FIPS INSIDE™

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

ICMC
May 2016

Carolyn French
Program Manager, CMVP

FIPS 140-2 IN CANADA

- The **Cryptographic Module Validation Program (CMVP)** is a program jointly managed by Communications Security Establishment (CSE) and National Institute of Standards and Technology (NIST)

- CSE is the Canadian certification authority for the validation of cryptographic modules to FIPS 140-2, and other cryptography based standards

THE US AND FIPS 140-2

- The Federal Information Processing Standard (FIPS) 140-2 is the **standard** applied to all US Federal agencies that use cryptographic-based security systems to protect sensitive information
- The standard is **mandatory for the design and implementation of cryptographic modules** that US Federal departments and agencies operate or have operated for them under contract

MEANWHILE IN CANADA

- Information designated Protected B should be encrypted by a FIPS 140-2 validated module running in FIPS mode.
- Agencies include procurement clauses for any type of Virtual Private Network (VPN), Authentication tokens, or other applications requiring cryptography:

Use cryptographic algorithms and cryptographic key sizes that:

✓ have been approved by CSE, are validated by the Cryptographic Algorithm Validation Program and are specified in ITSB-111 (or subsequent);

✓ are implemented in a Cryptographic Module or Modules, validated by the Cryptographic Module Validation Program and

✓ are used while with the module(s) operating in FIPS Mode.

USE OF UNVALIDATED CRYPTOGRAPHY

- FIPS 140-2 does not allow the use of unvalidated cryptography **for the cryptographic protection** of *sensitive or valuable data* within Federal systems.
- Unvalidated cryptography is viewed as providing **no protection** to the information or data
  - the data is considered unprotected plaintext.
- **If an agency specifies that the information or data needs cryptographic protection**, then FIPS 140-2 is applicable.
  - In essence, if cryptography is required, then it **must** be validated.

