Communications Security Establishment

Communications Security Establishment and the FIPS 140-1 and FIPS 140-2

Jean Campbell

CMVP Director

Communications Security Establishment

Role of the CSE

- For CLASSIFED information
  - CSE approves or endorses cryptography for the GoC
- For SBU information
  - CSE develops, maintain and promotes the use of GoC Cryptographic Requirements
  - Validation authority for CMVP

GoC Cryptographic Requirements

Products must:

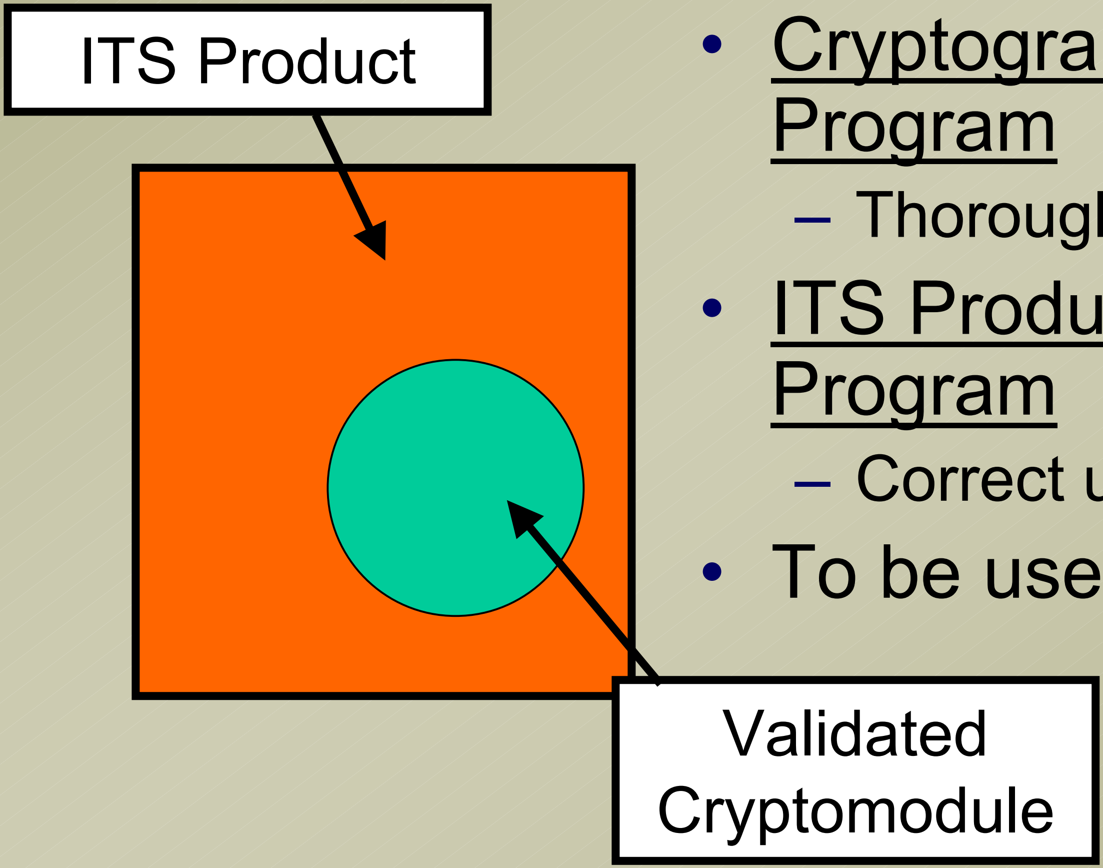
- Be, use or integrate a cryptomodule validated to FIPS 140-1 or FIPS 140-2
- Use GoC approved cryptographic algorithms
- Use GoC approved key management processes
  - Key distribution, cryptoperiods, key length, etc.
- www.cse-cst.gc.ca/en/services/crypto_services/crypto_algorithms.html

Is CSE successful with FIPS 140-1?

