Upcoming Changes to ISO/IEC 19790

Communications
Security Establishment

Centre de la sécurité
des télécommunications

Canada

ISO/IEC 19790 – Security Requirements for Cryptographic modules

Scope

“This International Standard specifies the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems. This International Standard defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g. low value administrative data, million dollar funds transfers, life protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location).”

ISO/IEC 19790:2012 Corr 2015 currently being used by the CMVP as the basis for FIPS 140-3

Project timeline for ISO/IEC 19790 & 24759

Circulation of first WD (20.20):	January 2021
Circulation of second WD (20.20):	July 2021
Circulation of third WD (20.20):	January 2022
Circulation of fourth WD (20.20):	July 2022
Circulation of first CD (30.20):	December 2022

DIS ballot initiated (4.20)	November 26 2023
Close of voting (4.60)	February 18 2024
Final text received (50.00)	June 09 2024
Publication (60.60)	September - October 2024

Evolution vs Revolution

- Fix technical issues or issues of clarity
- Remove requirements that are redundant, out-of-date, or not useful to the overall security of the module
- Introduce new requirements that reflect changes in technology
- Backwards compatible*

Changes presented here are NOT final and are subject to change

Major updates

- Improvements to degraded mode and error state
- Introduction of secure containers
- Definition of “internal protected paths”
- Collapse of multi-chip embedded and multi-chip standalone
- Option to support device attestation
- Rework of SSP import/export section for clarity and allowances at level 3
- Allowance for vendors to define some SSPs to be exempt from zeroisation
- Zeroisation of public keys

Localised Error State and Degraded Operation

- Updates (7.2.4.3) made to the allow a ‘localized error state’ (all levels): After entering an error state, the module may then enter degraded operation that is localized to a subset of the module functionality:
  - degraded operation **shall [02.24]** be entered only after exiting an error state;
  - ….
  - the mechanism or process that failed **shall [02.26]** be isolated;
  - …

  The error state in [02.24] may either impact the full module or can be localized to the mechanism or process isolated in [02.26]. Where a localized error is used, it **shall [02.29]** be shown that the target error can’t impact other approved services running outside the isolated mechanism or process
- Data output inhibition may be restricted to the subset of the module functionality affected by the error state/degraded operation.

Improved options to exit degraded operations

degraded operation

operation where a subset of the entire set of security functions, services or processes are available and/or configurable as a result of reconfiguration from an error state

- More precise language has been added to describe how a module exits degraded mode.

  The cryptographic module **shall [02.30]** remain in degraded operation until such a time as the cryptographic module has repeated pre-operational test self-tests covering either the entire module or the failed isolated mechanisms and processes of the cryptographic module

- An allowance is added to define a subset of self-tests that need to be rerun to exit degraded mode

  Where pre-operational self-tests re-run ahead of exiting degraded operation only cover a sub-set of tests performed on power-on, it **shall [02.31]** be demonstrated why the excluded self-tests do not need to be re-run.

Introduction of secure containers

Concept of ‘secure containers’ added for modules (all levels) with a limited OE.

- Similar to excluded code except that it allows for conditional loading of additional non-module code without negating module validations.
- Code loaded into the secure container doesn’t require validation or examination by a lab, and can be removed, replaced or updated without impacting the module version; it is considered outside the module boundary.
- Interfaces to the secure container are treated like they are on the module boundary.

Protected internal path

“Interfaces between ICs within the cryptographic boundary in a multi-chip module using approved cryptographic methods to protect the confidentiality and integrity of the data”

- Allows for the absence of physical protection at any level
- At level 3 allows for absence of protective tamper-evident coating or strong enclosure
- At level 4 allows for absence of removal resistant or strong enclosure

Aligns the physical protection requirements between single chip and multiple-chip embodiments

Combination of multiple-chip embedded and standalone

Embodiments dropped down to simply ‘single-chip’ and ‘multiple-chip’

- Collapses ‘multi-chip embedded’ and ‘multi-chip standalone’ into single embodiment.
- Aim in the future to drop the historical concept of embodiments but not yet achieved.

Experience with the FIPS 140-2 and 140-3 found that vendors were often undecided which embodiment to choose, since many modules could be used either standalone or embedded in a larger product

Updates to SSP management – Import/Export

- Clarified allowance to permit software modules or the software component of a hybrid software module to export plaintext keys at Levels 1 and 2, provided they do not leave the OE.

- Level 3 now allows keys to be imported/exported:
  - Encrypted or
  - Over a plaintext trusted path (was trusted channel) or
  - Via split knowledge procedures

SSPs exempt from zeroisation

19790 has always has the concept of exempting some SSPs from zeroization, e.g. the key used for the integrity test. A new general allowance permits the vendor to define some keys as being exempt from zeroization, where their compromise does not directly compromise operator SSPs, user data or privacy.

- originally included to support the inclusion of Attestation services, which require a private key to be maintained throughout the lifecycle of a module
- Acknowledges that the lifecycle of a user using a module may be different to that of the module itself

Zeroisation of Public Keys

- New requirement to address privacy concerns

> “A module **shall [09.30]** provide methods to zeroise all plaintext CSPs, plaintext PSPs, and plaintext key components within the module.”

- Similarly, plaintext PSPs are to be zeroised during maintenance and in response to tamper

Support for attestation

Attestation has been added as an option at all levels in section 11:

Attestation: process used to allow an entity outside the boundary of the cryptographic module to securely verify the identity and other physical or logical characteristics of the cryptographic module using an attestation record, and conforming to attestation standards and methods listed in Annex G

Requirements are only applicable if attestation is claimed by the vendor. Testing involves following the Security Policy instructions to retrieve and verify records.

CMVP Transition decisions

- How will the CMVP adopt the next revision of 19790?
  - 140-3 vs 140-4
- When will the CMVP adopt the next revision of 19790?
  - Doesn't happen automatically when the update is published
- CMUF group proposed to study differences 2012 ->2024 so that IG's etc can be planned

Questions?