

“Assembling Crypto Pieces in the Common Criteria Jigsaw Puzzle”

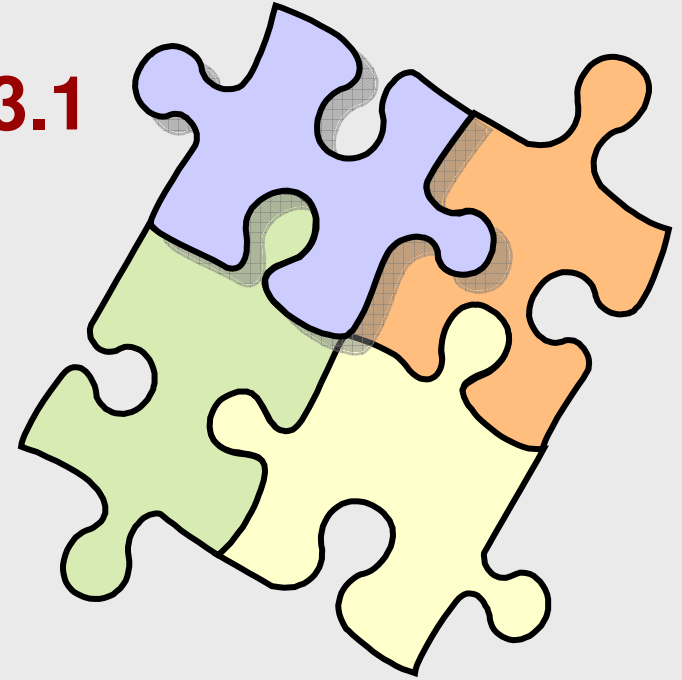


September 2010

Table of Contents

1) Crypto issues in current CC v3.1

- Crypto out of scope in CC?
- National crypto policies
- Using crypto standards in CC
- FCS: crypto support in SFRs



2) Extending the Depth of Crypto in CC

- a) Integration with “ISO-FIPS”
- b) Harmonizing the crypto penetration testing



“Crypto out of scope in CC” ?

CC v3.1 - Part 1

1 Introduction

“Certain topics, because they involve specialised techniques or because they are somewhat ~~peripheral to IT security~~, are considered to be outside the scope of the CC. Some of these are identified below. “

...

“f) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. Should independent assessment of mathematical properties of cryptography be required, the evaluation scheme under which the CC is applied must make provision for such assessments. “



“Crypto out of scope in CC” ?

Back to the former days of CC, origins

1970's (30-40 years ago!) → Orange Book & other DoD COMPUSEC standards

Layered approach for rating the strength of COMPUSEC features → *SEI-CMM*
(Software Engineering Institute – Capability Maturity Model, CMU)

Out of scope (CC P1 Intro): robustness of crypto algorithms ("acceptable" algorithms?)

“Cryptographic Strenght” → "traditional" definitions...

- a) In terms of **algorithm**: the characteristic of a crypto system to be free of mathematical weaknesses in its design
- b) In terms of **decryption keys**: their capability of having a high variability in order to resist brute force (direct) attacks – metrics? Key sizes



“Crypto out of scope in CC” ?

- CC **DOES NOT** perform mathematical crypto-analysis of the crypto algorithm design neither specifies lists of approved crypto algorithms/key sizes
 - *mathematical crypto-analysis* → high resources
 - *experts* → mathematicians vs. engineers
 - *local NSAs* → ad hoc guidance/directives
- CC **DOES** perform vulnerability analysis and penetration testing *including* the security functionality with crypto mechanisms

CC VA and penetration testing must include attacks to crypto mechanisms (limited by *EAL*) like *bypass, tamper, misuse, direct attacks (excluding crypto strenght!), or monitoring (analysing side channels, etc)*

Error! : to directly exclude some functionality in the vulnerability analysis due it contains crypto mechanisms



National Crypto Policies and CC certifications

Certification/validation aspects are **out** of CC/CEM standards

But the criteria to accept a certification requests from vendors used to *involve the crypto aspects specified in the ST (+PPs)* that it is provided with the application to the National Scheme

