PROJECT DESCRIPTION

AUTOMATION OF THE CRYPTOGRAPHIC MODULE VALIDATION PROGRAM (CMVP)

Apostol Vassilev
Chris Celi
Gavin O'Brien
Murugiah Souppaya

Information Technology Laboratory
National Institute of Standards and Technology

William Barker

Dakota Consulting

DRAFT

April 2021

applied-crypto-testing@nist.gov

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov/.

This document describes how automation can help address the challenges of the NIST Cryptographic Module Validation Program (CMVP). It outlines an approach for demonstrating proposed solutions built in collaboration with a Community of Interest, cryptographic product vendors, product testing organizations, and product validation staff.

Abstract

The NIST NCCoE is initiating a project to demonstrate the value and practicality of automation support for the Cryptographic Module Validation Program (CMVP). The outcome of the project is intended to be improvement in the efficiency and timeliness of CMVP operation and processes. This effort is one of a series of activities focused on automation of CMVP testing and data flow, and it follows the successful completion of the automation of the Cryptographic Algorithm Validation Program (CAVP), the automation of the processing of the cryptographic testing evidence, and the rollout of Web CRYPTIK, an application for submitting results to the CMVP. This project description documents the project background, a proposed scenario to be demonstrated, a high-level demonstration platform architecture with a list of desired components, and standards and guidance to be followed in project development and execution. The results of the demonstration project will inform the operational integration and deployment of automation in the NIST CMVP.

Keywords

automated cryptographic validation (ACV); Automated Cryptographic Validation Protocol (ACVP); Cryptographic Algorithm Validation Program (CAVP); Cryptographic Module Validation Program (CMVP); cryptography; first-party testing; Implementation Under Test (IUT); National Voluntary Laboratory Accreditation Program (NVLAP); third-party testing

Disclaimer

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

Comments on NCCoE Documents

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov/.

Comments on this publication may be submitted to applied-crypto-testing@nist.gov

Public comment period: April 12, 2021 to May 12, 2021

TABLE OF CONTENTS

1 Executive Summary

Purpose

The Cryptographic Module Validation Program (CMVP) validates third-party assertions that cryptographic module implementations satisfy the requirements of Federal Information Processing Standards (FIPS) Publication 140-3, *Security Requirements for Cryptographic Modules* [1]. Current industry cryptographic product development, production, and maintenance processes place significant emphasis on time-to-market efficiency. A number of elements of the validation process are manual in nature, and the period required for third-party testing and government validation of cryptographic modules is often incompatible with industry requirements.

The purpose of the project is to demonstrate the value and practicality of automation to improve the efficiency and timeliness of CMVP operation and processes. This effort is the complement to the automated Cryptographic Algorithm Validation Program (CAVP). The ultimate goal of this initiative is to provide mechanisms for testing by National Voluntary Laboratory Accreditation Program (NVLAP) accredited parties, to include first parties such as product/service providers and third parties such as independent testing laboratories. It will include automated tests for each of the test requirements found in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 24759 at all four security levels.

However, because of the large scope of the technologies and the corresponding security requirements the CMVP covers, this effort will be scaled into sequential phases. Each phase will cover specific, well-defined parts of the program. This project description details the initial phase, which involves foundational work needed for all subsequent phases.

Scope

The project will demonstrate a suite of tools to modernize and automate manual review processes in support of existing policy and efforts to include technical testing of the CMVP. These automated tools will employ a vendor/manufacturer testing concept that permits organizations to perform the testing of their cryptographic products according to the requirements of FIPS 140-3, then directly report the results to NIST using appropriate protocols. This means that participating organizations will have to identify corresponding personnel and organizational structures needed to perform this testing while complying with the laboratory requirements for testing programs established by NVLAP under NIST Handbook (HB) 150-17 [2].

NIST has already developed such requirements for organizations that participate in the automated CAVP in Annex G of HB 150-17. NIST will extend first-party requirements in NIST HB 150-17 to cover the scope of CMVP and amend existing third-party requirements in collaboration with industry and the laboratories. Collaborators in the CMVP automation demonstration project will participate in the development of these requirements to ensure they meet current best practices for the industry, including requirements to routinely update and evolve an environment to maintain a secure posture.

