

CRYPTOGRAPHY AND THE COMMON CRITERIA IN CANADA

ICMC
May 2016

Cory Clark
Senior Certifier

© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.



WHAT IS COMMON CRITERIA?

Common Criteria (CC) is an international program amongst 25 nations in which IT products (Targets of Evaluation) are certified against standard specifications, such as Protection Profiles.

The results of this process are mutually recognized by all participating nations, minimizing the need for multiple evaluations of the same product.

The Communications Security Establishment (CSE) operates a product certification capability under this program referred to as the Canadian CC Scheme.



HOW IS CRYPTOGRAPHY USED IN COMMON CRITERIA?

The security functionality of evaluated products is defined in CC by *security functional requirements (SFRs)*.

SFRs are broken down into different classes, such as *FCS: Cryptographic Support*.

The class *FCS : Cryptographic Support* covers cryptography used in CC with the following SFRs:

- FCS_CKM.1 Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Distribution
- FCS_CKM.3 Cryptographic Key Access
- FCS_CKM.4 Cryptographic Key Destruction
- FCS_COP.1 Cryptographic Operation



The current Protection Profiles (PP) all have additional cryptographic SFRs which are more focused.

WHAT ARE THE CANADIAN COMMON CRITERIA SCHEME REQUIREMENTS?

- Only approved algorithms are to be used. The list approved algorithms aligns with the approved security functions in FIPS 140-2.

The Canadian Common Criteria Scheme has guidance for testing facilities, known as Instruction #4, that covers how cryptography is assessed:

- For products whose primary purpose is user data protection, a full Cryptographic Module Validation Program (CMVP) certification is required.
- For products whose primary purpose is **not** user data protection, but is used for secondary functions such as securing the management connection, a Cryptographic Algorithm Validation Program (CAVP) certification is required.
- For products claiming conformance to a Protection Profile (PP), only a CAVP certification is required.

CRYPTOGRAPHIC CERTIFICATION

The use of a **CMVP** certification provides assurance about the functionality of the cryptographic component and enforces a standardization of how the testing should be performed.

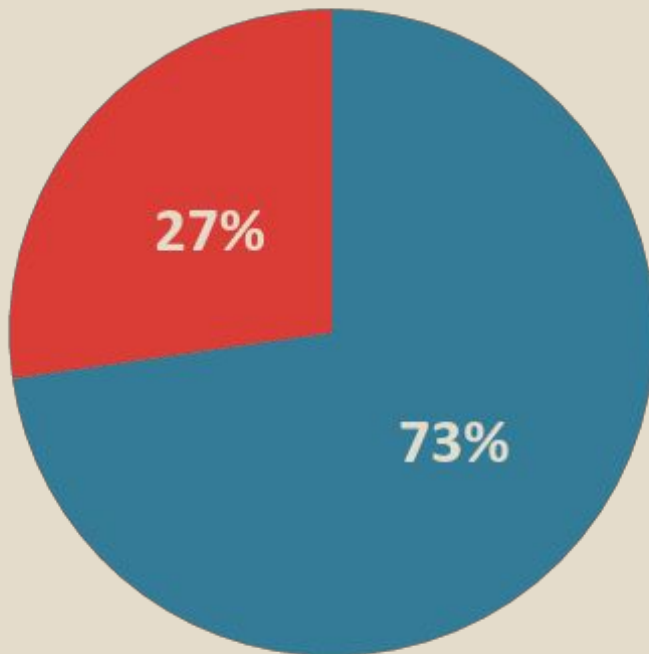
The use of a **CAVP** certification provides assurance that the cryptographic algorithms function properly, but doesn't cover any other functionality such as how a product would handle keys.

The current **Protection Profiles** have explicit testing requirements regarding cryptographic functionality, so a CMVP certification is not required, but CAVP certification is required to test the underlying algorithms.