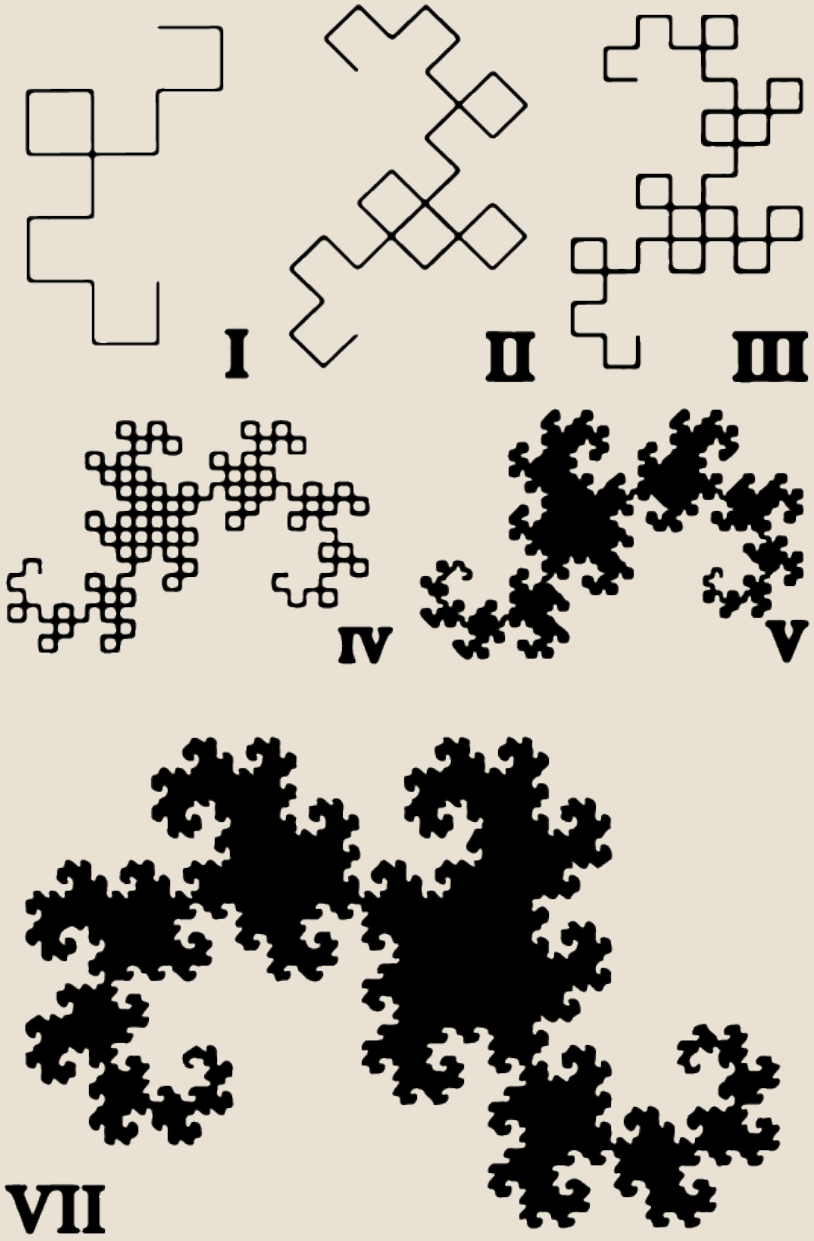
WHAT THIS MEANS…

To be considered protected, or not plaintext, information must be encrypted with:

1. An Approved algorithm; and
2. A key that has been generated or derived:
   - ✓ in an Approved manner; and
   - ✓ with an Approved strength (in both length and randomness)
     - i.e. sufficient entropy was used to seed the Deterministic Random Bit Generator (DRBG)

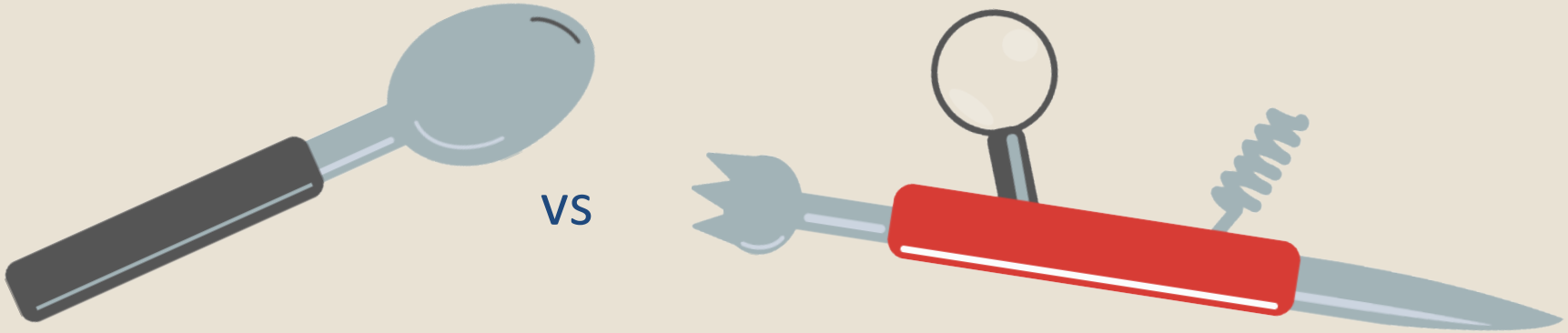
HOWEVER

THERE'S MORE TO IT THAN A CERTIFICATE NUMBER



DEFINITION OF A CRYPTOGRAPHIC MODULE

- A module, as defined by FIPS 140-2, has at least one approved cryptographic function



- Examples of where this is used:
  - Integrity checker (e.g. Secure Hash Algorithms (SHA)-2)
  - Random Bit Generators (RBG)
- A single validated module may not provide all functions
  - encryption, signature, key establishment, entropy, etc.

