

FIPS and the Common Criteria: Finding the Least Common Denominator

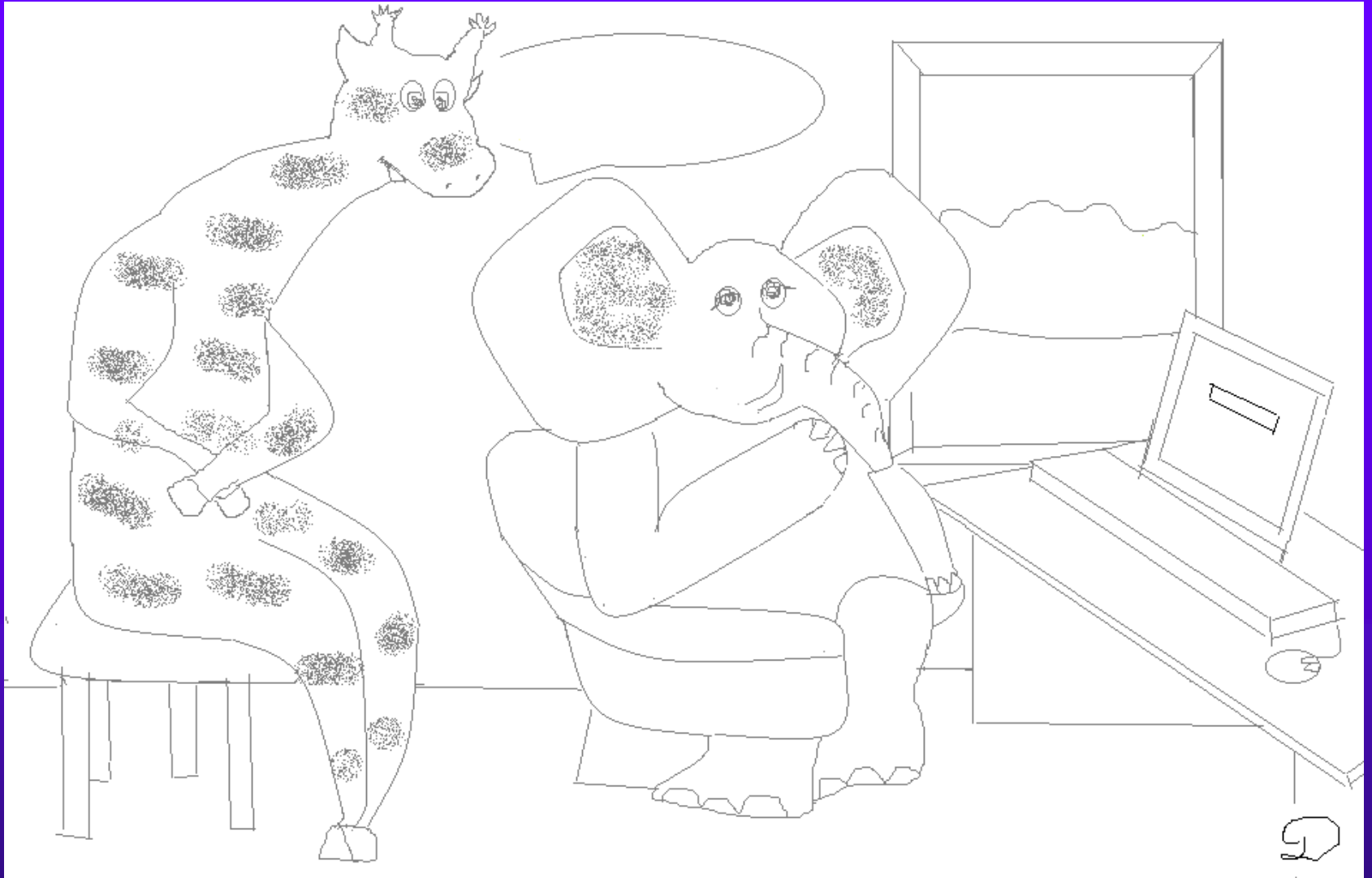


Eugene Polulyakh
Aspect Labs

FIPS and Common Criteria Lab



“FORGOT YOUR PASSWORD? AGAIN?”