The project will address the following considerations:

- develop the necessary schemas and protocols for evidence submission and validation for a scalable application programming interfaces (APIs) based architecture

- design and develop an infrastructure required to support a new automated validation program architecture
- provide reusable test harnesses for test automation for different types of modules within the program architecture
- maintain validation within a changing operational environment
- perform validation in third-party operational environments (e.g., cloud providers, contracted environments)
- identify positive and negative impacts that the new automation program may have on cryptographic product development, production, integration, and testing organizations, including lessons learned
- recommend policies and best practices for the automated validation scope in appropriate NIST documents
- recommend a roadmap for migrating organizations and their customers from the current human-effort-centric CMVP to the new automated program, including recommended practices based on lessons learned

This project will focus on operational, real-world automation tools. The solution may utilize proprietary vendor products as well as commercially viable open-source solutions. The project will also include practice descriptions in the form of white papers, playbook generation, and implementation demonstrations, which aim to improve the ability and efficiency of organizations.

The project will focus on creating first-party and third-party tests and test tools for automation of CMVP, as well as first-party processes and means for communicating the results to NIST in a form that conforms to module validation requirements. (Note that the existing third-party processes will continue.) The project will leverage current and future NIST and industry guidelines and projects. The project will adopt the current and future relevant standards and guidance documents. Section 4 provides examples of relevant standards and guidance.

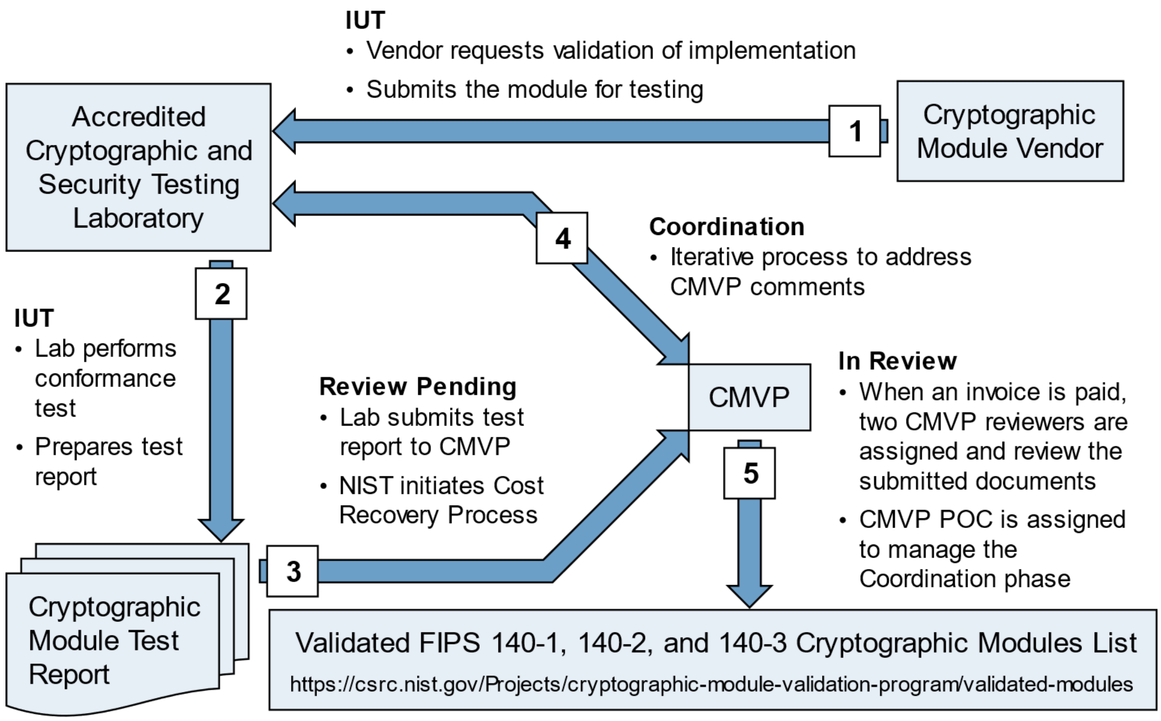
The project will also specifically address the need to routinely update the module operating environments to maintain a secure state while also maintaining the relying module validation status. Because organizations' environments may be in a state of constant evolution to maintain a secure posture, the cryptographic validation processes need to align with the pace of change of this ecosystem. Automation and process improvement will be areas of focus to achieve this.