- CSE can not dictate to GoC departments
  - At beginning, probably mitigated
- Now a lot of government major projects require FIPS 140-1 and FIPS 140-2
- Availability of a variety of product types and brands
- Use of IPPP by GoC departments
  - www.cse-cst.gc.ca/en/services/industrial_services/its_prod_pre-qual_prog.html

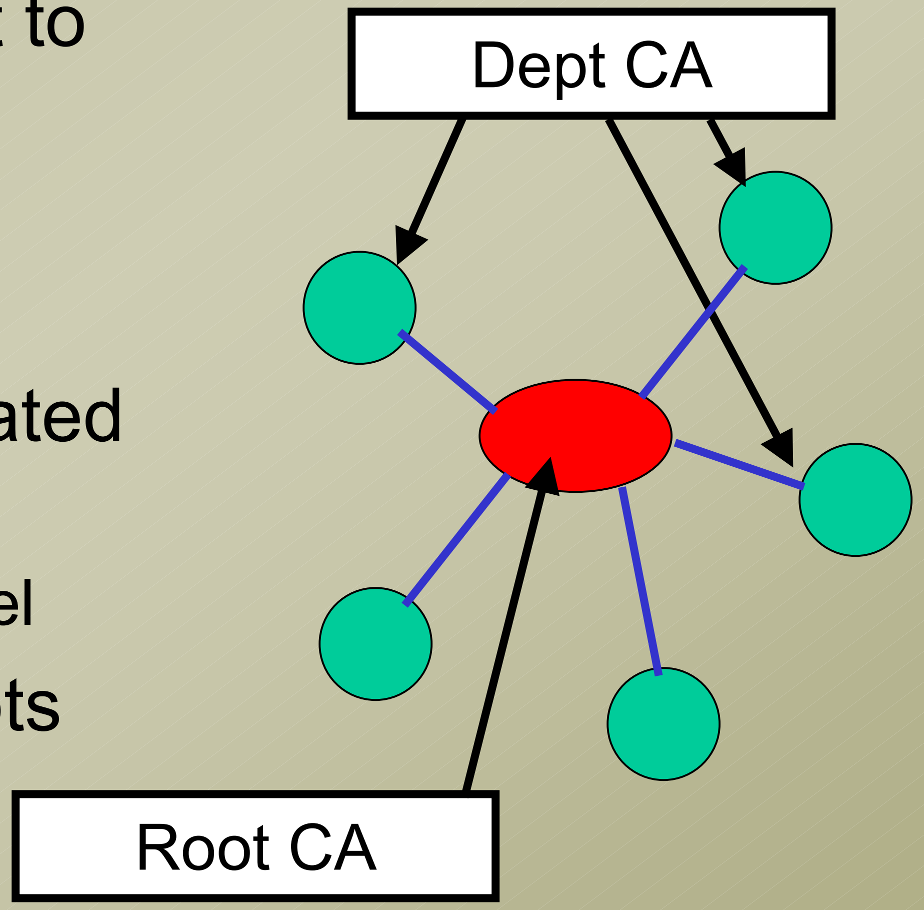
CSE Programs

- Use validation a basis for further analysis
- Cryptographic Endorsement Program
  - Thorough product analysis
- ITS Product Pre-qualification Program
  - Correct use of module
- To be used only by GoC



Government of Canada Public Key Infrastructure

- Provide PKI support to all GoC depts
- Cross-certified to a Root CA
- Entrust-based validated cryptomodule
  - Entrust Crypto Kernel
- Majority of GoC depts cross-certified or supported



Government of Canada Government On-Line

- Provide secure communication for Canadian citizens to government services
- Entrust-based validated cryptomodule
  - Entrust TruePass
- Java-based cryptomodule
  - Accessible to all citizens with appropriate Internet browser (to operate in FIPS mode)

Classified Message Handling System

- Provide protection to certain Canadian originated information classified SECRET
  - E-mail encryption and hardened PKI
  - Desktop security
- Add security measures on top of products validated to FIPS 140-1
  - PKI, full disk encryptor, tokens

Questions ???

Jean Campbell

Canadian CMVP Director

Communications Security Establishment

jean.campbell@cse-cst.gc.ca

(613) 991-8121