USE OF CRYPTOGRAPHIC MODULES IN CC EVALUATIONS

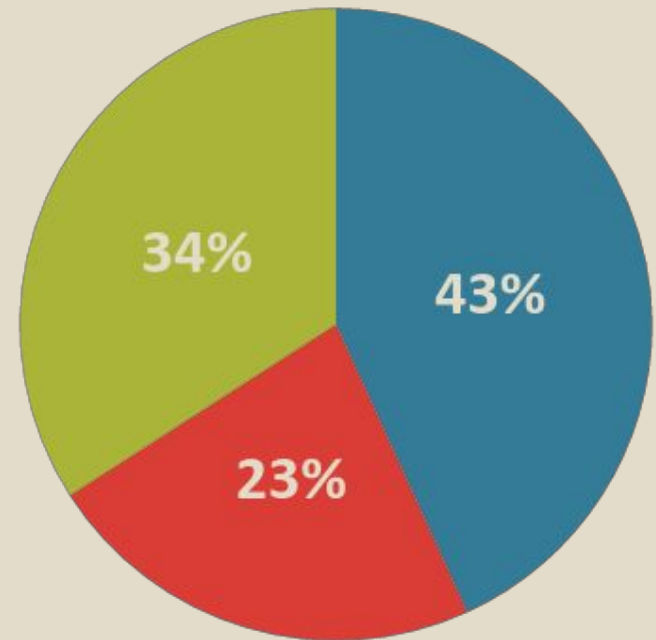
Use of Crypto

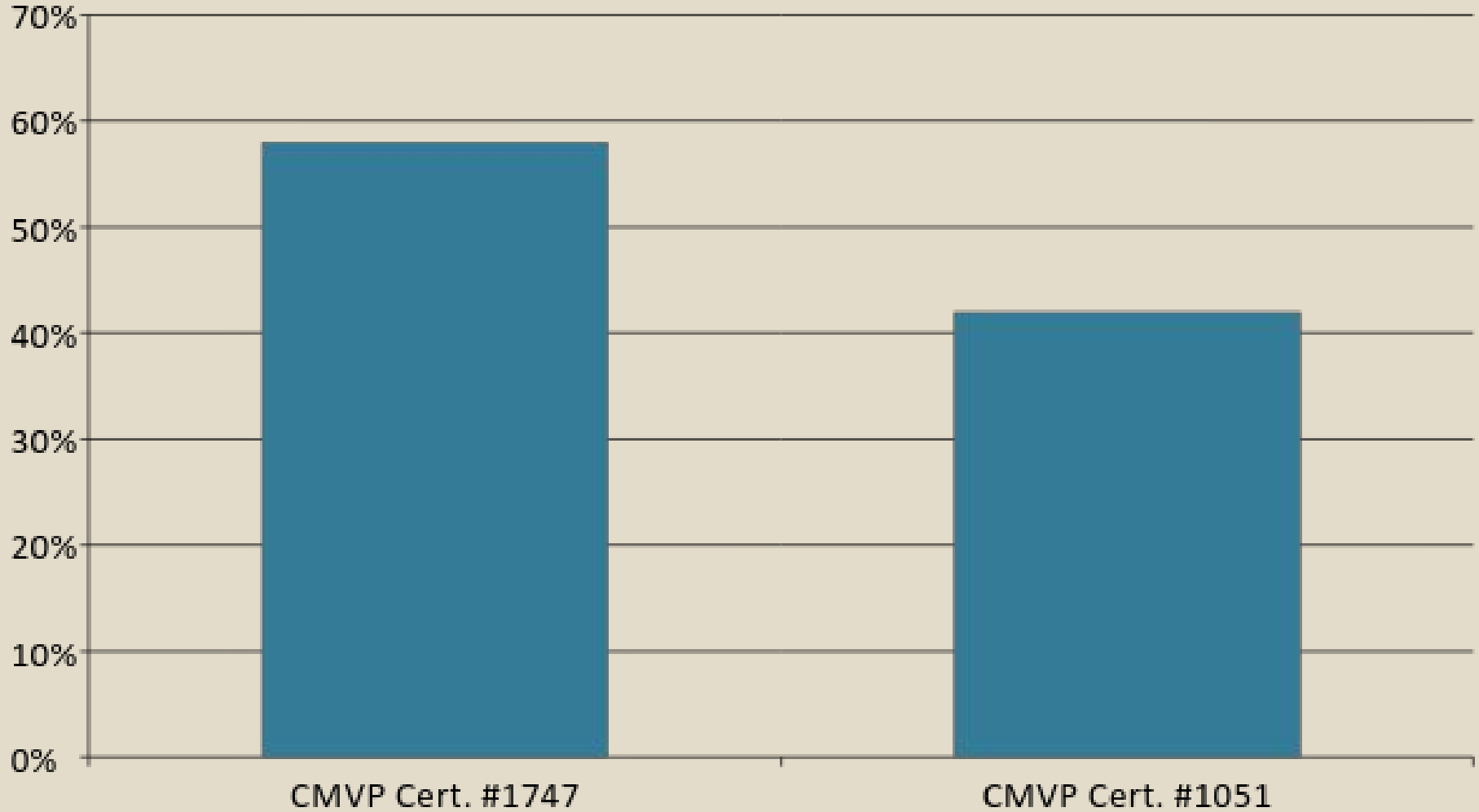
