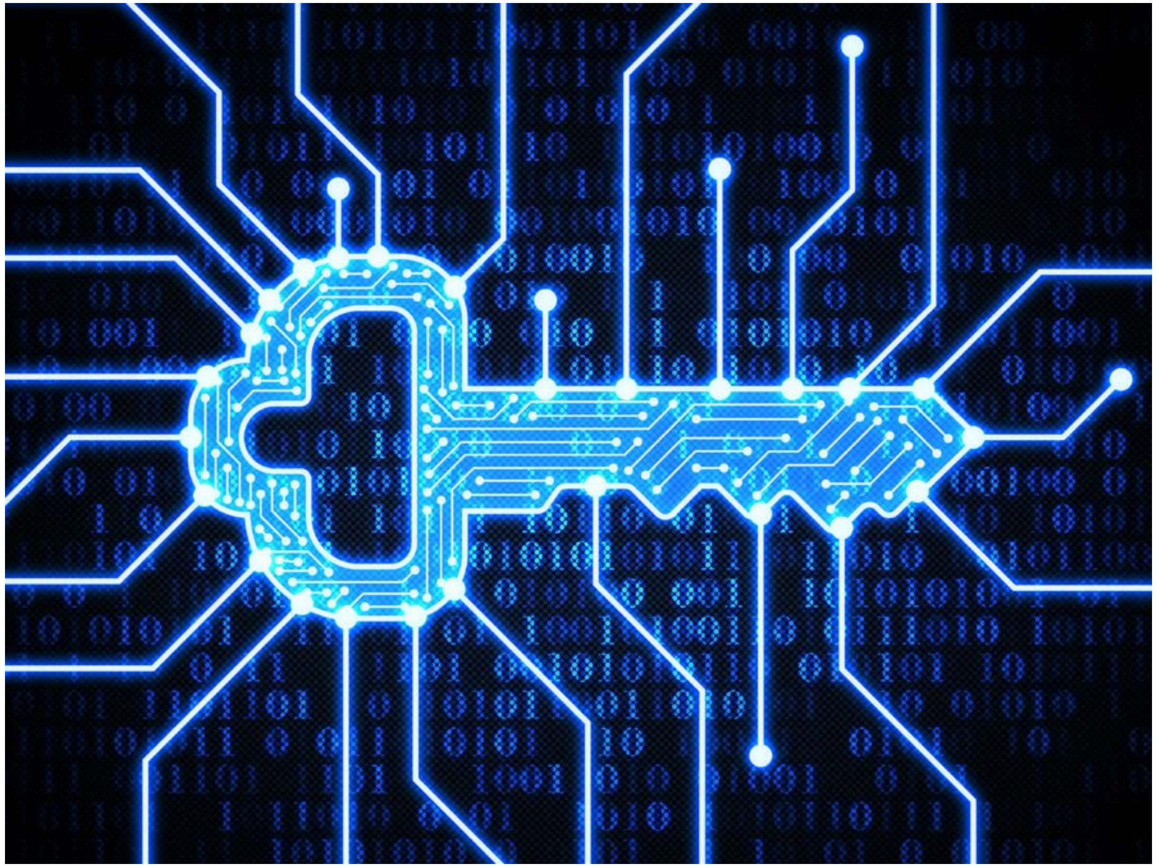
Federal Office
for Information Security

Agenda

- Who are we

- Crypto SFR catalogue

- Next steps and future plans



Federal Office
for Information Security

N I A P®

Who are we

- **CCDB Crypto Working Group**
  - Tasked by the CCDB to harmonize the specification and evaluation of crypto mechanisms in collaborative Protection Profiles (cPPs) and product evaluations within CCRA
  - Chaired by BSI, Germany and NIAP, US
  - Further active members: FMV/CSEC, Sweden

Major Achievements

- Definition of new crypto SFRs and their introduction to CC:2022
  - FCS_CKM.5, FCS_RBG.1/.2/.3/.4/.5/.6, FTP_PRO.1/.2/.3

- Delivery of a tailored set of crypto SFRs and corresponding evaluation methodology for the USB cPP and corresponding SD