SOME SAY ELEPHANTS NEVER FORGET ...



Intro to FIPS 140-2 and 140-3

- ❖ FIPS 140-1 became a mandatory standard for the protection of sensitive data when the United States Secretary of Commerce signed the standard on January 11, 1994
- ❖ On July 17, 1995, the United States National Institute of Standards and Technology established the Cryptographic Module Validation Program to validate cryptographic modules to FIPS 140-1 and other FIPS cryptography based standards



Intro to FIPS 140-2 and 140-3

- ❖ **FIPS 140-2**, Security Requirements for Cryptographic Modules, was released on May 25, 2001 and superseded FIPS 140-1
- ❖ **FIPS 140-3** is being developed. Public comment period for second draft was closed on 11 March 2010
- ❖ Government of Canada recommends the use of validated modules



FIPS 140-2

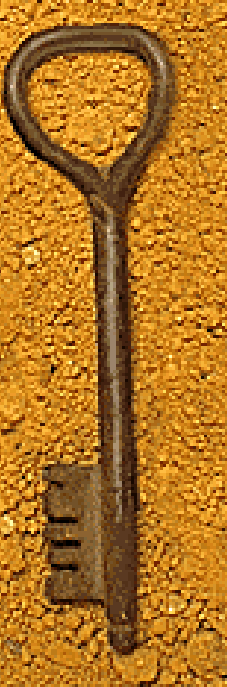
- FIPS 140-2 defines four increasing, qualitative levels of security
- Overall rating is lowest rating in all sections
- FIPS 140-2 defines 3 physical embodiments:
 - Single-chip cryptographic modules
 - Multiple-chip embedded cryptographic modules
 - Multiple-chip standalone cryptographic modules

FIPS 140-2

FIPS 140-2 Defines the Following Security Areas:

- cryptographic module specification
- cryptographic module ports and interfaces
- roles, services, and authentication
- finite state model
- physical security
- cryptographic key management
- electromagnetic interference/electromagnetic compatibility (EMI/EMC)
- self-tests
- design assurance
- operational environment
- and mitigation of other attacks





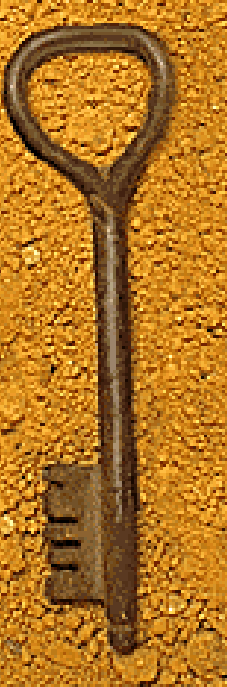
FIPS 140-2 Level 1

- Security Level 1 provides the lowest level of security
- At least one Approved security function is required
- Physical protection is not required
- Any general purpose computing system can be used

FIPS 140-2 Level 2

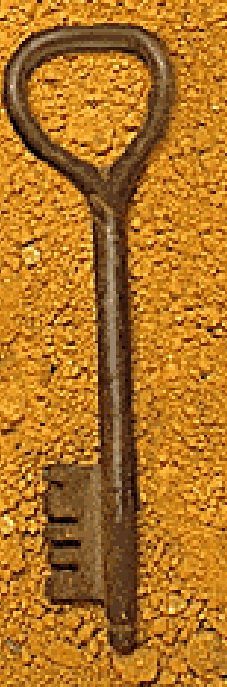
- Security level 2 adds tamper-evidence requirements
- Tamper-evident coatings or seals
- Pick-resistant locks on removable covers or doors
- Security level 2 adds authentication requirements
- Role-based authentication
- The operating system must meet functional requirements specified in the Common Criteria Protection profiles (Annex B) and evaluated at EAL2 or higher, or equivalent