Basically to approaches in Schemes worldwide:

- a) To have a National policy with lists of “approved” crypto algorithms/ key sizes, directly reject STs with references to algorithms not included in such a list
- b) Independently of the National crypto policies, to accept the application and analyze during the evaluation if the crypto specification is ok or not to achieve the security objectives of the TOE (*considering the crypto mechanisms as part of more complex security functions, and considering the specific SPD of the ST, the EAL level, etc*)

Using Crypto Standards in CC v3.1

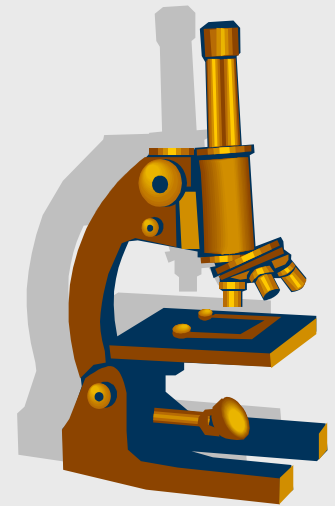
CC v3.1 Part 1 - Annex A “Specification of Security Targets”

A.13 “Referring to other standards in a ST” - E.g. crypto standards

- a) Crypto standard included in an OSP
- b) Crypto standard included in a SFR
- c) Crypto standard included in the TSS

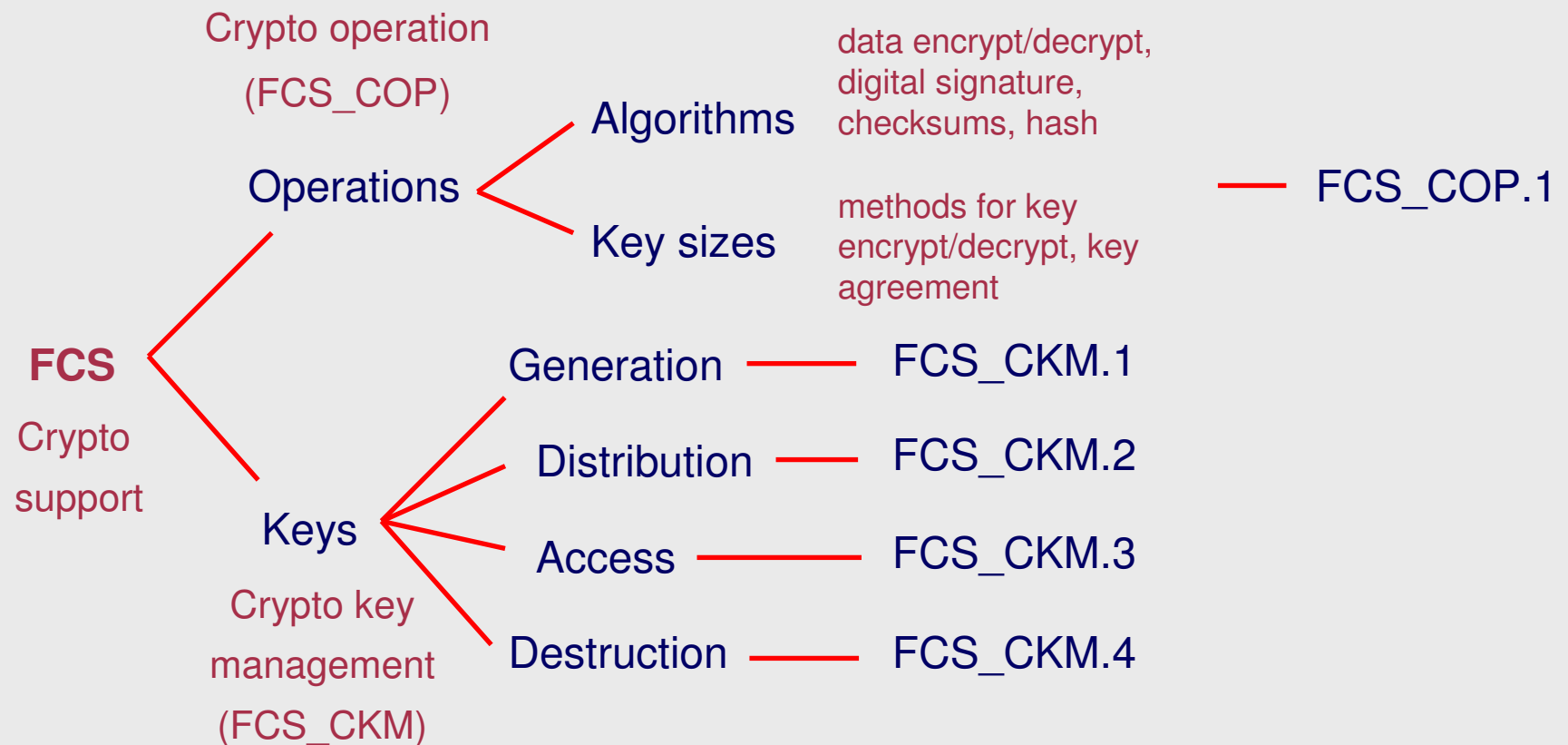
ADV_INT (TSF internals) → it requires a complexity analysis where developer must provide information related to demonstrate the use of standards in the development process.