■ Yes ■ No

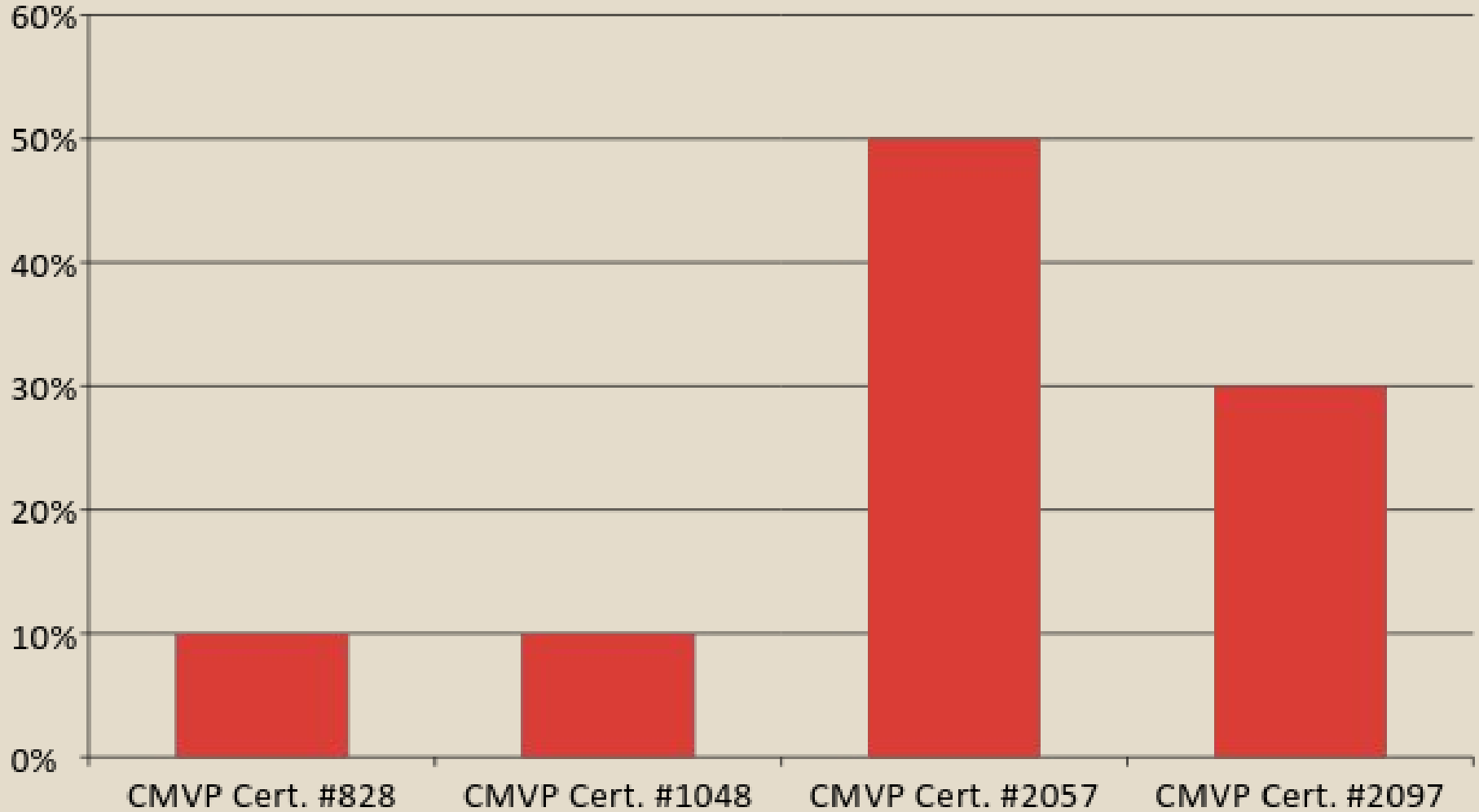


Modules

■ OpenSSL ■ RSA Bsafe ■ Other







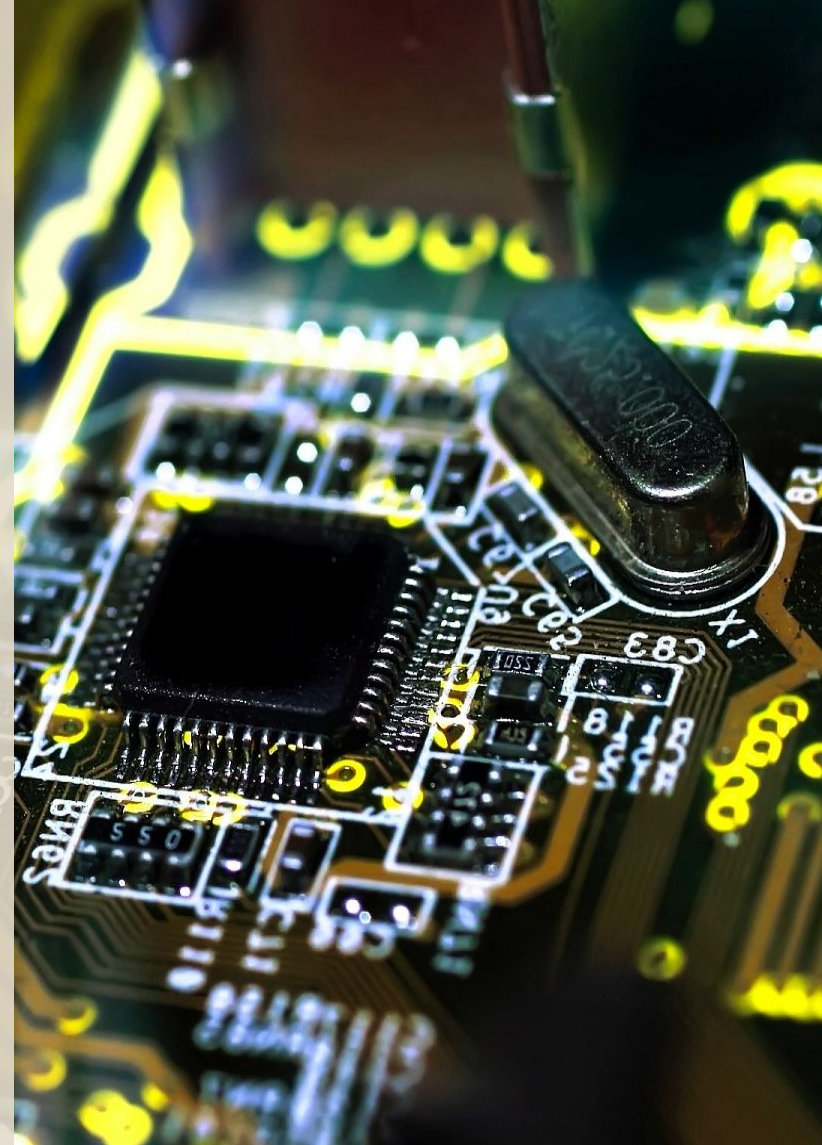
CURRENT CHALLENGES

- Module identification
- Vendor affirmation
- Non-conformant implementations
- Certification timelines
- Entropy assessments



