NIST SPECIAL PUBLICATION 1800-40A

Automation of the NIST Cryptographic Module Validation Program

Volume A:
Executive Summary

Apostol Vassilev
Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

William Barker
Dakota Consulting
Silver Spring, MD

June 2023

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/automation-nist-cryptographic-module-validation-program

Executive Summary

NIST established the Cryptographic Module Validation Program (CMVP) to ensure that hardware and software cryptographic implementations conform to specified standard security requirements. This is a joint program with the Government of Canada. Since its start, the volume, complexity, and speed-to-market of modules to be tested and validated has steadily increased. The rapid pace of industry innovation, release cycle of cloud services, and cryptographic module fixes and patch releases now outstrips available human resources for product vendors, labs, and validators.

We also live in times of unprecedented levels of threats and exploits that require deploying the latest technology and frequent product updates to fix defects and remove security vulnerabilities--that doesn't fit in the current CMVP workflows and processes.

This limits product options for many organizations required to use validated cryptography, especially federal agencies. NIST has started a broad effort to modernize and automate all aspects of the CMVP.

This guide summarizes how the National Cybersecurity Center of Excellence (NCCoE) and its collaborators are developing a schema, protocols, and technology to create standardized tests and mechanisms for test evidence submission as part of automation of CMVP. As the project progresses, this preliminary draft will be updated, and additional volumes will also be released for comment.

The primary goal of the completed guide will be to integrate the developed application, process, and protocols into the NIST CMVP to help the test labs, technology producers, and validation authorities leverage this modern approach to shorten the validation cycle while maintaining and improving the level of assurance. The guide will help the CMVP community to stay informed and understand the approaches and changes that will be made to the program.

CHALLENGE

The CMVP validates first and third party test laboratory assertions that cryptographic module implementations satisfy the requirements of Federal Information Processing Standards (FIPS) Publication 140-3, *Security Requirements for Cryptographic Modules*. Module testing and reporting is conducted in accordance with International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 24759 as specified and constrained by the NIST Special Publication 800-140 series, and combines reporting of both functional and nonfunctional security requirements. Current industry cryptographic product development, production, and maintenance processes place significant emphasis on time-to-market efficiency while also striving to deliver quality and security. A number of elements of the test and validation process are manual in nature and use nonstandard tests and test evidence, and the period required for laboratory testing and government validation of cryptographic modules is often incompatible with industry and customer requirements. This process can take up to two years; industry may have several innovative releases in that time frame that are backlogged for validation due to the current process.

OUTCOME

The outcome of this project is to develop a proof of concept to include a CMVP test and validation service; a set of structured tests, schema, and protocols for evidence submission; a repeatable approach

for testing, including cloud-based testing; and corresponding computing infrastructure to automate the validation of FIPS 140-3 security requirements for cryptographic modules. The developed code, schema and protocol specifications, supporting documentation, and findings will be published in this practice guide, a NIST Special Publication (SP) 1800 that is composed of multiple volumes.

This preliminary practice guide can help your enterprise organization, e.g., Federal Agencies:

- understand the value and practicality of automation to improve the efficiency and timeliness of CMVP operation and processes
- understand the considerations associated with decisions regarding a potential future ability to perform first-party testing, such as with product/service providers

This preliminary practice guide can help CMVP test labs and vendors:

- understand the value and practicality of automation to improve the efficiency and timeliness of CMVP operation and processes
- learn about the automation of the test report format and protocols for exchanging test evidence
- leverage sample code to develop their own client to interface with the developed test server
- replicate and host their own test environment using the architecture and supporting content

SOLUTION

NCCoE is currently collaborating with technology providers on finalizing the demonstration architecture to show the value and practicality of automation for improving 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. Ideally, the project would lead to standardized tests and a schema for test evidence submission where feasible for each of the test requirements found in ISO/IEC 24759 at all four security levels.

Because of the large range of the technologies and the corresponding security requirements the CMVP covers, this project will be executed in phases. The initial project phase is for software module validation at security level 1, which is foundational and will inform future phases. This activity demonstrates an evidence catalog that maps test evidence (TE) references to specific TEs and a schema for standardized evidence submission for the validation testing of cryptographic software modules. The demonstration includes a suite of tools for modernizing and automating manual review processes in support of existing policy and efforts, including technical acceptance testing. The demonstration also includes a cloud-based approach to automate the manual review processes.

These automated tools integrate in common vendor/manufacturer testing processes that permit organizations to test their cryptographic products according to the requirements of FIPS 140-3, then directly report the results to the NIST validation server using appropriate protocols and obtain certificates of compliance. Participating organizations will identify personnel and organizational structures needed to perform this testing and report results to the CMVP to comply with the laboratory requirements for testing programs established by NVLAP under NIST Handbook (HB) 150-17. The accreditation requirements in HB 150-17 are hierarchical and compositional in nature so that organizations can tailor the scope of accreditation according to their specific product/service portfolio.

Collaborators		
Acumen Security	atsec	Microsoft Corporation
AEGISOLVE	Cisco	NXP Semiconductors
Amazon Web Services (AWS)	Cloudflare	SUSE
Apple	Lightship Security	

While the NCCoE will use a suite of commercial and open source products to address this challenge, this guide does not endorse particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security officers, product managers, test laboratory managers, and technology officers can use this part of the guide, *NIST SP 1800-40A: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Other roles including technology, security, and privacy program managers and architects and software developers, engineers, and IT professionals may find value in this Executive Summary, as well as future releases of this publication which will include greater details about the approach and technical implementation information.

SHARE YOUR FEEDBACK

You can view or download the preliminary draft guide at the Automation of the NIST Cryptographic Module Validation Program project page. NIST follows an agile process to publish this content. Each volume is made available as soon as possible rather than delaying release until all volumes are completed. Work continues on designing and implementing the example solution and developing other parts of the content. As a preliminary draft, this volume will have at least one additional draft released for public comment before it is finalized.

Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. Once the example implementation is developed, you can adopt this solution for your own organization. If you do, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and recommended practices for transforming the processes associated with implementing this guide.

To provide comments or join the CMVP Automation community of interest, contact the NCCoE at applied-crypto-testing@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.