Cryptographic Key Management Workshop

March 4-5, 2014

Session 6: Testing, Assessment and Validation

Elaine Barker, Dennis Branstad,
Ron Ross and Miles Smid

Testing and System Assurances

Dennis K. Branstad

Terminology Overview

- **Testing**: Performing specific test procedures and **comparing the results** with the anticipated results.
- **Assessing**: Reviewing a subject to determine that the **specific desirable results** are exhibited.
- **Verification**: **Determining** that the **result**s of testing and assessing **are acceptable (**or not**).**
- **Assurance**: Being **convinced of something**, e.g., that keys, metadata, and data are secure.
- **Validation/Certification**: A **formalized validation** process for which a **certificate is issued** by an authority after obtaining assurance that validation **results are correct and acceptable.**

Types of Testing

- CKMS Designer and Implementer Testing
- Third Party Testing
- Procurement Acceptance Testing
- Functional and **Security** Testing
- Physical Security and Utility Service Testing
- Ease-of-use Testing
- Scalability Testing
- System Load Stress Testing
- Operational Self Testing

Pre-Procurement Testing 1

- Implementation Testing (Section 9.1)
  - An FCKMS **must be tested** to ensure that it:
    - ✓ **Conforms** to its design documentation and required standards,
    - ✓ **Operates** according to its implementation and procurement specifications, and
    - ✓ **Rejects** service requests that could compromise its security.

Pre-Procurement Testing 2

- Third-party Testing (Section 9.2)
  - Cryptographic modules **shall** be validated using the CMVP (PR:9.2).
  - NIST-approved algorithms **shall** be validated using the CAVP (PR:9.3).
  - Non-cryptographic modules and devices **should** be tested, e.g., by the National Information Assurance Partnership (NIAP) (PA: 9.3 and 9.4).
- Interoperability Testing (Section 9.3)
  - Interoperability is not a requirement, but **could** be specified by an FCKMS using-organization and tested (PF:9.1).

Pre-Procurement Testing 3

- Self-Testing (Section 9.4)
  - Self-testing **shall** be performed to **verify the correct operation of modules and devices** (PR:9.4).
- Scalability Testing (Section 9.5)
  - Scalability **shall** be tested using the anticipated maximum number of users, devices, applications, and modules (PR: 9.5).
  - FCKMS operation should **degrade gracefully** when subjected to increasing numbers of service requests that stress its capabilities.

Pre-Procurement Testing 4

- Ease-of-Use Testing (Section 9.8.5)
  - FCKMS-User interfaces **should** be evaluated and approved **for ease-of-use** (PA: 9.6).
    - ✓ A panel of people having different expertise and experience **should** create evaluation criteria, develop ease-of-use evaluation tests, and evaluate the results of tests that are performed by a test group of users.
  - An FCKMS **should** automatically detect incorrect user inputs, based on parameters such as length, format, or acceptable range (PA: 9.7).

Pre/Post Procurement Testing

An FCKMS:

- ✓ **Could support demonstrations** of correct usage (PF:9.5),
- ✓ **Could** be designed to **adapt to a user's experience and abilities** (PF:9.6), and
- ✓ **Could** be evaluated by a third-party for its **ease-of-use characteristics prior to initial operation** and **after** interface **changes are made (PF:9.7)**.

Pre-Procurement Verification

- Implementer tests on a candidate CKMS, its modules and devices **shall** be reviewed by a Federal Procurement Authority for satisfactory results **(PR:9.1).**

- Any pre-procurement and user acceptance test results **should** be verified by Federal procurement representatives prior to procurement **(PA:9.1**).

Pre-Procurement Verification 2

- **Verify** (by Federal procurement representatives) that all third-party tests performed for **conformance** to procurement specifications and standards have been performed **and** that all test **results are satisfactory**. [Note: May need a PR in final Profile]

- **Verify** that the candidate CKMS **satisfies the procurement specifications** for key management services, cryptographic functions, human-CKMS interfaces for all specified roles, ease-of-use, and interoperability requirements. [Note: Done by Fed. Procurement reps; May need a PR.]

- Note: **Verification is binary**: i.e., Results are either Yes or No.

Pre-Operational Testing

- Functional and Security Testing (Section 9.6)
  - Objective: Perform functional and security tests that assure that the FCKMS will **function correctly** in accordance with its design and implementation specifications and that it operates securely.
  - Appropriate tests and test results **should** result in **assurances** that an **FCKMS will perform as desired**.
  - Security testing **should** include penetration testing.