Assumptions/Challenges

To assess the security aspects related to real hardware and software cryptographic implementations, NIST and the Canadian Centre for Cyber Security (CCCS) established the CMVP in 1995 to validate cryptographic modules against the security requirements in FIPS 140-1. The CMVP is run jointly with the Government of Canada for the benefit of the federal agencies in the US and Canada, but the actual impact of this program is much wider. Many other industry groups and local governments in the US, Canada, and other countries also rely on it.

The existing CMVP leverages independent testing laboratories to test commercial-off-the-shelf cryptographic modules supplied by industry vendors. The structure and process of the current CMVP are illustrated in Figure 1. Testing utilizes manual techniques, and validation relies on human-readable test reports in the form of English language essays.

Figure 1: Current CMVP Process



As technology progresses and cryptography becomes ubiquitous in the information infrastructure, the number and complexity of modules to be validated increase. The plethora of cryptographic module validations has outstripped available human resources for vendors, labs, and validators alike. When evaluation package submissions finally reach the validation queue, inconsistent and possibly incomplete evidence presentation further strains the ability for a finite number of validators to provide timely turnaround. Additionally, security and compliance requirements for the environments in which modules operate mandate routine updates, which further stresses the validation program and creates a drift between module validation state and a secure operating environment. Finally, automation that can be integrated into the development process of cryptographic modules and their corresponding products will improve time-to-market for government users.

It is expected that the majority of the demonstration architecture components will be located in a lab at the NCCoE facility in Rockville, Maryland or hosted in the cloud. This will ease the integration of the components and allow an open and transparent environment for the participants to collaborate remotely on building and testing the environment.

Background

Current industry and government cybersecurity recommendations state that organizations should patch promptly, including application of patches to update cryptographic modules. Technology products are highly complex, and the cost of testing them fully to guarantee trouble-free use is prohibitively high. As a result, products contain vulnerabilities that attackers and the companies providing the products are competing to discover first: for the companies to fix, and for the attackers to exploit. Patching products change the game for attackers and slow down their progress. Thus, patching promptly is a way of staying ahead of the attackers.

However, patching also changes the environment in which a cryptographic module runs and may also change the module itself, thus invalidating the previously validated configuration. Federal users and others who depend on validated cryptography face a dilemma when frequent updates and patches are important for staying ahead of the attackers, but the existing CMVP validation process does not permit rapid implementation of these updates while maintaining a validated status.

2 Demonstration Scenario

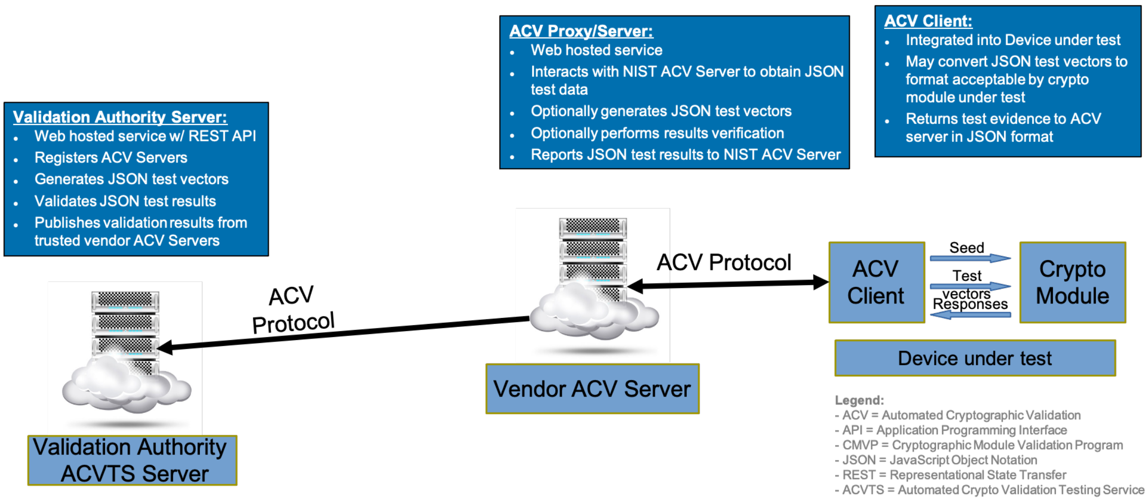
The CMVP automation project scenario for the initial phase of the project includes:

