SP 800 140x Overview

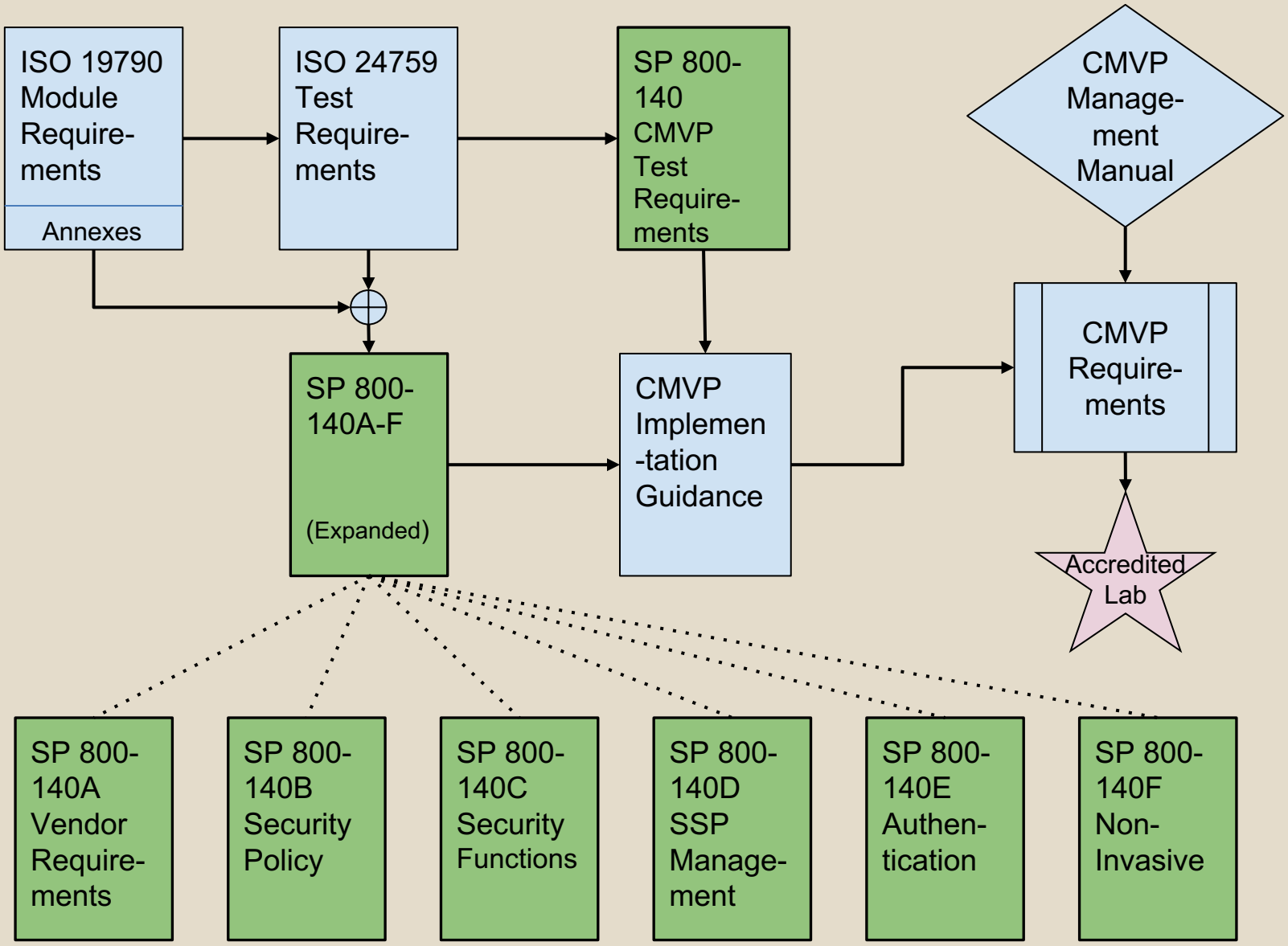
ICMC 2020

Kim Schaffer, DSc

September 23, 2020

Agenda

- Summary of integration
- CMVP Modifications:
  - Testing
  - Vendor Documentation
  - Security Policy
  - Security Functions
  - SSP Management
  - Authentication
  - Non-Invasive