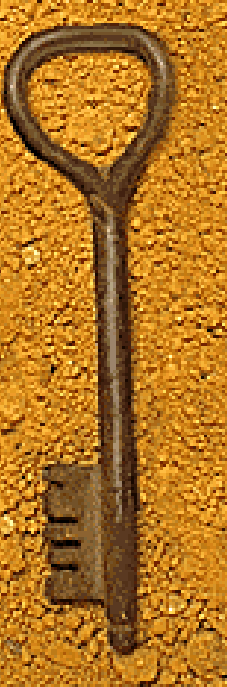
FIPS 140-2 Level 3

- Security level 3 requires a high probability of detecting and responding to physical access, use or modification attempts
- Strong enclosures and tamper detection/response
- Security level 3 adds authentication requirements
- Identity-based authentication
- Entry or output of plaintext CSPs using separate ports or a trusted path
- The operating system must meet the additional Trusted Path requirement and be evaluated at EAL3 or higher, or equivalent



FIPS 140-2 Level 4

- Security level 4 requires a complete envelope of physical protection
- Penetration of the enclosure from any direction has a highest probability of being detected. All plaintext CSPs are immediately zeroized
- Detection of fluctuations outside of the normal operating ranges for voltage and temperatures. The CSPs are zeroized
- Environmental failure testing
- The operating system must be evaluated at EAL4 or higher, or equivalent



FIPS 140-2 Annex A

Describes Approved Security Functions

- Advanced Encryption Standard (AES)
- Triple-DES Encryption Algorithm (TDEA)
- Escrowed Encryption Standard (EES)
- Digital Signature Standard (DSS)
- Key Management
- Secure Hash Standard (SHS)
- Random Number Generators (RNG and DRBG)
- Message Authentication (Triple-DES MAC, CMAC, CCM, GCM, GMAC and HMAC)

FIPS 140-3 Status



FIPS 140-3 Development Status	
TBD	Validation under FIPS 140-2 ends.
TBD	FIPS 140-3 effective. Labs may begin accepting modules for validation under FIPS 140-3
TBD	Derived Test Requirements are published.
1Q 2011	FIPS 140-3 presented to the Commerce Department for signature by the Secretary of Commerce
4Q 2010	Prepare document for publication.
Oct 2010	All public comments received for the revised (second) draft of FIPS 140-3 are processed and have been resolved.
11 Mar 2010	Public comment period for second draft of FIPS 140-3 closed. A complete set of all comments received in response to the July 2007 FIPS 140-3 draft and NIST's responses to these comments may be accessed here .
11 Dec 2009	The Revised Draft of FIPS 140-3 published for public comments. This draft addressed the comments received on the first public draft posted in July 2007 and from the FIPS 140-3 Software Security Workshop held by NIST on March 18, 2008.
18 Mar 2008	FIPS 140-3 Software Security Workshop



FIPS 140-3


- FIPS 140-3 defines four increasing, qualitative levels of security
- FIPS 140-3 defines three physical embodiments:
 - ✓ Single-chip cryptographic modules
 - ✓ Multiple-chip embedded cryptographic modules
 - ✓ Multiple-chip standalone cryptographic modules

FIPS 140-3 (Cont.)