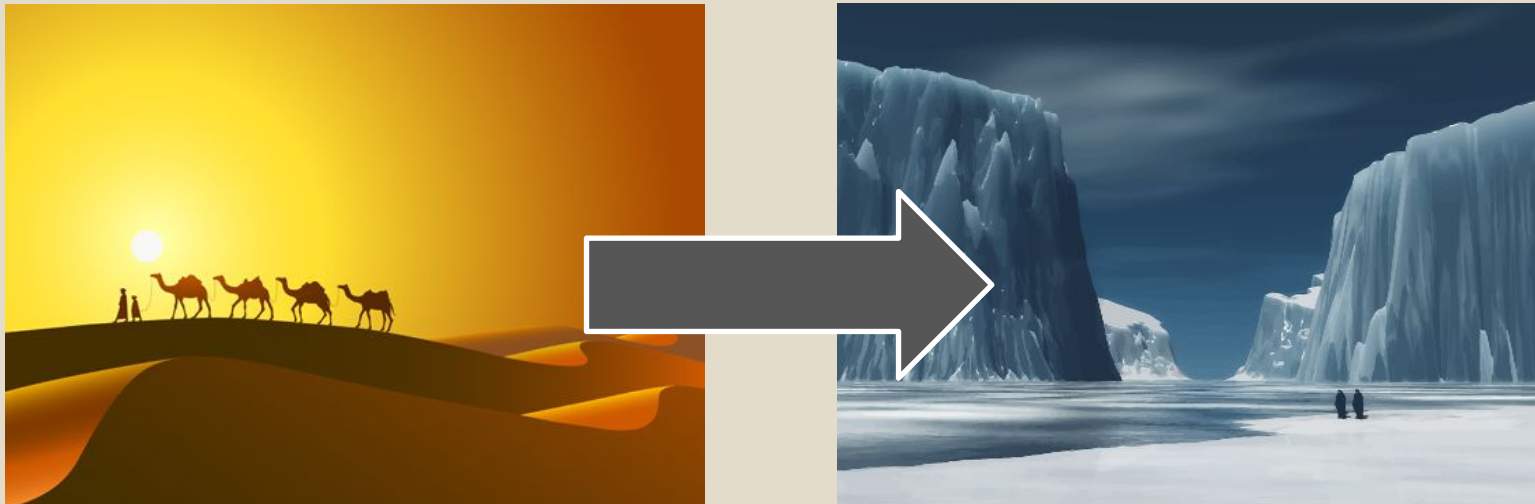
MODULE IDENTIFICATION

- ◆ Since the cryptographic module is often a component of the product vs. being the product itself, it can be challenging to independently identify it.
- ◆ A key component of module identification is determining the validity of the implementation.
 - What the module was tested on vs. what the CC evaluation is testing.



VENDOR AFFIRMATION

- Vendor Affirmation is used when “porting” a module.
- Refers to a validated module maintaining conformance in an operational environment not listed as part of the original evaluation.
- Applies to Software and Firmware modules.
- Specific rules about what is and is not allowed are located in FIPS IG.5.



NON-CONFORMANT IMPLEMENTATIONS

Several cryptographic modules have a “FIPS Mode” of operation, where requirements such as algorithm selection are implemented.

In some cases the product needs to be configured to enable FIPS Mode.