Catalogue overview – 1 of 3

- FCS_CKM.1/AKG and /SKG – Cryptographic Key Generation
- FCS_CKM.2 – Cryptographic Key Distribution
- FCS_CKM_EXT.3 – Cryptographic Key Access
- FCS_CKM.5 – Cryptographic Key Derivation
- FCS_CKM.6 – Timing and Event of Cryptographic Key Destruction
- FCS_CKM_EXT.7 – Cryptographic Key Agreement
- FCS_CKM_EXT.8 – Password-based Key Derivation

Catalogue overview – 2 of 3

- FCS_COP.1/SKC – Cryptographic Operation (Symm Key Crypto)
- FCS_COP.1/Hash – Cryptographic Operation (Hashing)
- FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash)
- FCS_COP.1/CMAC – Cryptographic Operation (CMAC)
- FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation)
- FCS_COP.1/SigVer – Cryptographic Operation (Signature Verification)
- FCS_COP.1/KeyEncap – Cryptographic Operation (Key Encapsulation)
- FCS_COP.1/KeyWrap – Cryptographic Operation (Key Wrapping)

Catalogue overview – 3 of 3

- FCS_ETC_EXT.1 – Export of Key
- FCS_ITC_EXT.1 – Import of Key
- FCS_KYC_EXT.1 – Cryptographic Key Chaining
- FCS_OTV_EXT.1 – One-Time Value
- FCS_RGB.1 to FCS_RBG.6 – Random Bit Generation

Example 1: FCS_CKM.2 – Cryptographic Key Distribution

FCS_CKM.2.1
The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **[selection: key encapsulation, key wrapping, encrypted channels]** that meets the following: **[none]**.

Application Note:
If key encapsulation is chosen, then FCS_COP.1/KeyEncap SHALL be included.
If key wrapping is chosen, then FCS_COP.1/KeyWrap SHALL be included.
If encrypted channels is chosen, then FTP_PRO.1 SHALL be included.

Guidance:
Key distribution (or key transport) is a key establishment scheme in which one party creates a key and sends it to another party.

Example 2: FCS_COP.1/SKC Cryptographic Operation – Symmetric-Key Cryptography

FCS_COP.1.1/SKC
The TSF shall perform **symmetric-key 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]**.

Identifier	Cryptographic Algorithm	Cryptographic Key Sizes	List of Standards
AES-CBC	AES in CBC mode with non-repeating and unpredictable IVs	[selection: 128 bits, 192 bits, 256 bits]	[selection: ISO/IEC 18033-3 (Sub Clause 5.2), FIPS PUB 197] [AES] [selection: ISO/IEC 10116:2017 (Clause 7), NIST SP 800-38A] [CBC]

Examples 3: FCS_CKM_EXT.8 – Password-Based Key Derivation

FCS_CKM_EXT.8.1
The TSF shall perform **password-based key derivation functions** in accordance with a specified cryptographic algorithm **[HMAC-[selection: SHA-256, SHA-384, SHA-512]]**, with iteration count of **[assignment: number of iterations]** using a randomly generated salt of length **[assignment: length of salt]** and output cryptographic key sizes **[selection: 128, 192, 256]** bits that meet the following standard: **[NIST SP 800-132 Section 5.3 (PBKDF2)]**.

How to use the catalogue

- **Intention of the catalogue**
  - Supporting Document Guidance, i.e. not mandatory
  - Filled out operations (partly in tables) propose well known algorithms with key length and standards
  - Not a closed list – cPPs/PPs/STs can have more or other rows
  - Catalogue serves as a model for a harmonized presentation of SFRs
  - If you deviate from the catalogue, talk to your scheme in advance

How to use the catalogue

- **How to use the tables**
  - Copy and paste the rows that you want
  - Copy only complete rows
  - Do not only reference to the catalogue

- **Operations from CC:2022 are changed from assignments to selections**

Next steps

- Received 10 sets of comments (more that 250 comments) from different organizations (schemes, iTCs, labs, developers, standardization organizations) during public review of the draft catalogue
- Finalize review of comments and provide response
- Publish the revised catalogue after CCDB approval in spring 2024

Future Plans

- Develop evaluation methodology for the SFRs from the catalogue
- Extend the catalogue, e.g. with filled out operations for FTP_PRO
- Post-quantum cryptography

Contact

- Referat-sz22@bsi.bund.de

- NIAP@niap-ccevs.org

Thank you for the attention!

Any questions?

Federal Office
for Information Security