FIPS 140-3 Defines the Following Security Areas

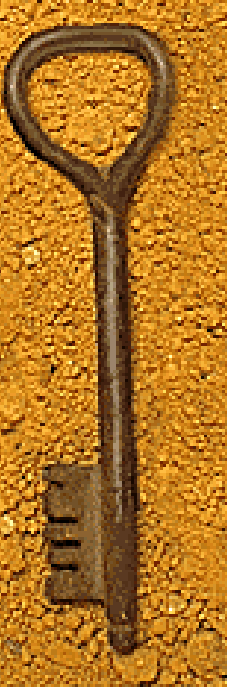
- cryptographic module specification
- cryptographic module interfaces
- roles, authentication, and services
- software/firmware security
- operational environment
- physical security
- physical security – non-invasive attacks
- sensitive security parameter management
- self-tests
- life-cycle assurance
- and mitigation of other attacks





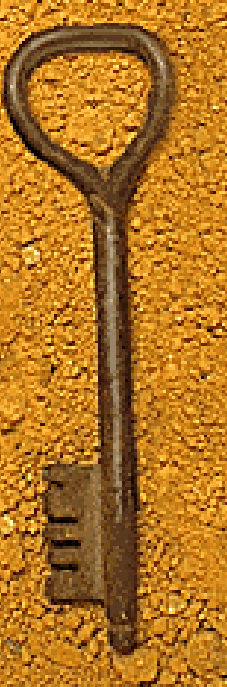
FIPS 140-3 Level 1

- Security Level 1 provides a minimum set of assurance requirements
- At least one Approved security function is required
- Does not provide protection of CSPs
- Any general purpose computing system can be used



FIPS 140-3 Level 2

- Security level 2 adds tamper-evidence requirements
- Tamper-evident coatings or seals
- Pick-resistant locks on removable covers or doors
- Security level 2 adds authentication requirements
- Role-based authentication
- Role-based access controls for the software environment, or
- Discretionary access control with groups and permissions (ACLs)
- Protection against unauthorized execution, modification, or reading of cryptographic software

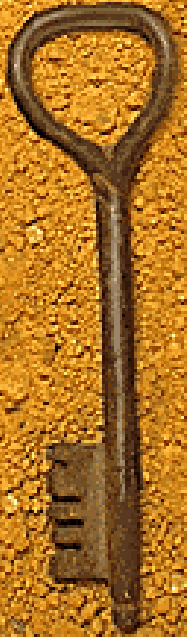


FIPS 140-3 Level 3

- Security level 3 requires a high probability of detecting and responding to physical access, use or modification attempts, and probing
- Strong enclosures and tamper detection/response
- Security level 3 adds authentication requirements
- Identity-based authentication
- Entry or output of CSPs using Trusted Channel (separate ports or interfaces)
- Mitigation assurance for non-invasive attacks
- Approved mode indication
- Can not be achieved by software modules
- Additional life-cycle requirements for CM, design, testing and authentication

FIPS 140-3 Level 4

- Security level 4 requires a complete envelope of physical protection
- Penetration of the enclosure from any direction has a high probability of being detected. All plaintext CSPs are immediately zeroized
- Multi-factor authentication using two of the following:
 - known secret
 - key or token
 - physical property, e.g. biometric





FIPS 140-3 Level 4 (Cont.)

- Detection of fluctuations outside of the normal operating ranges for voltage and temperatures. The CSPs are zeroized
- Environmental failure testing
- Non-invasive attacks testing
- Informal proof of correspondence between pre- and post-conditions and functional specification



FIPS 140-3 Additions

- High-level, non-proprietary language for all software or firmware above Level 1
- Software modules above Level 1 shall not include unnecessary code, parameters, or symbols
- Software modules can only be validated at Levels 1 and 2
- Common Criteria requirements have been dropped
- Approved Authentication techniques have been added
- Error log requirement at Levels 3 and 4
- Control inputs, status outputs, and authentication data must use Trusted Channel at Levels 3 and 4
- Non-Invasive Attacks for Single Chip modules at Levels 3 and 4



FIPS 140-3 Additions (Cont.)