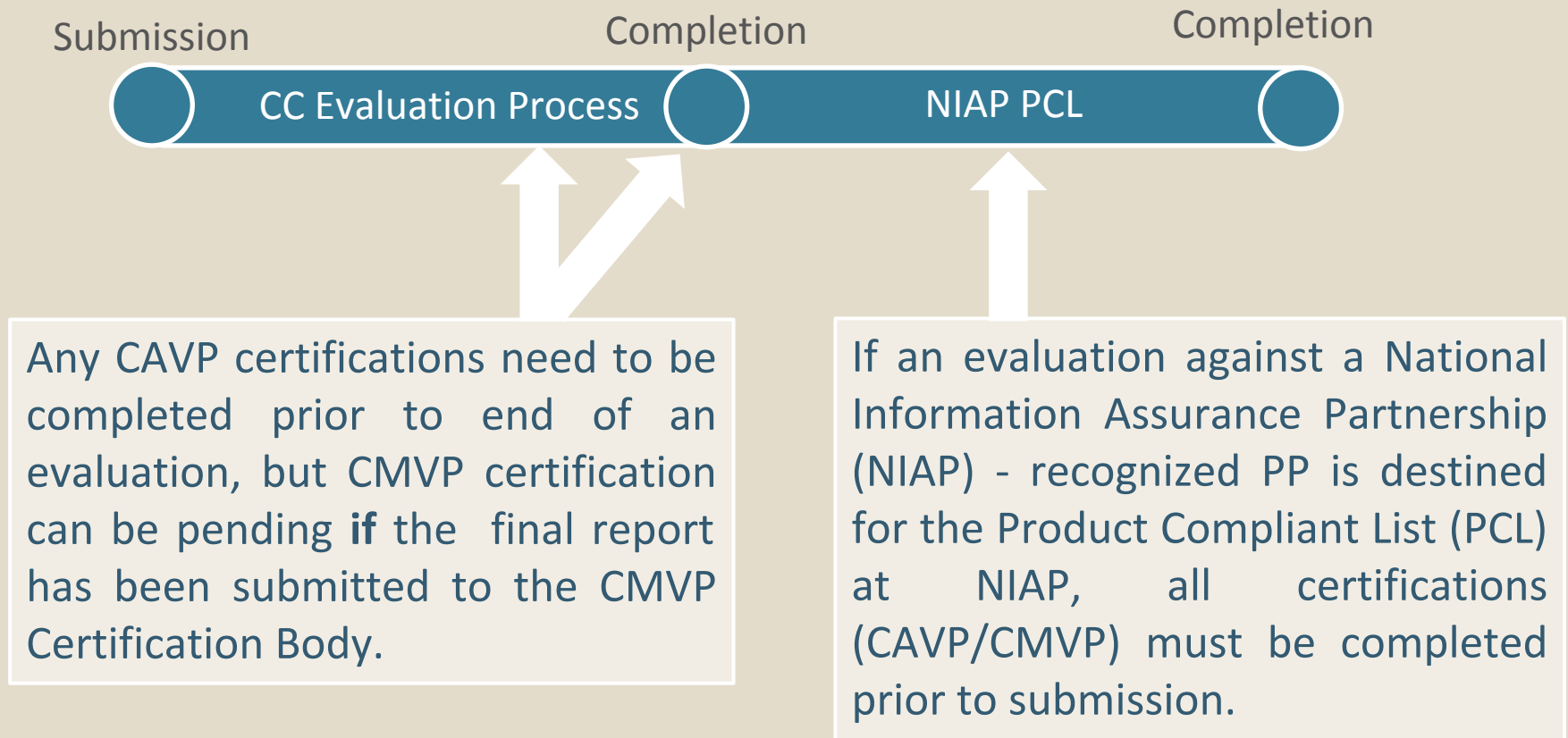


Important considerations:

- Ensure that FIPS Mode doesn't conflict with the CC evaluated configuration, is actually part of the installation guidance, and the product is tested in FIPS Mode.
- If the cryptographic module requires a particular mode of operation to be valid, then that must be how it is configured for the CC evaluation to be valid.

CERTIFICATION TIMELINES

As CMVP/CAVP certification is required for CC product evaluations that use cryptography, the CMVP/CAVP certification activities should be underway prior to the CC evaluation.



CERTIFICATION TIMELINE CHALLENGES

Challenges arise when the CMVP certifications are delayed or if the CMVP evaluation fails.

- Either due to the sponsor cancelling the evaluation; or
- Non-compliance found during the CMVP Certification Body testing.

This has resulted in CC evaluations being modified, or certificates being revoked.



