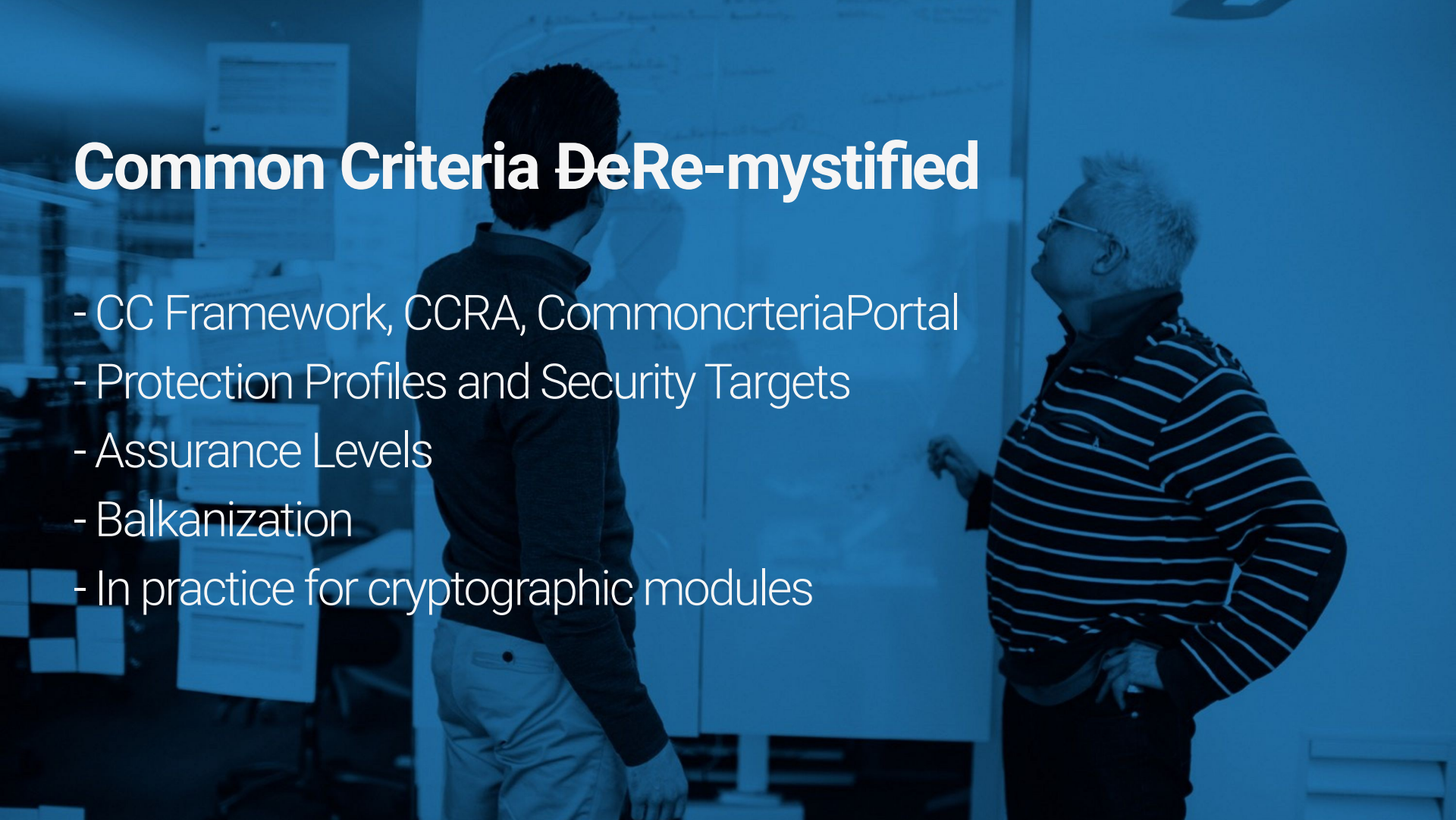


Common Criteria ~~De~~Re-mystified

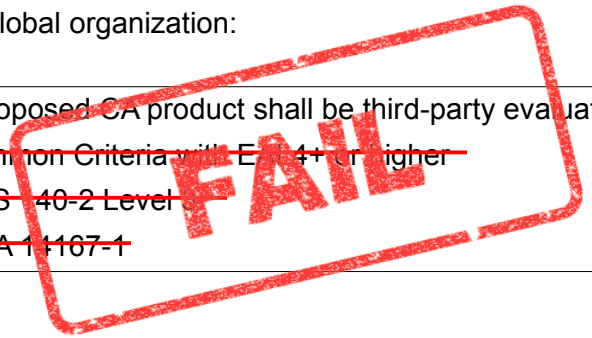
- CC Framework, CCRA, CommoncrteriaPortal
- Protection Profiles and Security Targets
- Assurance Levels
- Balkanization
- In practice for cryptographic modules

What can go wrong?

