

NIST CRYPTOGRAPHIC CONFORMANCE TESTING UPDATE

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
INFORMATION TECHNOLOGY LABORATORY
COMPUTER SECURITY DIVISION
SECURITY TESTING, VALIDATION, AND MEASUREMENT

MICHAEL COOPER – MANAGER STVM

ISPAB June 25, 2020

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.

TESTING GROUP MISSION

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, set against a blue background.

- ▶ 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

PROGRAMS IN STVM

- ▶ 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.

TESTING PROGRAMS: CAVP

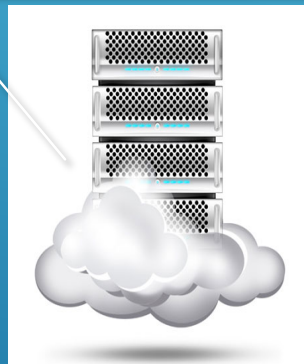


ACVTS Base Architecture

Automated Cryptographic Validation Protocol

ACV Server:

- Web hosted service
- Generates JSON test vectors
- Performs results verification



ACV Server

ACV Protocol

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

Entropy Source

Seed

ACV Client

Test Vectors

Responses

Crypto Module

Device Under Test

ACV Protocol:

- Standards-based protocol
- Developed in partnership w/ CMVP
- Extensible to mitigate additional vectors over time
- Open Source to enable independent verification

- ▶ 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>

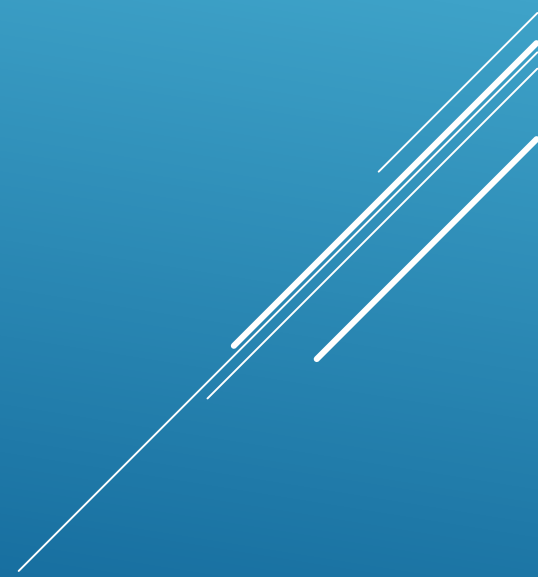
CAVP - REFERENCES



- ▶ 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

TESTING PROGRAMS: CAVP


CURRENT STATUS



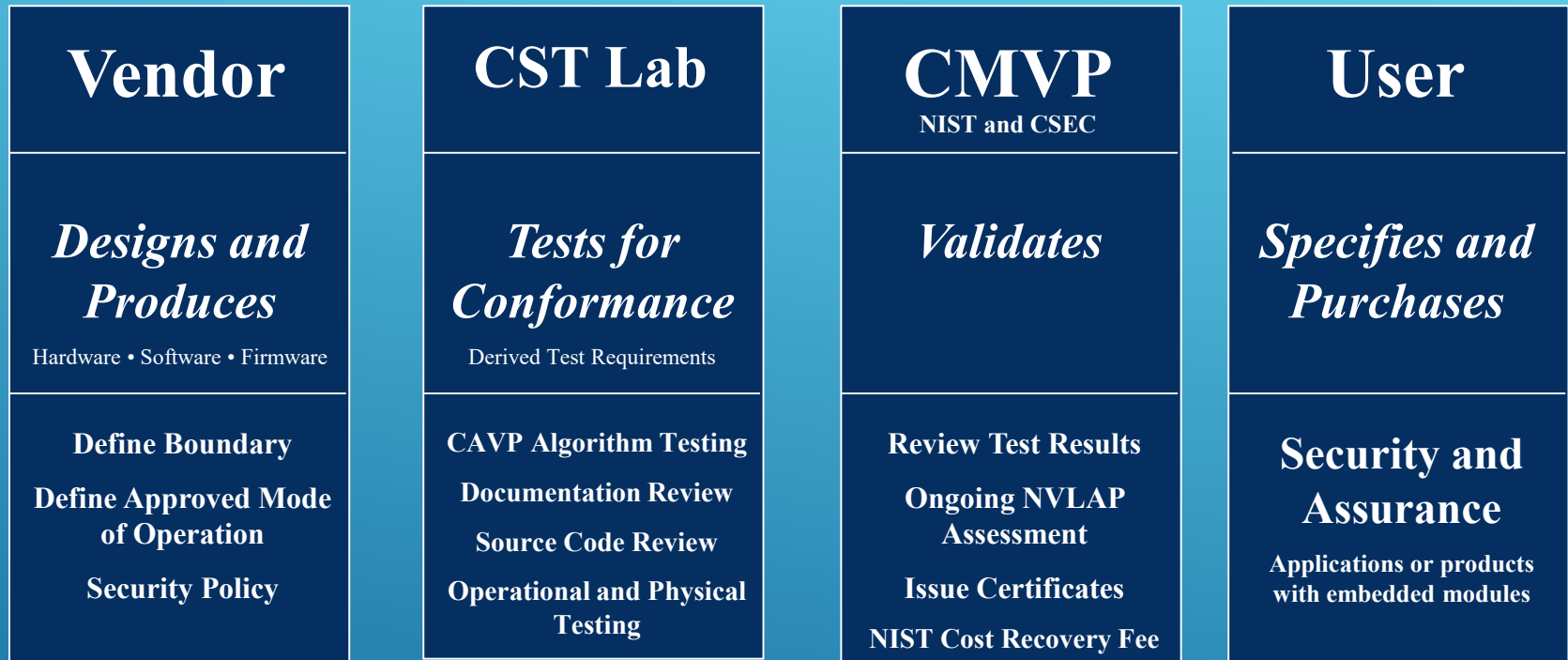
- Vendors of cryptographic modules use independent, accredited Cryptographic and Security Testing (CST) laboratories to test their modules.
- CST laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules 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.