Note → same concepts are included in the annex for Protection Profiles (without the TSS part of course)



FCS Class (Cryptographic support)

→ Cryptographic Security Functional Requirements related to the cryptographic algorithms and keys used by the TSF



+Minimal and basic set of actions to be audited with FAU_GEN

Extending the Depth of Crypto in CC



Integration with “ISO-FIPS”

- ➡ FIPS PUB → “Federal Information Processing Standards Publication”
→ NIST (National Institute of Standards and Technology) → USA & CAN
- ➡ Crypto → *FIPS PUB 140-2* “Security Requirements for Cryptographic Modules”
“Best practices” requirements for CMs organized in 4 SLs
US Federal Governmental systems → non-classified info
- ➡ Include sections for: design, implementation, roles, services, authentication, FSM, physical security, operational environment, key management, EMI/EMC, self-test, and mitigation of other attacks.
- ➡ CMVP (Cryptographic Module Validation Program) → CM validation vs. FIPS 140-2 → NIST + CSE (Communications Security Establishment).
- ➡ NVLAP → CMVP is based on labs from the National Voluntary Laboratory Accreditation Program (NVLAP).
- ➡ FIPS PUB 140-3 → ongoing, focused on CM pen testing e.g. DPA with SASEBO

Extending the Depth of Crypto in CC



Integration with “ISO-FIPS”

⇒ Parallelism... CC/CEM → criteria/method
...FIPS 140-2 → ISO 19790 (criteria) + ISO 24759 (method)

⇒ “ISO-FIPS” → compliance/conformity functional testing
→ Mixing SFRs and SARs

SFRs at...

- CC → P2 SFRs are a tool/help (catalog to be used) for developers → PPs are related to national scheme certification policies or industry forums
- ISO-FIPS → prescribes SFRs like a mandatory PP for developers

Extending the Depth of Crypto in CC



Integration with "ISO-FIPS"

Gross point estimation on the main relations between "ISO-FIPS" and CC v3.1



Extending the Depth of Crypto in CC



Integration with “ISO-FIPS”