- FCKMS Environmental Testing (Section 9.7)
  - **Environmental testing should be performed** (PA:9.5)**.**
  - Testing should include: **physical security, environmental safety, and reliable utility services.**

Pre-Operational Verification

- Functional and security tests, including penetration tests, **shall** have been passed Before Initial Operation (BIO) (PR:9.6).
- Any environmental tests performed **should** have been passed BIO (PA:9.5).

Testing During Normal Operations

- Self tests **should** be performed to verify acceptable functionality, integrity, and security (PA:9.2 and PR:9.4).
- Functional and security testing **shall** be conducted and passed annually and periodically to assure continuity of secure operations (PR:9.7).

Areas Needing Security Assurance

- CKMS: Design and Implementation -
  - Delivery and Installation.
- FCKMS: Procurement Procedures -
  - Configuration Management,
  - System Initialization and Operation,
  - Physical & Environmental Security,
  - Role-Performing Personnel Management,
  - Security Policy Administration, and
  - Life-cycle Operation and Maintenance.

Development, Delivery and Maintenance Assurances 1

- Configuration Management (Section 9.8.1)
  - **Protect an FCKMS against unauthorized modification** during the entire lifecycle, including implementation, delivery, installation, operation, & maintenance.
  - Place **under configuration management** from design though final destruction (PR:9.8).
  - **Automated configuration management** control could be used (PF: 9.3).
- Secure Delivery (Section 9.8.2)
  - Verify that the product has not be tampered with or replaced, and that delivery is timely (PR:9.9).
  - Notification of delivery problems to FCKMS management **shall** be supported (PR:9.10).

Development, Delivery and Maintenance Assurances 2

- Development and Maintenance Environment Security (Section 9.8.3)
  - Verify that the claimed procedures were followed and documented per FR:9.12 (PR: 9.11).

    Note: Profile requirements sometimes specifically reference Framework requirements.
  - Development and maintenance environments **shall** be protected against physical, technical and personnel threats (PR:9.12).

Development, Delivery and Maintenance Assurances 3

- Flaw Remediation (Section 9.8.4)
  - **Detection, reporting, and correction** of FCKMS flaws must be done in an expeditious and secure manner.
  - Users should **report potential and detected flaws** to management.
  - Support the detection, reporting and timely **correction of security-compromising flaws** (PR: 9.13).
  - **Configuration management is critical** for flaw detection and installing software/hardware fixes.
  - Automated flaw-detection techniques **could** continuously monitor an FCKMS's security status, report potential problems, and minimize reliance on human monitoring (PF:9.4).

Security Maintenance
(Section 11.4)

- **PR:11.14** A Federal CKMS **shall** verify that:
  - The **latest security** updates and security patches have been **installed** as soon as they are available, and
  - **Periodic testing** against the hardening guidelines has been **performed and passed**:
    - ✓ **After changes** have been made to the FCKMS, and
    - ✓ **Before** the FCKMS returns to an **operational status**.
- Security incidents **should be reported, investigated**, and **mitigated** (PA:11.11 and PA:11.12).

Workshop Participant Discussion

- Questions?
- Suggestions?

FIPS 199, FIPS 200 and SP 800-53

See Ron Ross's slides, which are provided separately.

Security Assessments
(Sections 11.1 – 11.3)

See Miles Smid’s slides, which are provided separately.

Validation Issues

Elaine Barker

Validation Issues 1

- Few validation programs are currently available.
  - Cryptographic Algorithm Validation Program (CAVP) tests NIST-approved cryptographic algorithms against specifications.
  - Cryptographic Module Validation Program (CMVP) tests cryptographic modules against FIPS 140.
  - National Information Assurance Partnership (NIAP) tests non-cryptographic software and hardware against the Common Criteria Standard.

Validation Issues 2

- What other validation programs are needed?
  - FCKMS/FCKMS Module interoperability?
  - Functional and security testing?
  - Environmental testing?
  - Ease-of-use testing?

Validation Issues 3

- Setting up a validation program:
  - How is a validation program set up?
  - Who will perform the testing and who will validate the tests?
  - How are the testing and validation entities deemed to be qualified?
  - How is a validation program financed? How big a market is there?
- Discussions/volunteers, etc.?

Questions and Comments?