- identifying an appropriate project scope that would allow successful completion of objectives within the timeline of the project:
  - automation of software module validation at level 1
  - the reporting infrastructure for modules in the cloud, due to the significant progress made in specifying the protocols and infrastructure required for supporting validations of modules in the cloud
- developing data schema that would enable the generation and validation of standardized evidence produced by the operational testing of an Implementation Under Test (IUT) executing on a Device Under Test (DUT) within the selected subordinate project scope
- developing protocols for submitting evidence and receiving comments and results based on that evidence for the selected subordinate project scope
- developing capabilities that associate Automated Cryptographic Module Validation Protocol (ACMVP) evidence with other evidence, such as the cryptographic algorithm validation data produced using the Automated Cryptographic Validation Protocol (ACVP), that would enable the complete and verifiable representation of an IUT
- leveraging the ACVP to the greatest extent possible to maintain a consistent system architecture
- leveraging the data model established in the recently developed Web CRYPTIK prototype [3], with possible enhancements to improve data traceability and verification. Examples of cryptographic mechanisms for the latter are shown in the early schema proposal by industry.
- leveraging the data model and protocols for the new CMVP entropy source validation (ESV) service
- developing implementation validation tools and services to enable an end-to-end validation scope for the CMVP, for the selected subordinate project scope
- updating the processes and procedures used by developers, implementers, validators, and consumers of validated implementations for the selected subordinate project scope. This should include lessons learned and recommendations for best practices.

3 High-Level Architecture

This section provides a high-level illustration of the demonstration architecture and a list of the components that are part of the architecture. Figure 2 provides a logical depiction of the proposed demonstration implementation.

Figure 2: Demonstration Architecture for Future CMVP Process

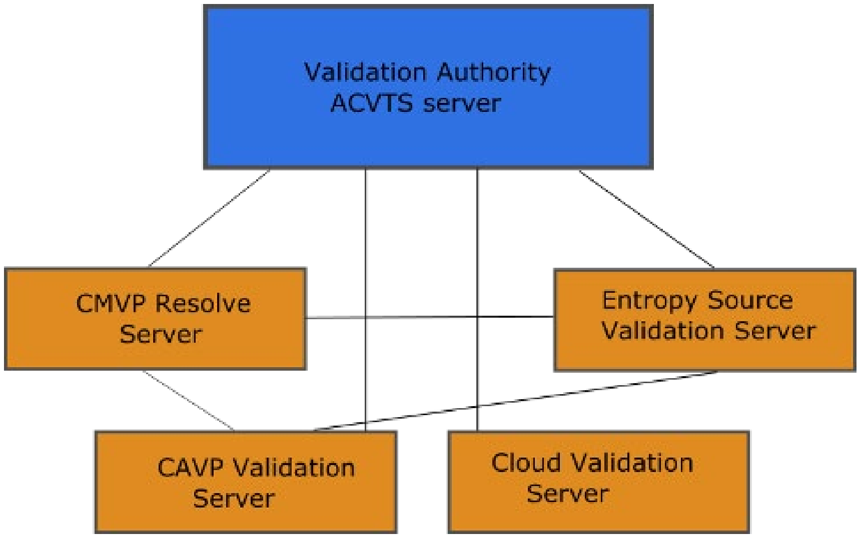


Architectural components will include the following:

- **Validation authority ACTVS server**. It will provide a web-hosted service with a Representational State Transfer (REST) API. It will also register automated cryptographic validation (ACV) servers, receive evidence, communicate feedback, validate module test results using JavaScript Object Notation (JSON), and publish validation results from trusted vendor ACV servers. The ACVTS server will act as a front-end server for the family of Validation Authority Servers handling different parts of the validation (CAVP Server, CMVP Resolve Server, ESV Server, Cloud Validation Server, etc.) – see Figure 3 below. A goal of this project is to define a mechanism for interacting with the different services using a unified protocol and a single point of contact (the ACVTS server) that will delegate the appropriate portions of the payload to the corresponding service. The front-end server will permit access only to trusted ACV servers and thus allow the subordinate service components to not be burdened by authentication. Currently, the three known service components are accessible directly from the internet. Over time, along with the definition of the protocol and the corresponding data schema, it is expected that these servers will transition behind a firewall and no longer be accessible directly from outside. Only the ACVTS server will remain accessible to accredited laboratories.
- **One or more vendor ACV proxy servers**. ACV proxy servers will provide a Web-hosted service and interact with a NIST validation authority server to exchange module test results. The proxy servers may optionally perform results verification, and they will report module test results to a NIST validation authority server.
- **DUTs that include both an ACV client and cryptographic modules**. The ACV client will be integrated into a DUT. The ACV client may request JSON schema test requirements in a form usable by a cryptographic module under test, and will return test results to an ACV server in JSON format.

