

Virtual Workshop: Transition to ACVP

Challenges and Benefits of Automated Algorithm Validation

Barry Fussell

Cisco Systems
October 2020



Agenda

- **Certification Organization**
- **CAVS vs ACVP Process Restructuring**
- **Managing the Transition**
 - Process Decisions
 - Organizational Impact
 - New roles and skill sets
 - Resource Impact



Historical Certification Organization

- **Fed Sales Team**
- **Product Developers**
- **Global Certification Team(GCT)**
- **Crypto Module Developers**
- **Third-Party Lab**



CAVS Process

- **Sales Initiates Request to Product Team**
- **Product Team works with GCT/Module Developers**
- **Schedule engagement with third-party labs**
- **Module Developers**
 - Request Vectors
 - Run Tests
 - Upload results to lab, rinse, repeat.
 - Run module tests if required.



ACVP Process Restructuring Decisions

- **First-Party lab ? If so, how ?**



ACVP Proxy

Proxy/Validation Authority Architecture

Automated Cryptographic Validation System

Validation Authority Server:

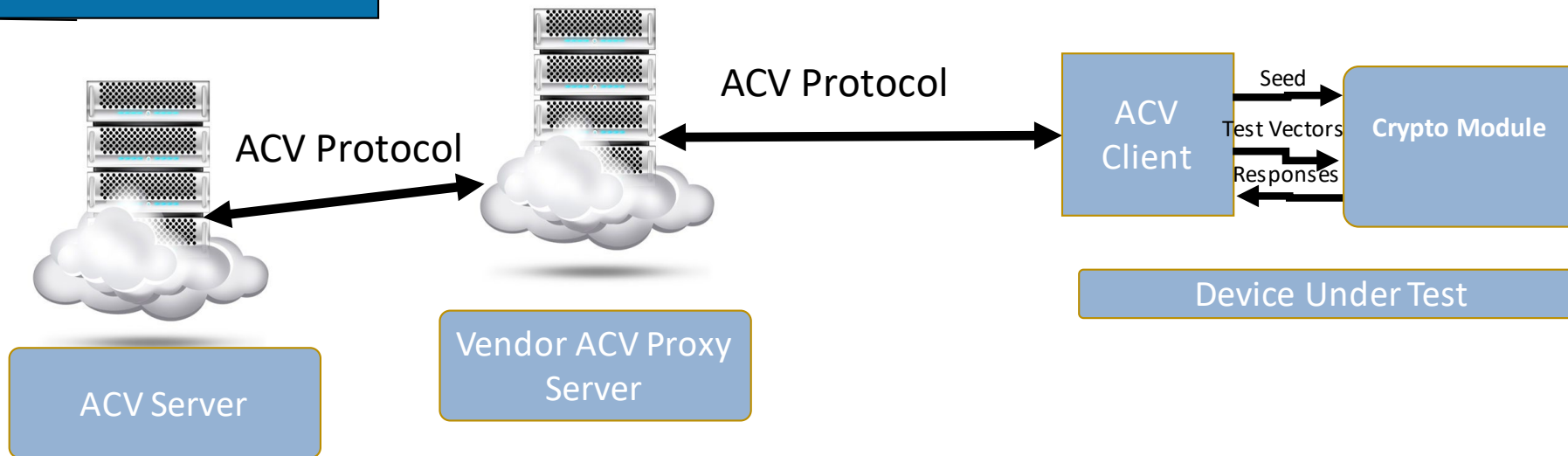
- Web hosted service w/ REST API
- Registers ACV client
- Generates JSON vectors
- Validates JSON results
- Publishes validation results from trusted vendor ACV Servers

ACV Proxy/Server:

- Web hosted service with short-lived token based authentication
- Maintains credentials
- Business Logic to control access to NIST server
- Interacts with NIST ACV Server to obtain JSON vectors
- DB for storing test evidence required by NIST
- Reports JSON results to ACV Server

ACV Client:

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



Resturcturing Decisions(continued)

- **New skill sets ?**
- **Role changes in the process?**
- **Which ACV client ?**



Resource Challenges

- **Upfront**
 - ACVP client development
 - ACVP proxy development
- **Long Term**
 - Client support and maintenance
 - Proxy support and maintenance
 - NVLAP Accreditation(lab manager)



Changes in Roles and Skill Sets

Module Developers – Technology switch from CAVS test harness to libacvp. We still run algorithm and module testing for our FOM FIPS validations.

Global Certification Team(GCT) – Now runs all incremental algorithm tests. Had to learn to build and run ACV app for various targets. Had to learn ACV Server validation operational flow. Hired a lab manager.

Product Developers – Majority had no real impact

ACV Proxy Team(new) – Responsible for proxy maintenance and support.



ACVP Process

- **Sales Initiated Request**
- **Product Team works with GCT**
- **GCT runs ACVP demo**
- **GCT runs ACVP production**
- **GCT requests algorithm certificate**



Benefits and Challenges after Automation

- **Cycle time for algorithm tests reduced.**
 - **Testing Time**
 - **Certificate Posting Time**
- **Registration Accuracy**
- **Vector Accuracy**
- **Failure Feedback**
- **Metadata**



Q&A