- Modules above Level 1 must zeroize temporary SSP when they are no longer needed
- Current automated security diagnostic tools for software and firmware modules (such as buffer overflow detection)
- The module shall verify the input data format for all input data, and reject invalid inputs
- Detailed Security Policy requirements
- Vendor functional testing or Low-Level testing (Levels 3 and 4)



Department of the Army Letter

Letter to Industry Concerning the Approval and Acquisition of IA Tools and Products in the Army. May 21, 2009

- Specifies minimum FIPS levels for cryptographic modules
- Software modules: Overall Level 1 with
 - Level 2 for Roles, Services and Authentication and
 - Level 3 for Design Assurance sections
- Hardware and firmware modules: Overall Level 2 with Level 3 for Cryptographic Module and Design Assurance sections
- Mobile Devices, Smart Phones, PDAs, USB memory devices: Level 3 for Roles, Services, and Authentication section



New Algorithm Requirements

- SP 800-131, June 2010
- Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes
- Specifies Acceptable and Restricted use algorithms
- Specifies Transition Schedule

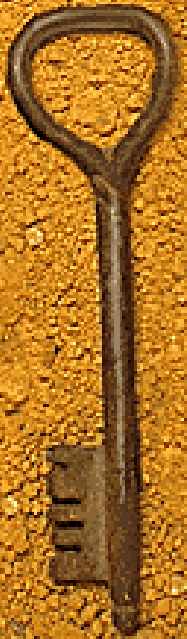
FIPS 140 vs. Common Criteria

FIPS 140

COMMON CRITERIA

- ✓ Functional and assurance requirements are bundled in the DTR
- ✓ Derived Test Requirements
- ✓ Security Level is a combination of functional and assurance requirements

- ✓ Separate Functional Requirements, Assurance Requirements, and CEM
- ✓ Security Target and PP requirements
- ✓ Assurance Level (EAL)



Consistency Issue

- FIPS certification only applies to the FIPS validated version of the module running in the FIPS-approved mode of operation
- FIPS-approved mode of operation shall be consistent with the CC Evaluated configuration
- Product modifications may be required to comply with the requirements of a PP or ST
- FIPS revalidation may be required
- Evaluation Schedule impact





Choosing FIPS Level and Features

- Protection Profile for Traffic Filter Firewall

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 -The TSF shall perform [encryption of remote authorized administrator sessions] in accordance with a specified cryptographic algorithm:

- [AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67)] and cryptographic key sizes [that are at least 128 binary digits in length] that meet the following: [FIPS PUB 140-2 (Level 1)].

- The cryptographic module must perform AES encryption



Choosing FIPS Level and Features

- WLAN Access System Protection Profile

FCS_BCM_(EXT).1.1 All FIPS-approved cryptographic functions implemented by the TOE shall be implemented in a cryptomodule that is FIPS 140-2 validated, and perform the specified cryptographic functions in a FIPS-approved mode of operation. The FIPS 140-2 validation shall include an algorithm validation certificate for all FIPS-approved cryptographic functions implemented by the TOE.

- Simply states the FIPS validation requirement



Choosing FIPS Level and Features

FCS_BCM_(EXT).1.2 All cryptographic modules implemented in the TOE [selection:

Entirely in hardware shall have a minimum overall rating of FIPS PUB 140-2, Level 3,

Entirely in software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2, Level 3 for the following: Cryptographic Module Ports and Interfaces; Roles, Services and Authentication; Cryptographic Key Management; and Design Assurance.

As a combination of hardware and software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2, Level 3 for the following: Cryptographic Module Ports and Interfaces; Roles, Services and Authentication; Cryptographic Key Management; and Design Assurance.]

- FIPS 140-2 Level 1 testing is not sufficient
- Stricter requirements for hardware modules



Choosing FIPS Level and Features

FCS_CKM.1.1(1) Refinement: The TSF shall generate symmetric cryptographic keys using a FIPS-Approved Random Number Generator as specified in FCS_COP_(EXT).1, and provide integrity protection to generated symmetric keys in accordance with NIST SP 800-57 "Recommendation for Key Management" Section 6.1.