TESTING PROGRAMS: CMVP

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



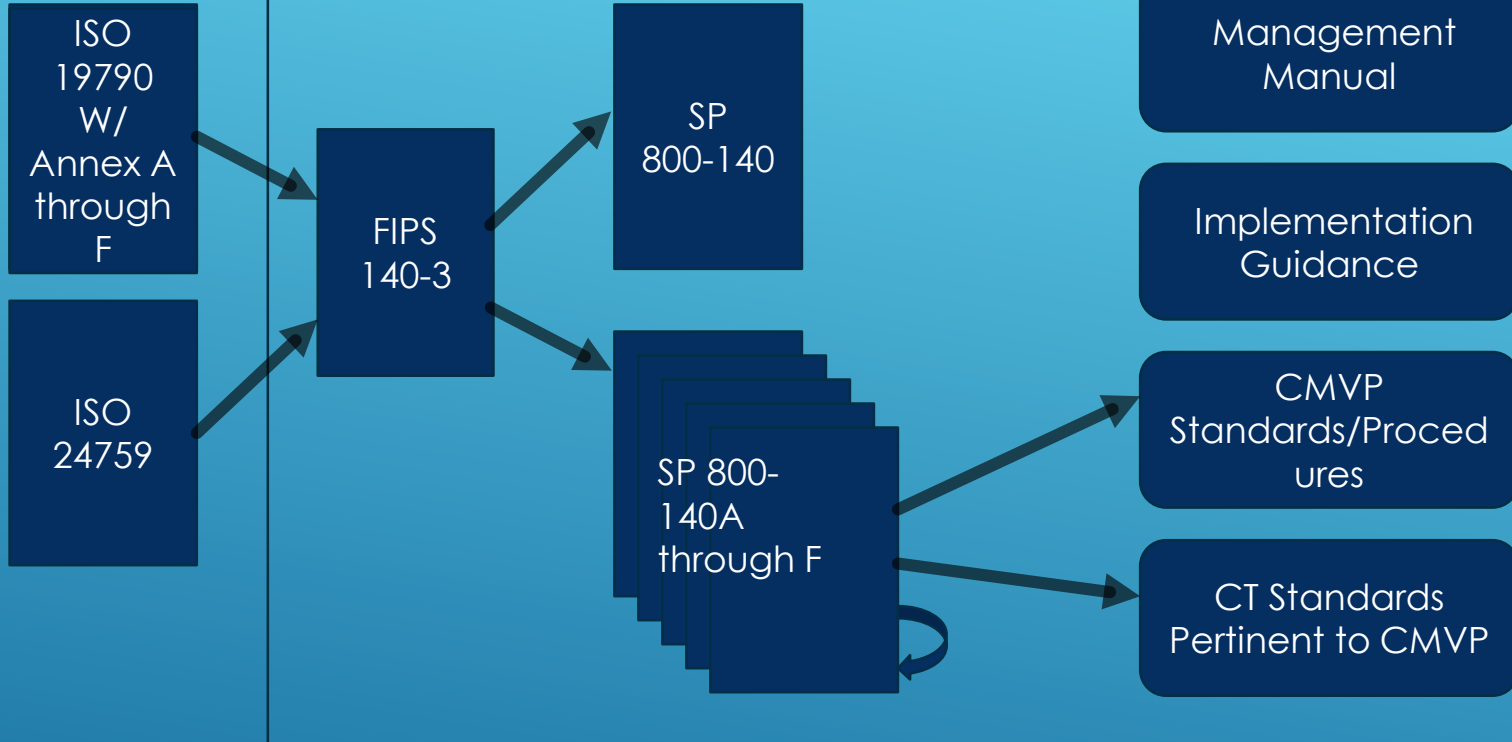
TESTING PROGRAMS: CMVP

▶ 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*

FIPS 140-3 / ISO 19790

CMVP FIPS 140-3 Program Documents



▶ **SP 800-140x documents**

▶ <https://csrc.nist.gov/Projects/fips-140-3-transition-effort/transition-to-fips-140-3>

- ▶ *SP 800-140 - FIPS 140-3 Derived Test Requirements (DTR)*
- ▶ *SP 800-140A - CMVP Documentation Requirements*
- ▶ *SP 800-140B - CMVP Security Policy Requirements*
- ▶ *SP 800-140C – CMVP Approved Security Functions*
- ▶ *SP 800-140D – CMVP Approved Sensitive Security Parameter Generation and Establishment Methods*
- ▶ *SP 800-140E – CMVP Approved Authentication Mechanisms*
- ▶ *SP 800-140F - CMVP Approved Non-Invasive Attack Mitigation Test Metrics*

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

TESTING PROGRAMS: CMVP

FIPS 140-3 CURRENT STATUS

- ▶ 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

TESTING PROGRAMS: CAVP

ENTROPY TESTING

- ▶ 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.
- ▶ POC – Apostol Vassilev – Security Testing Research Team Lead.

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



- ▶ 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

NIST CONTACTS