RFQ from a large global organization:

The proposed CA product shall be third-party evaluated by any of following:

- ~~Common Criteria with EAL 4+ or higher~~
- ~~FIPS 140-2 Level 3~~
- ~~CWA 14167-1~~



What can be wrong with this?

1) There is no Common Criteria Protection Profile for CAs with EAL level 4+ or higher that can be used (under the Swedish scheme at least).
2) FIPS 140-2 is a certification for cryptographic modules, not for CA products
3) CWA 14167-1 was an audit standard, not a product certificaton, and was withdrawn 2016, superseded by ETSI eIDAS audits

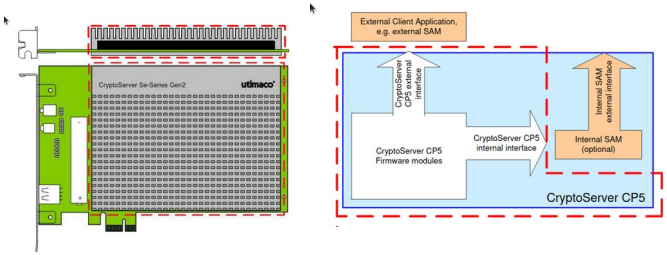
Common Criteria

ISO/IEC 15408

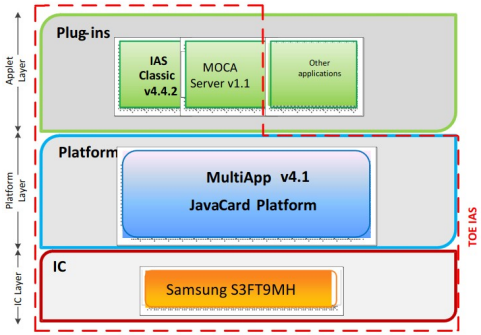
- Common Criteria for Information Technology Security Evaluation
  - Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) in a Security Target (ST)
  - Products evaluated by independent licensed laboratories to determine the fulfilment of security properties, to a certain extent or assurance
  - Current CC v3.1
- Common Criteria Recognition Arrangement (CCRA)
  - The *CCRA* allows vendors of a certified products (a product which has been evaluated, in a given country by a given laboratory, and certified to be conformant to some set of SFR's and SAR's) to be recognized in all CCRA nations
- https://www.commoncriteriaportal.org/
  - All issued (and archived) CC certificates and Security Targets for download

Security Target and Protection Profiles

- Security Target
  - TOE: Target of Evaluation
  - Claims conformance to PP
- Protection Profile
  - a document, created by a user community, which identifies security requirements for a class of security devices (for example, smart cards or network firewalls) relevant to that user for a particular purpose.
  - Certification without a Protection Profile is pretty much useless



Utimaco CP5 / EN 419 221-5



eToken 5110 CC / IDPrime 940CC / IAS classic 4.4.2 on MultiApp 4.0.1 EN 419 211-2, etc

Assurance levels

- EAL (Evaluation Assurance Level)
  - EAL 1-6
    - SAR's "level of effort" (Security Assurance Requirement)
  - Adequacy of a product to a given field/function is contained in the PP's SFR's, not by the (optional) SAR's
- non-EAL
  - cPP (NIAP)
  - a cPP does not usually specify an EAL, because cPP's focus on adequate SFR's (Security Functional Requirements) for a given product/technology. "fit for purpose"
  - uses so-called "extended components" of the CC, with added assurance activities that augment the assurance requirements beyond those of EAL1
- EU Cyber Security Act
  - Basic, Substantial, High
  - commensurate with the level of the risk associated with the intended use of the product, service or process

Balkanization of Common Criteria

- Usually refers to different requirements of certifications in different areas
  - CCRA ensures certificates are recognized everywhere
  - But authorities and countries can require their own PPs
  - Best example SOG-IS in EU and NIAP in US
    - NIAP approved protection profile required for use in Federal Gov
    - SOG-IS approved protection profile required for use in EU Gov
    - Different approaches – no consistency with regards to PPs
      - especially true before EU Cybersecurity Act
  - Forces vendors to do multiple, time consuming and expensive certifications

Writing Requirements?

- Strong recommendation to specify Protection Profile
  - Without specifying PP it’s not possible to compare between products
    - One certification with testing of random number generator, the other one without?
- Technical specifications
  - eIDAS
    - EN 419 221-5 / EN 419 211-2 / ...
  - Other, mostly FIPS 140-2 L2 or L3
- Public Procurement
  - References eIDAS / EN 419 221-5
  - ...or just Common Criteria…
  - ...or FIPS…
- Audits

What’s practical?

