The Re-use of CMVP Results within a CC Evaluation

Common Criteria Evaluation Methodology for Cryptography

Pamela Grannum ***P Eng***

Communications Security Establishment

pamela.grannum@cse-cst.gc.ca

Introduction

To describe a methodology of re-using CMVP results within a CC evaluation.

Background

Development of the Methodology

Overview

Issues

Question Session

Background

Canadian CCS labs and CMVP labs are *both* accredited to ISO/IEC 17025

CC: a set of *security functions* and *assurance criteria* used to evaluate security properties of IT products and systems

CMVP: a *validation test* for cryptographic algorithms and modules

Can results of the CMVP tests be fully accepted into the CC evaluation?

Can the assurance measures be mapped from CMVP to CC?

Can the security functions be mapped from CMVP to CC?

Is integration testing required?

Anything else?

Development of a Methodology

Initial studies:

- *Comparison Analysis*
- *Impact of FIPS 140-1 & FIPS 140-2 on CC evaluations*

Comparison of *FIPS 140-1* & *FIPS 140-2* to *CC*

Assurance Class	FIPS 140-1	FIPS 140-2
Configuration management	*Partially Met*	*Partially Met*
Delivery and operation	*Not Met*	*Partially Met*
Development	*Met with Interpretation*	*Met with Interpretation*
Guidance documents	*Partially Met*	*Partially Met*
Life cycle support	*Not Met*	*Not Met*
Tests	*Met with Interpretation*	*Met with Interpretation*
Vulnerability assessment	*Partially Met*	*Partially Met*

Cryptographic Operation in the CC

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [**assignment:** ***list of cryptographic operations***] in accordance with a specified cryptographic algorithm [**assignment:** ***cryptographic algorithm***] and cryptographic key sizes [**assignment:** ***cryptographic key sizes***] that meet the following: [**assignment:** ***list of standards***].

Cryptographic Key Access in the CC

FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform [**assignment:** ***type of cryptographic key access***] in accordance with a specified cryptographic key access method [**assignment:** ***cryptographic key access method***] that meets the following: [**assignment:** ***list of standards***].

CMVP Requirements restraints on CC Evaluation

- Non-FIPS approved operating mode
- Different operating system than the validation
- Cryptographic Algorithms

Common Criteria Evaluation Verification

As verified by independent evaluator, analysis and testing TOE security requirements have to be:

effective at solving the security problem defined for the environment

and

correctly implemented in the product

Cryptographic Algorithm Validations

CMVP-Recognised

Cryptographic Algorithms

Canadian Government –Recognised

Cryptographic Algorithms

Re-use of CMVP module validation results

FIPS 140-1/FIPS 140-2 results can be reused in CC evaluation *if these conditions met*:

Certificate is valid for the exact version of the TOE/TOE component cryptographic module

and

OS configuration is consistent with evaluated configuration

Issues

- Non-CMVP algorithms and key management standards

Summary

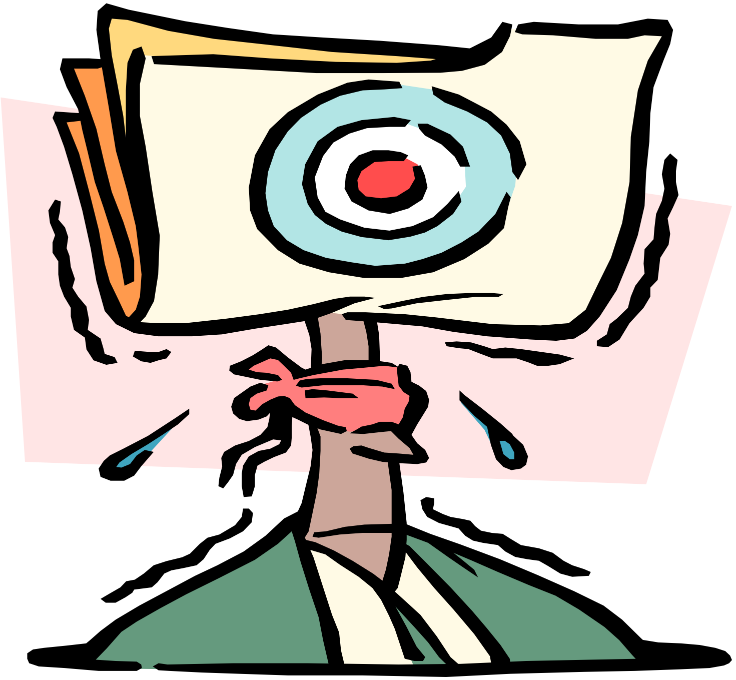
CMVP Algorithm validations

can be accepted without further testing

Module validations

not necessarily accepted without further testing

Any Questions?



Thank you for your attention.

Pamela Grannum *P Eng*

Communications Security Establishment

pamela.grannum@cse-cst.gc.ca