- Adds integrity protection requirements
- May not be covered by FIPS testing



Choosing FIPS Level and Features

FCS_CKM_(EXT).2.2 The TSF shall store persistent secret and private keys when not in use in encrypted form or using split knowledge procedures.

- Adds key encryption requirements
- May not be covered by FIPS testing



Choosing FIPS Level and Features

- FCS_CKM.4.1

- c) The TSF shall zeroize each intermediate storage area for plaintext key/critical cryptographic security parameter (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/critical cryptographic security parameter to another location.
- d) For non-volatile memories other than EEPROM and Flash, the zeroization shall be executed by overwriting three or more times using a different alternating data pattern each time.

- Adds zeroization requirements
- May not be covered by FIPS testing

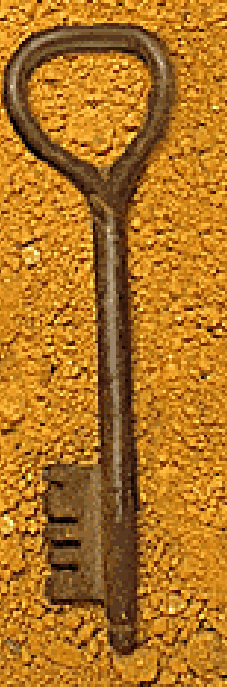


Choosing FIPS Level and Features

FCS_COP.1.1(3) Refinement: The TSF shall perform cryptographic hashing services using the FIPS-approved security function Secure Hash Algorithm and message digest size of *[selection: one or more of 256 bits, 384 bits, 512 bits]*.

- Stronger HASH requirements
- May not be covered by FIPS testing

Choosing FIPS Level and Features



FPT_TST.1.1(1) **Refinement:** The TSF shall run a suite of self tests in accordance with **FIPS PUB 140-2** and **Appendix C** of this profile during initial start-up (on power on), at the request of the cryptographic administrator (on demand), under various conditions defined in section 4.9.1 of FIPS 140-2, and periodically (at least once a day) to demonstrate the correct operation of the following cryptographic functions:ⁱ

- a) key error detection;
- b) cryptographic algorithms;
- c) RNG/PRNG

FPT_TST.1.2(1) **Refinement:** The TSF shall provide authorized cryptographic administrators with the capability to verify the integrity of **TSF** data related to the cryptography by using **TSF-provided** cryptographic functions.ⁱⁱ

- Stronger self test requirements
- May not be covered by FIPS testing



FIPS 140 and CC Overlaps

- CC authentication requirements:

FIA_UAU.1.1

The TSF shall allow [ST Author Assignment: list of TSF mediated actions] on behalf of users to be performed before the user is authenticated.

FIA_UAU.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

- FIPS authentication requirements:

AS03.17: (Level 2) If role-based authentication mechanisms are supported by the cryptographic module, the module shall require that one or more roles either be implicitly or explicitly selected by the operator and shall authenticate the assumption of the selected role (or set of roles).



FIPS 140 and CC Overlaps

- CC identification requirements:

FIA_UID.2.1

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

- FIPS identification requirements:

AS03.19: (Level 3 and 4) If identity-based authentication mechanisms are supported by the cryptographic module, the module shall require that the operator be individually identified, shall require that one or more roles either be implicitly or explicitly selected by the operator, and shall authenticate the identity of the operator and the authorization of the operator to assume the selected role (or set of roles).



FIPS 140 and CC Overlaps

- CC CM requirements:

ALC_CMC.2.1C *The TOE shall be labelled with its unique reference.*

ALC_CMC.2.2C *The CM documentation shall describe the method used to uniquely identify the configuration items.*

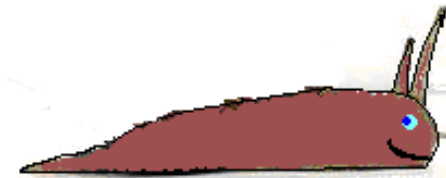
ALC_CMC.2.3C *The CM system shall uniquely identify all configuration items.*

- FIPS CM requirements:

AS10.01: (Levels 1, 2, 3, and 4) A configuration management system shall be implemented for the cryptographic module and module components within the cryptographic boundary, and for associated module documentation.