MODULES VS PRODUCTS

- Vendor determines the boundary of the cryptographic module
- Vendor may choose to validate their entire product, or just the cryptographically relevant component of it
  - Full appliance vs. Dynamic Link Library (DLL) performing the cryptographic functions
- The smaller module boundary:
  - Allows the FIPS testing lab to focus only on the relevant aspects of the product
  - Longer time between re-validations

FIPS INSIDE™

Additionally…

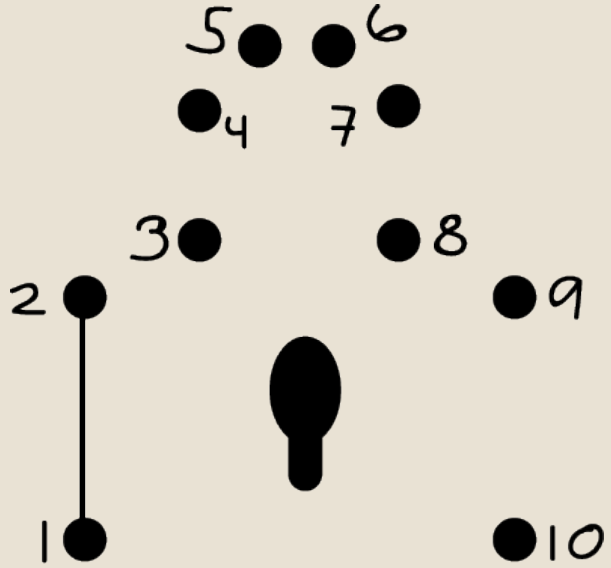
- A vendor may incorporate a validated module from another vendor (e.g. a software library) into their product
- **In either case** the CMVP recommends that users obtain a signed letter from the product vendor affirming the presence and version of the validated module

FIPS INSIDE™ IS A GOOD THING:

- Allows for elegant, re-usable solutions
- Many products seeking Common Criteria (CC) evaluations leverage FIPS Inside™

CHALLENGES

- But… what about:
  - Key management?
  - Entropy?
  - Multiple libraries/modules in the same product?
  - How does the user connect the dots to ensure that the information leaving the box, for example, is considered secure?



WHAT THE VENDOR CAN DO

- **When you are providing the signed letter, connect the dots for the user. Let them know:**
  - ✓Certificate number of module that provides entropy
  - ✓Certificate number of module(s) generating keys
  - ✓Certificate number of module(s) performing encryption
  - ✓Certificate number of module(s) performing signing and verification (if applicable)

WHAT THE USER SHOULD DO

- Ask questions – what is actually "inside"?
  - e.g. What module is generating the keys?
- In addition to checking the certificate and version number, check the caveats:
  - *No assurance of the minimum strength of generated keys*.
  - *This module has been validated with very limited cryptographic functionality which requires a risk assessment before use. Refer to the Security Policy, Section x for details.*

LEVERAGE COMMON CRITERIA (CC)

- For added confidence use CC evaluated products
- Look for a CC Evaluation certificate against an appropriate Protection Profile (PP)
- Learn more about the CC during session ***R21C: Cryptography and the Common Criteria in Canada***

PROCUREMENT LISTS

- Some Procurement Lists such as the DoD UC APL do some of this work
  - ***The UC APL recently began to enforce the requirement that the cryptographic modules be FIPS 140-2 validated. They are requiring vendors provide certificate numbers when submitting their products for consideration.***

WHAT FIPS CERTIFICATION CAN DO

- The use of the FIPS 140-2 logo on products and associated materials must be accompanied by the following:
  - "TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments"
- **If the cryptographic module is a component of a product, the phrase "FIPS 140-2 Inside" must accompany the logo.**

PERMISSION TO USE THE LOGO WITH FIPS INSIDE™

- Checklist could be implemented, including:
  - ✓Certificate number of module that provides entropy
  - ✓Certificate number of module(s) generating keys
  - ✓Certificate number of module(s) performing encryption
  - ✓Certificate number of module(s) performing signing and verification (if applicable)

http://csrc.nist.gov/groups/STM/cmvp/validation.html#06

QUESTIONS?