NIST Cryptographic Conformance Testing Update

- NIST Security Testing Group Overview
- Automated Cryptographic Testing
- FIPS140-3 / ISO 19790
- Entropy Testing
- Crypto Module Automated Testing
- Outreach Activities

DISCUSSION TOPICS
Advance information security testing, measurement science, and conformance.

STVM’s testing-focused activities include validating cryptographic algorithm implementations, cryptographic modules, and Security Content Automation Protocol (SCAP)-compliant products; developing test suites and test methods; providing implementation guidance and technical support to industry forums; and conducting education, training, and outreach programs.
- CAVP – Cryptographic Algorithm Validation Program
- CMVP – Cryptographic Module Validation Program
- SCAP – Security Content Automation Protocol Validation Program
- PIV – Personal Identity Verification Validation Program
- NVD – National Vulnerability Database
- NCP – National Checklist Program
- USGCB – US Government Configuration Baseline
- Metrics Research – shared with the math division
Tests each individual cryptographic algorithm implementation against the associated standard.

Test tool – Crypto Algorithm Validation System (CAVS) – being retired – 1 July

ACVTS – Automated Cryptographic Validation Testing System – in production use.
ACVTS Base Architecture
Automated Cryptographic Validation Protocol

**ACV Server:**
- Web-hosted service
- Generates JSON test vectors
- Performs results verification

**ACV Protocol:**
- Standards-based protocol
- Developed in partnership with CMVP
- Extensible to mitigate additional vectors over time
- Open Source to enable independent verification

**ACV Client:**
- Integrated into Device under test
- May convert JSON test vectors to format acceptable by crypto module under test
- Returns KAT answers to ACV server in JSON format

**ACV Protocol:**
- Standards-based protocol
- Developed in partnership with CMVP
- Extensible to mitigate additional vectors over time
- Open Source to enable independent verification

**Device Under Test**

**Crypto Module**

**Entropy Source**

**ACV Server**

**ACV Client**

**Test Vectors**

**Responses**
CAVP Program Overview
- https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program

Automated Testing Project Overview
- https://csrc.nist.gov/Projects/Automated-Cryptographic-Validation-Testing

GitHub - Open Source Development Project Page
- https://github.com/usnistgov/ACVP

Currently Running Development Server
- https://demo.acvts.nist.gov/acvp/home
ACVTS – has tests for all NIST approved algorithms, and improved test cases for all algorithms.

All labs have shown the capability to use the new system.

Demo system vs Production

Open Source

1st party Labs
Vendors of cryptographic modules use independent, accredited Cryptographic and Security Testing (CST) laboratories to test their modules.

CST laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against FIPS 140-2.

NIST's Computer Security Division (CSD) and CSEC jointly serve as the Validation Authorities for the program, validating the test results and issuing certificates.
FIPS-140

• FIPS 140-1 was issued on January 11, 1994
  - developed by a government and industry working group
  - NIST established the Cryptographic Module Validation Program

• FIPS 140-2 was issued on May 25, 2001
  - only very modest changes compared to predecessor
  - same year when AES became a standard
  - FISMA-2002 removed the statutory provision that allowed agencies to waive mandatory FIPS
## CMVP Testing and Validation Flow

<table>
<thead>
<tr>
<th>Vendor</th>
<th>CST Lab</th>
<th>CMVP (NIST and CSEC)</th>
<th>User</th>
</tr>
</thead>
</table>
| **Designs and Produces**  
Hardware • Software • Firmware  
Define Boundary  
Define Approved Mode of Operation  
Security Policy | **Tests for Conformance**  
Derived Test Requirements  
CAVP Algorithm Testing  
Documentation Review  
Source Code Review  
Operational and Physical Testing | **Validates**  
Review Test Results  
Ongoing NVLAP Assessment  
Issue Certificates  
NIST Cost Recovery Fee | **Specifies and Purchases**  
Security and Assurance  
Applications or products with embedded modules |

**TESTING PROGRAMS: CMVP**
Implementation Schedule

- **March 22, 2019** –
  - FIPS 140-3 Approved
- **September 22, 2019** –
  - FIPS 140-3 Effective Date
  - Drafts of SP 800-140x available for public comment (See status page)
- **March 22, 2020** –
  - Publication of SP 800-140x documents
  - Implementation Guidance updates
  - Tester exam updated to include FIPS 140-3
  - Updated CMVP Program Management Manual
- **September 22, 2020** –
  - CMVP accepts FIPS 140-3 submissions
- **September 22, 2021**
  - CMVP stops accepting FIPS 140-2 submissions
SP 800-140x documents

- [SP 800-140 - FIPS 140-3 Derived Test Requirements (DTR)](https://csrc.nist.gov/Projects/fips-140-3-transition-effort/transition-to-fips-140-3)
- [SP 800-140A - CMVP Documentation Requirements](https://csrc.nist.gov/Projects/fips-140-3-transition-effort/transition-to-fips-140-3)
- [SP 800-140B - CMVP Security Policy Requirements](https://csrc.nist.gov/Projects/fips-140-3-transition-effort/transition-to-fips-140-3)
- [SP 800-140C - CMVP Approved Security Functions](https://csrc.nist.gov/Projects/fips-140-3-transition-effort/transition-to-fips-140-3)
- [SP 800-140D - CMVP Approved Sensitive Security Parameter Generation and Establishment Methods](https://csrc.nist.gov/Projects/fips-140-3-transition-effort/transition-to-fips-140-3)
- [SP 800-140E - CMVP Approved Authentication Mechanisms](https://csrc.nist.gov/Projects/fips-140-3-transition-effort/transition-to-fips-140-3)
- [SP 800-140F - CMVP Approved Non-Invasive Attack Mitigation Test Metrics](https://csrc.nist.gov/Projects/fips-140-3-transition-effort/transition-to-fips-140-3)

FIPS 140-3 / ISO 19790
Published the relevant Special Pubs in March

Updating Implementation guidance

Ongoing development for new testing submission tool

- Current tool – Cryptik – MS Access desktop app
- New tool – Web based submission
Based on SP 800-90B – Recommendation for Entropy Sources Used for Random Bit Generation

Separate validation from the module
  - Allows for reuse of validated entropy sources

New NVLAP Scope

New tool – Web based submission application in development
NCCOE Project in development

Workshop targeted for 1 September

Goal of working with Crypto developers to develop automated testing techniques for most of the requirements in FIPS 140.


TESTING PROGRAMS: CMVP
CRYPTO MODULE AUTOMATED TESTING
RSA - February 24 – 28 – San Francisco
ICMC – April 28 – May 1 – Bethesda
  ▶ Postponed until August 25 – 28
  ▶ Planned to be Live and Virtual
CMUF – Monthly Calls
ICCC – 20 – 22 October – Toledo, Spain
CCUF – workshops and conference

NIST CRYPTO TESTING OUTREACH
NIST CONTACTS

- Matt Scholl – Computer Security Division Chief
  - matthew.scholl@nist.gov
- Michael Cooper – Manager of the Security Testing Group
  - michael.cooper@nist.gov
- Tim Hall – CAVP Program Manager
  - tim.hall@nist.gov
- Apostol Vassilev – Security Testing Research Team Lead
  - Apostol.Vassilev@nist.gov
- Beverly Trapnell – CMVP Program Manager
  - beverly.trapnell@nist.gov
- Lily Chen – Manager of the Crypto Technology Group
  - lily.chen@nist.gov