

Status of the Automaton of NIST Cryptographic Validation Programs

How it all started?

Initiated an Industry Working Group in December 2015

a mix of industry and government participants

17 companies and Open-Source entities, 2 Govt. agencies

organized in several working areas led by industry participants

Made (uneven) progress towards the desired goals

1. Automated algorithm validations
(defacto) a joint effort between Cisco and NIST, later joined by atsec (Stephan M.)
2. Accreditation requirements for 1st- party labs
3. Validation methodology for modules in the cloud
AWS put forward a promising concept
4. Automated module validations
schema for data submission – proposal by Google

Where are we now?



- 1. Completed and delivered ACVP**
transitioned to production w/ [adoption by CAVP](#) in 2019
mandatory to use as of September 30, 2020
NIST server [architecture and implementation](#) underwent many iterations
stable and efficient, keeps improving
substantial and growing [coverage of testing](#) of approved algorithms
- 2. Completed and delivered an accreditation scope for algorithm testing**
published in [NVLAP HB 150-17](#), Annex G
available to **1st-party** testing laboratories, **3rd-party** labs grandfathered,
first successful accreditation of a **1st-party** lab completed in Sept. 2020!

Where are we now?



3. Development of validation methodology for modules in the cloud was put on hold

as of mid-summer 2019, the working group had developed a solid draft, a good candidate to revive quickly

4. Automation of cryptographic module validations paused

as of mid-summer 2019

a preliminary schema for test evidence submission provided (Google)

... plenty of downtime to reflect and plan

What lessons we learned?

- 1. Automation is powerful but hard to sell**
impressive results with ACVP demonstrated at ICMC 2020
early expectations far exceeded
... but to get here had to overcome strong early opposition
especially about 1st-party testing
- 2. The initial development model is inefficient and risky**
ad-hoc working groups w/ loose structure and vague commitments
do not work for large and complex problems

What is the challenge now?

The plethora of cryptographic module validations has proven to outstrip available human resources for Vendors, Labs and Validators alike.

So, there exists a dire need for consistent and reproducible evidence generation, reporting, and processing of cryptographic module validations **at machine speed.**

Project objectives

1. Develop **schemas** and **protocols** for test evidence submission and validation open, allowing independent implementation by all stakeholders
2. Develop **standard testing methodologies** for classes of technologies against FIPS 140-3 requirements
similar to NIAP PP's
including **cloud environments**, based on existing proposal
3. Develop a **system** w/ services using the schemas and protocols to enable automated validation of cryptographic modules based on standardized testing
leverage the available ACVP infrastructure to the extent possible
4. Develop commensurate **accreditation scopes** for NVLAP HB 150-17
available to 1st- and 3rd-party laboratories alike

The background of the slide is a complex, abstract composition. It features a light gray grid with various geometric shapes and lines. Overlaid on this are several network diagrams. Some consist of blue dots connected by thin blue lines, while others use green dots and lines. There are also orange dots and lines. The overall effect is a sense of interconnectedness and technical complexity.

This is it. Let's do it. Thanks!