- Currently available cryptographic modules
  - HSMs
    - FIPS 140-2 Level 2/3 (and FIPS 140-3 Level 2/3)
    - EN 419 221-5
  - Smart cards/USB tokens/TPMs
    - FIPS 140-2 Level 2/3 (and FIPS 140-3 Level 2/3)
    - CC: PC Client Specific TPM 2.0 Protection Profile
    - CC: EN 419 211-2/ and -3 (Secure signature creation device)
    - CC: Security IC Platform Protection Profile
    - CC: Java Card Protection Profile - Open Configuration

What is the CSCWG purpose of the cryptographic module?

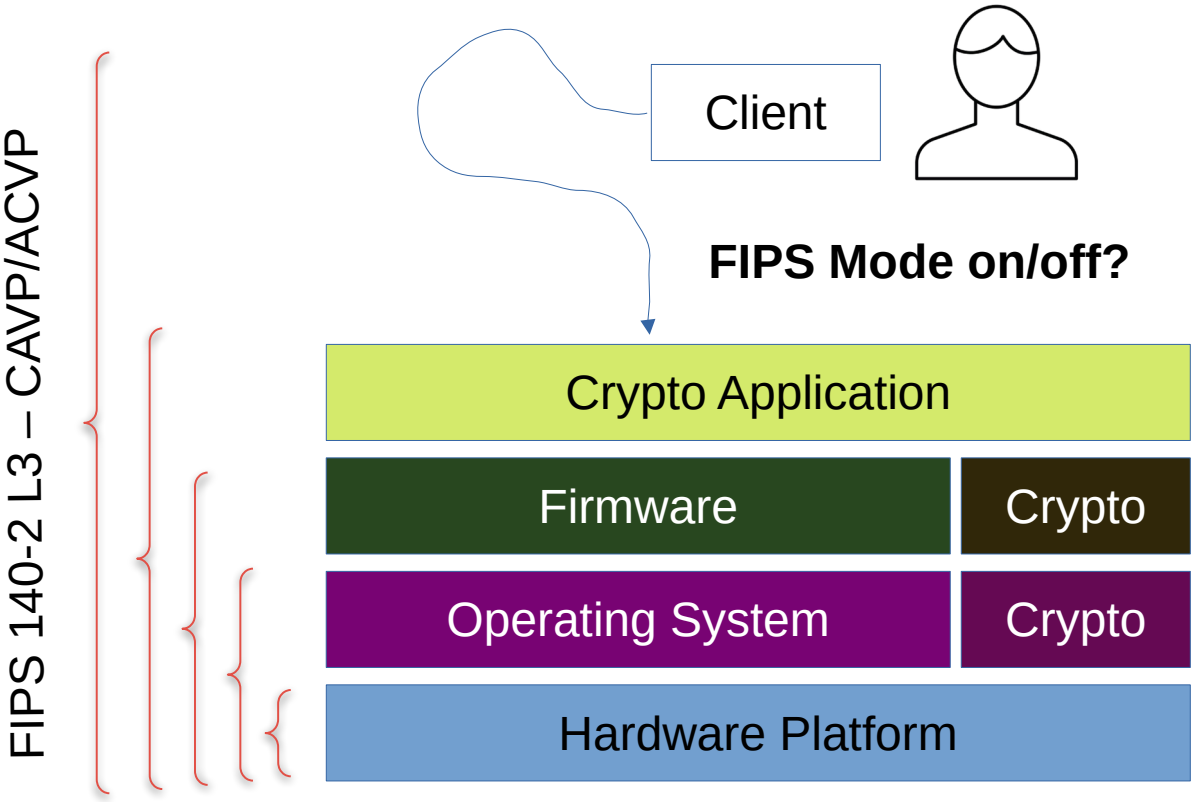
“*FIPS ... or Common Criteria*” would target all of the above. Unlikely to find/allow any shady home-grown certifications...but HW/SW/Client…key generation?

Confused yet?

Users typically do not use Common Criteria in the way anticipated by the CCRA…

- Broad/invalid requirements
- Vendor lock-out and lock-in (single-vendor)
- “Certified version” (with known security vulnerabilities)
- Audit inconsistencies (one auditor approves something another auditor would not)
- Usability
- Cost
- ...

How about FIPS?



Mixing FIPS requirements, with other requirements, not specifying enough in detail →

- Single-vendor
- Audit inconsistencies
- …

FIPS mode on/off?

- You may not want/be able to limit algorithms, curves and key sizes
- Auditor mileage may vary