Communications between these components will employ a protocol based on the ACVP used by the CAVP.

Figure 3: Validation Authority Server Architecture



Transport of test results will be based on using HTTPS to carry an encoding and message format, which is negotiated, and a set of message exchanges. The platform will be designed to work over the internet where the testing system is remote from the cryptographic module.

The platform will enable discovery of the capabilities of the module being tested and generate corresponding tests. It will also enable the request/response exchanges between the testing server and the tested module, and provide a standard communication method. The platform should also provide extensibility that can be used to introduce new tests for module validation and new protocol features without changing tests.

Component List

- Validation authority server
- ACV proxy server
- ACV client
- Hardware or software cryptographic modules
- Host processors for software cryptographic modules
- Network devices supporting web-based exchange of information in JSON format
- Harnesses for integration of ACV clients with hardware or software cryptographic modules
- Automated cryptographic module testing expertise

4 Relevant Standards and Guidance

Here is a list of existing relevant standards and guidance documents.

- Federal Information Processing Standards (FIPS) 140-3, *Security Requirements for Cryptographic Modules*, https://doi.org/10.6028/NIST.FIPS.140-3
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19790:2012(E), Information technology — Security techniques —

Security requirements for cryptographic modules, https://www.iso.org/standard/52906.html

- ISO/IEC 24759:2017(E), Information technology — Security techniques — Test requirements for cryptographic modules, https://www.iso.org/standard/72515.html
- NIST Handbook (HB) 150-17, *NVLAP Cryptographic and Security Testing*, https://doi.org/10.6028/NIST.HB.150-17-2020
- NIST Special Publication (SP) 800-52 Rev. 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, https://doi.org/10.6028/NIST.SP.800-52r2
- NIST SP 800-140A, *CMVP Documentation Requirements: CMVP Validation Authority Updates to ISO/IEC 24759*, https://doi.org/10.6028/NIST.SP.800-140A
- NIST SP 800-140B, *CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B*, https://doi.org/10.6028/NIST.SP.800-140B
- NIST SP 800-140C, *CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759*, https://doi.org/10.6028/NIST.SP.800-140C
- NIST SP 800-140D, *CMVP Approved Sensitive Security Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759*, https://doi.org/10.6028/NIST.SP.800-140D
- NIST SP 800-140E, *CMVP Approved Authentication Mechanisms: CMVP Validation Authority Requirements for ISO/IEC 19790 Annex E and ISO/IEC 24759 Section 6.17*, https://doi.org/10.6028/NIST.SP.800-140E
- NIST SP 800-140F, *CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759*, https://doi.org/10.6028/NIST.SP.800-140F
- NIST SP 1800-16, *Securing Web Transactions: TLS Server Certificate Management*, https://www.nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management
- NIST SP 1800-19, *Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments*, https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud/hybrid

Appendix A References

[1] U.S. Department of Commerce. *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards (FIPS) Publication 140-3, Mar. 2019, 11 pp. https://doi.org/10.6028/NIST.FIPS.140-3

[2] B. W. Moore, B. Trapnell, J. Fox, and C. French, National Institute of Standards and Technology Handbook 150-17, *NVLAP Cryptographic and Security Testing*, Apr. 2020, 86 pp. https://doi.org/10.6028/NIST.HB.150-17-2020

[3] National Institute of Standards and Technology and Canadian Centre for CyberSecurity, Draft *FIPS 140-3 Cryptographic Module Validation Program Management Manual, Version 1.0*, Sep. 2020, 97 pp. https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual

Appendix B Acronyms and Abbreviations

ACMVP	Automated Cryptographic Module Validation Protocol
ACV	Automated Cryptographic Validation
ACVP	Automated Cryptographic Validation Protocol
ACVTS	Automated Cryptographic Validation Testing Service
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CCCS	Canadian Centre for Cyber Security
CMVP	Cryptographic Module Validation Program
DUT	Device Under Test
ESV	Entropy Source Validation
FIPS	Federal Information Processing Standards
HB	Handbook
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IUT	Implementation Under Test
JSON	JavaScript Object Notation
KAT	Known Answer Test
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
REST	Representational State Transfer
SP	Special Publication
TLS	Transport Layer Security