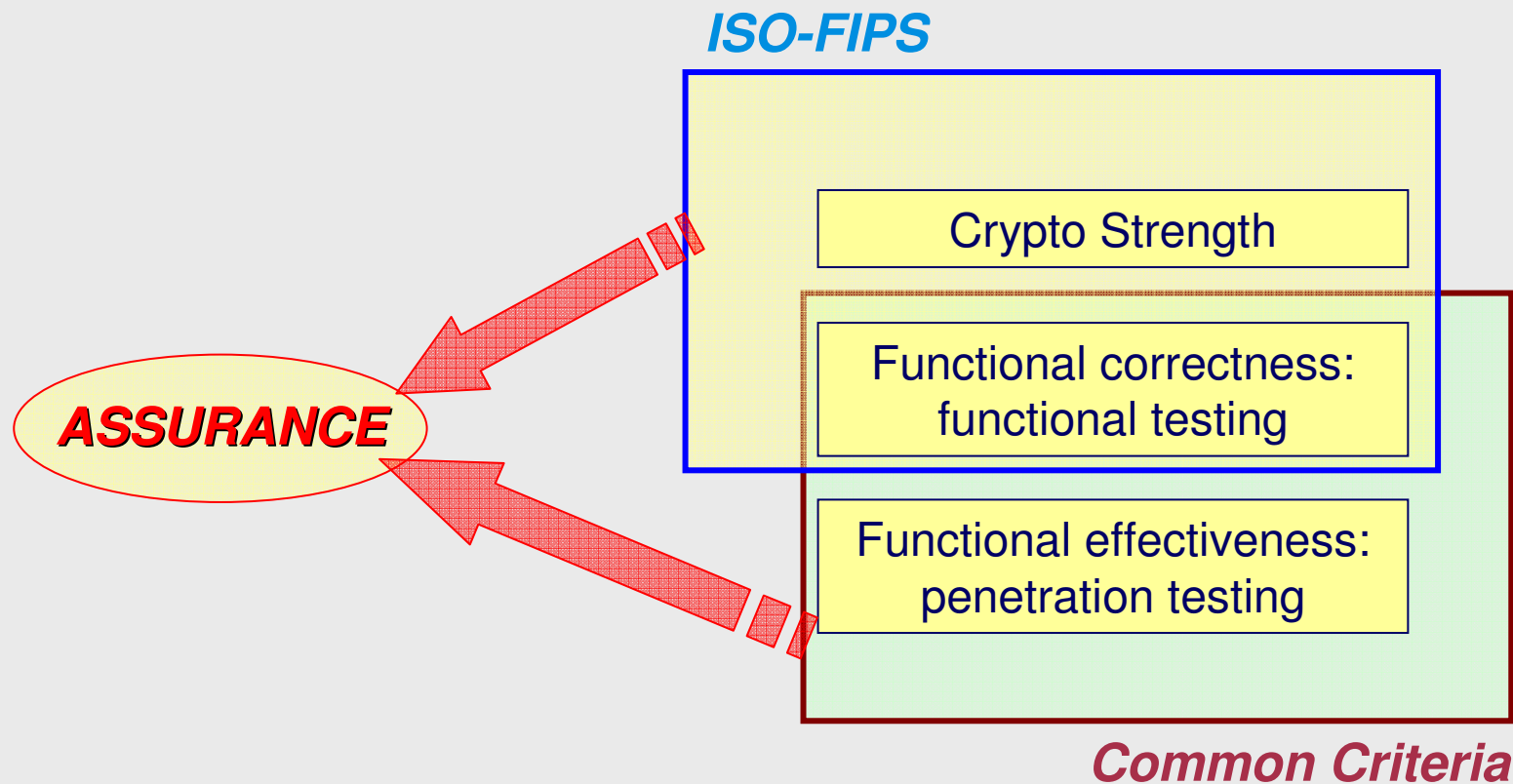
- ➡ ISO-FIPS Focus: the robustness of the data encrypted by the TOE, not in the robustness of the TOE itself
- ➡ CC → evaluates functional **correctness** (with sampling) but also the **effectiveness** of TSF for the security objectives of the TOE
- ➡ CC includes **penetration testing** (AVA) in addition to functional testing (ATE)
- ➡ ISO-FIPS → covers *crypto strength* due it uses **lists of approved algorithms** and key sizes originally based on the lists created by US NIST
- ➡ ISO-FIPS **certificate** → input for objectives sufficiency rationale at CC Security Target (ST)

Extending the Depth of Crypto in CC



Integration with “ISO-FIPS”

Simplifying the view for the assurance consumer...