AS10.02: (Levels 1, 2, 3, and 4) Each version of each configuration item (e.g., cryptographic module, module components, user guidance, security policy, and operating system) that comprises the module and associated documentation shall be assigned and labeled with a unique identification number.

Security v. Speed





Recommendations

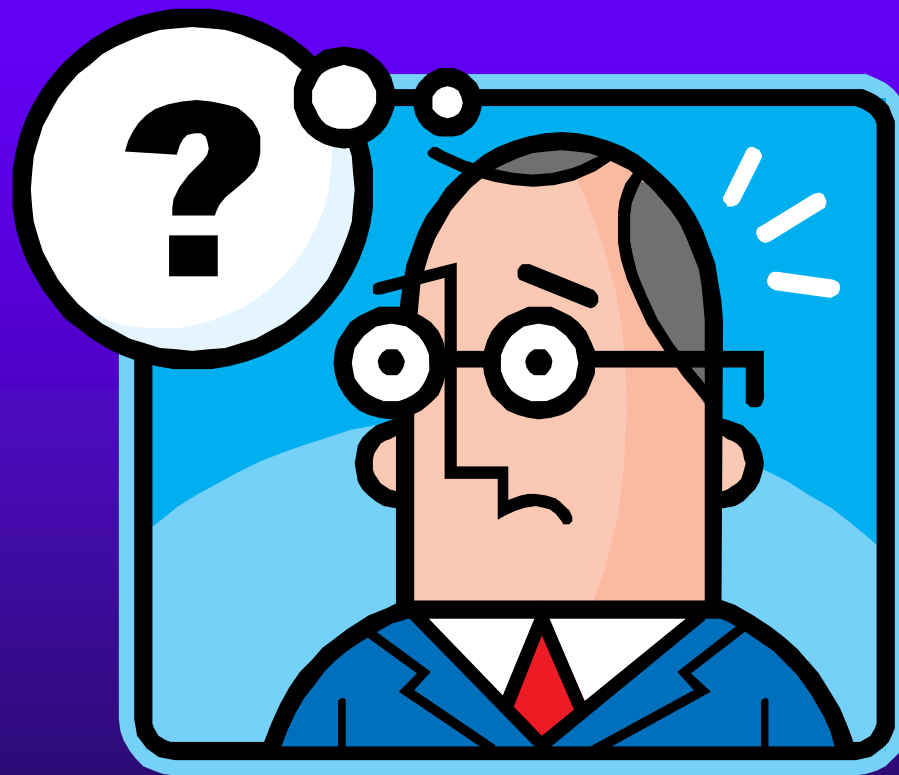
- Review of the cryptographic module features specified in the PP or ST
- Review of the FIPS 140 levels and requirements
- Review of any additional customer requirements related to FIPS 140, e.g. the Army Letter
- Review of the new crypto algorithm requirements and transition schedule, i.e. NIST SP 800-131
- Review of the OS CC requirements
- Determination of the minimum set of FIPS levels, features, algorithms, and OS versions



Recommendations

- FIPS and CC product features should be implemented simultaneously
- Development documentation, test plans, and other FIPS and CC documentation should be developed simultaneously and should satisfy both FIPS and CC requirements
- FIPS and the Common Criteria design analysis and code reviews should be performed simultaneously

Questions





Contact Information

Eugene Polulyakh

Aspect Labs

FIPS and Common Criteria Lab of Silicon Valley

3080 Olcott Street

Santa Clara, California 95054 USA

Phone: +1-408-876-7470

Web: www.aspectlabs.com

E-mail: ep@aspectlabs.com