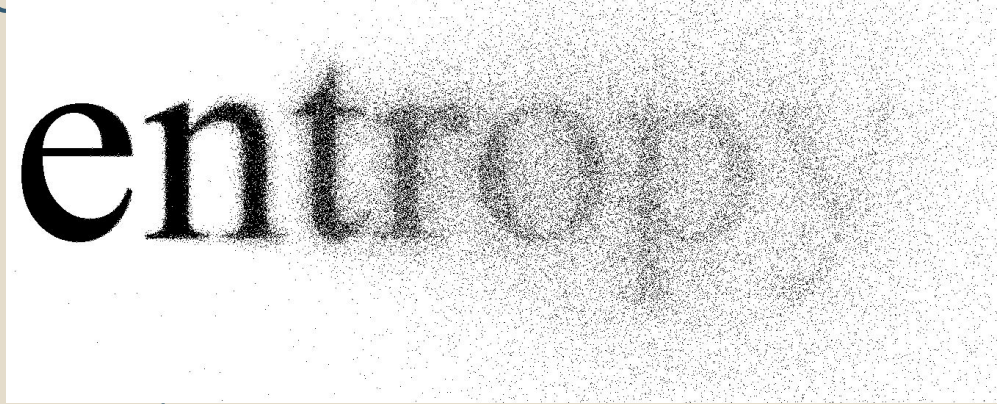
ENTROPY

The key generation process requires random values to generate keys; this randomness is provided by an Entropy source.

The current PPs and Collaborative Protection Profiles (cPPs) require that documentation be provided regarding the entropy source.

This entropy write-up consists of several sections:

- design description;
- entropy justification;
- operating conditions; and
- health testing.

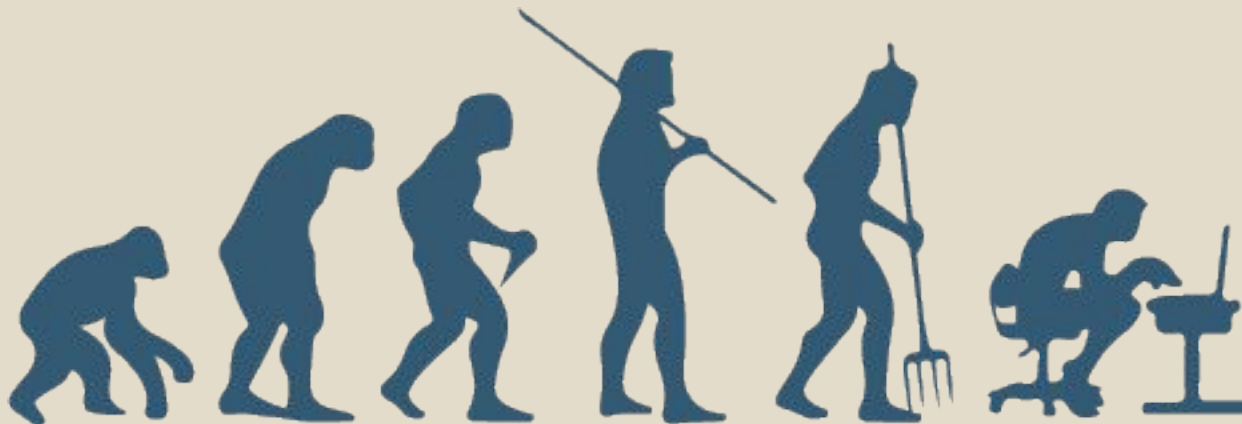


entropy

One of the challenges is dealing with 3rd party sources of entropy, where the product vendor is not the owner/creator of the entropy source.

CONCLUSION

- Cryptography is an important part of CC, and many vital security functions rely on it.
- Assurance that the cryptography functions properly is gained from the CAVP and CMVP programs, in addition to the testing required under CC.
- Evaluation of cryptographic functions in CC is not without its challenges. As requirements change, new policies and processes will need to be implemented to address any areas of concern.



FOR MORE INFORMATION



Need IT Security Advice and Guidance?

cse-cst.gc.ca/its

itsclientservices@cse-cst.gc.ca

QUESTIONS?