Extending the Depth of Crypto in CC



Improving the crypto work with the CCRA framework

Scheme Proposals or ideas

(1) Integration with “ISO-FIPS” → general target: reduce evaluation overhead due overlapping

- Guidance → developers using ISO-FIPS certificates in ST rationales
- PPs+ISO-FIPS SFRs specific technologies → CCRA certified in the form, outside policies
- Guidance for ISO-FIPS labs → “detailed ETR” evidence input for CC “sampling principle”
→ structured based on the overlapping points between ISO-FIPS and the CC SFRs/SARs
- Supporting docs for new SARs (if necessary) → *maybe out CCRA?*

(2) Harmonizing the crypto penetration testing → general target: consolidate and improve the technical competence

- Define subject areas → base for supporting docs in “key” crypto areas
- Provide taxonomies/guidance on *attack methods* → Technical Communities → *Research!*



General Taxonomy: Attack Methods for Crypto Mechanisms

Symmetric Key attacks

- Brute force attacks
- Inspection attacks against the Electronic Codebook mode of use of block ciphers
- Differential cryptanalysis attacks
- Related-key attack against AES
- Linear cryptanalysis attack to block ciphers
- Attack against TDES



Note: initial coverage based on SP scheme experience with commercial products



General Taxonomy: Attack Methods for Crypto Mechanisms

Asymmetric Key attacks

→ RSA Cryptosystem

- Attacks to factoring
- Attack to small encryption exponent e
- Attack to small decryption exponent d
- Message concealing Attack
- Cyclic Attacks

→ Elliptic Curve Cryptosystem

- Brute-force attack
- Pohlig-Hellman attack
- Frey-Rück/MOV attack
- Anomalous attack
- Weil descent attack
- Benign malleability attack
- Small subgroup attack
- Malleability attack when using the XOR function



Harmonizing the crypto penetration testing



General Taxonomy: Attack Methods for Crypto Mechanisms

Digital Signature attacks

→ Attacks on DSA

- Exhaustive search attack
- Baby-step, giant-step
- Pollard's rho attack to DLP
- Pohlig-Hellman attack
- Index-calculus and Number Field Sieve attacks
- Attacks to repeated per-message key k
- Restart attack

→ Attack against the partially known nonces

→ Attacks on ECDSA

- Repeated ephemeral keys attack
- Heuristic lattice attack



Harmonizing the crypto penetration testing



General Taxonomy: Attack Methods for Crypto Mechanisms

Hash Function attacks

- Brute-force Attack
- Collision Attack
- Pre-image Attack



Random Number Generators attacks

- True Random Number Generators
- Pseudo Random Number Generators
- General requirements that must meet all random number generators
- Distinguishing attack
- Cryptanalytic attacks on PRNGs

Harmonizing the crypto penetration testing

General Taxonomy: Attack Methods for Crypto Mechanisms

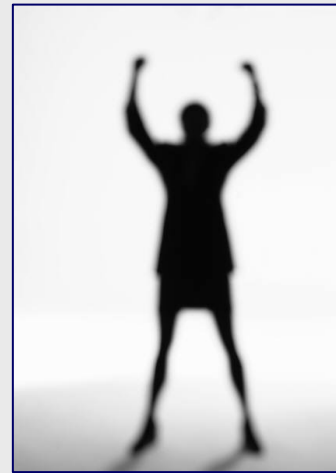
Prime Number Generators

- Prime generation
- Primality detection
- Primality proving algorithms
 - Algorithm AKS and follow-ups
 - Lucas-Lehmer primality test
 - Pocklington-Lehmer primality test
 - Jacobi sum test
 - Elliptic-curve primality test
- Probabilistic primality tests
 - Fermat's test
 - Solovay-Strassen test
 - Miller-Rabin test
- Generation of probable primes
 - Maurer's algorithm
 - Random search with Miller-Rabin algorithm



Summary

- **Current points related to Crypto in CC v3.1**
...*"Crypto outside CC scope"* ??
- **Integration alternatives: CC and FIPS or ISO**
- **Harmonizing the Crypto Penetration Testing with Attack Taxonomies**



Thank you by your attention
Questions?

<http://www.oc.ccn.cni.es>
organismo.certificacion@cni.es