ISO 19790 Module Require-ments
Annexes
ISO 24759 Test Require-ments
SP 800-140 CMVP Test Require-ments
CMVP Manage-ment Manual
CMVP Require-ments
SP 800-140A-F
(Expanded)
CMVP Implemen-tation Guidance
Accredited Lab
SP 800-140A Vendor Require-ments
SP 800-140B Security Policy
SP 800-140C Security Functions
SP 800-140D SSP Manage-ment
SP 800-140E Authen-tication
SP 800-140F Non-Invasive

SP 800-140

- NIST Special Publication directly supporting CMVP testing
- Does not modify ISO/IEC 19790 requirements (ISO/IEC 24759 AS)
- Adds/modifies/deletes vendor evidence (VE) and testing (TE) necessary to demonstrating the module meets the requirements.
  - Does modify an authentication related example given in a AS statement.

SP 800-140A - Documentation Requirements

- Affirms ISO/IEC 19790 Annex A requirements
- Adds the requirements that the vendor must address and the tester verify all information required to support the SP 800-140x documents, IGs, and CAVP/CMVP requirements.
- In future may place requirements on validation data input for import into validation authority tools.

SP 800-140B - Crypto Module Security Policy

- Dictates the presentation of ISO/IEC 19790 Annex B requirements as required by CMVP
- By standardizing security policy inputs we can work toward
  - Less errors as the information passes through the organizations
  - Easier new Cryptik entry & checking
  - Less time & energy during final processing
  - Easier validation entry verification
- Increase possibility of automation in the future
  - Less chance of entry errors in submission report, security policy, and validation certificate

SP 800-140C - Approved Security Functions

- Replaces ISO/IEC 19790 Annex C requirements
- Closely parallels FIPS 140-2 Approved Security Functions
  - May differ in some transitions
- Standards referenced include
  - Symmetric Key Encryption and Decryption (AES, TDEA, SKIPJACK)
  - Digital Signatures (DSA, RSA and ECDSA)
  - Hash (SHS, SHA-3,)
  - Message Authentication (Triple-DES, AES and HMAC)

SP 800-140D - Approved SSP Generation and Establishment

- Replaces ISO/IEC 19790 Annex D requirements
- Closely parallels FIPS 140-2 Approved Security Functions
  - May differ in some transitions
- Standards referenced include
  - SSP Generation
  - RBG
  - Entropy

SP 800-140E Approved Authentication Mechanisms

- Replaces ISO/IEC 19790 Annex E requirements (currently none defined)
- No approved authentication mechanisms, allowed listed below
  - recommend following SP 800-63B when possible

FIPS 140-3 Level	Authentication
Level 1	None required—may be implicit. If authentication is used, it should meet the requirements of Level 2 as a minimum.
Level 2	Memorized secret or Level 3 authentication mechanism
Level 3	Memorized Secret; Look-Up Secret; Out-of-Band; Single-Factor One Time Password (OTP) Device; Multi-Factor OTP Device; Single-Factor Crypto Software; Single-Factor Crypto Device; Multi-Factor Crypto Software; Multi-Factor Crypto Device
Level 4	Multi-Factor Crypto Software; Multi-Factor Crypto Device

- IGs will provide further guidance until SP 800-140E can updated

SP 800-140F Non-Invasive Attack Mitigation Test Metrics

- Replaces ISO/IEC 19790 Annex F requirements (currently none defined)
- Currently no approved test metrics
- Planned addition to SP 800-140F in 2021
  - ISO/IEC 17825 Information technology – Security techniques – Testing methods for the mitigation of non-invasive attack classes against cryptographic modules
    - ISO/IEC 20085-1 Information technology – Security techniques – Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques (pending publication)
    - ISO/IEC 20085-2 Information technology – Security techniques – Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 2: Test calibration methods and apparatus.

Questions?

Kim Schaffer – Kim.Schaffer@NIST.gov

nist.gov/cmvp