Current Process and New Process for a Submitter

Entropy Source Validation Workshop

April 29, 2021

Chris Celi (NIST)

Outline

- Current Process
    - Entropy Assessment Tool
    - Report Submission
    - Interacting with CMVP during module submission and review
- New Process
    - Independent from module submission
    - Entropy Assessment Tool – local testing
    - Report preparation
    - Submit for review
    - Certificate listing, ESV listing could look like
    - Include ID for module process

Background

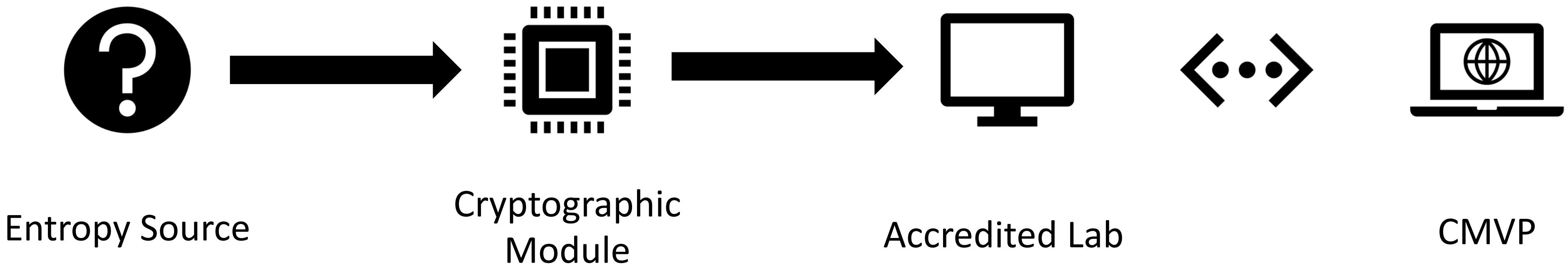
- 30% of attendees have not participated in a FIPS 140 module validation
- 52% of attendees belong to a vendor or entropy source implementor
- Since November 7, 2020, SP800-90B compliance is mandatory for FIPS 140-2 modules that utilize RBGs
  - Required since introduction of FIPS 140-3 validation process
- Entropy source validation process is a part of CMVP
- Access to the validation server will be limited to accredited labs and testers
  - A demo server will be otherwise available
- Report review is still a manual process

Outline

- How does the entropy validation process work now?

- How will this change over time? When?

Current Process



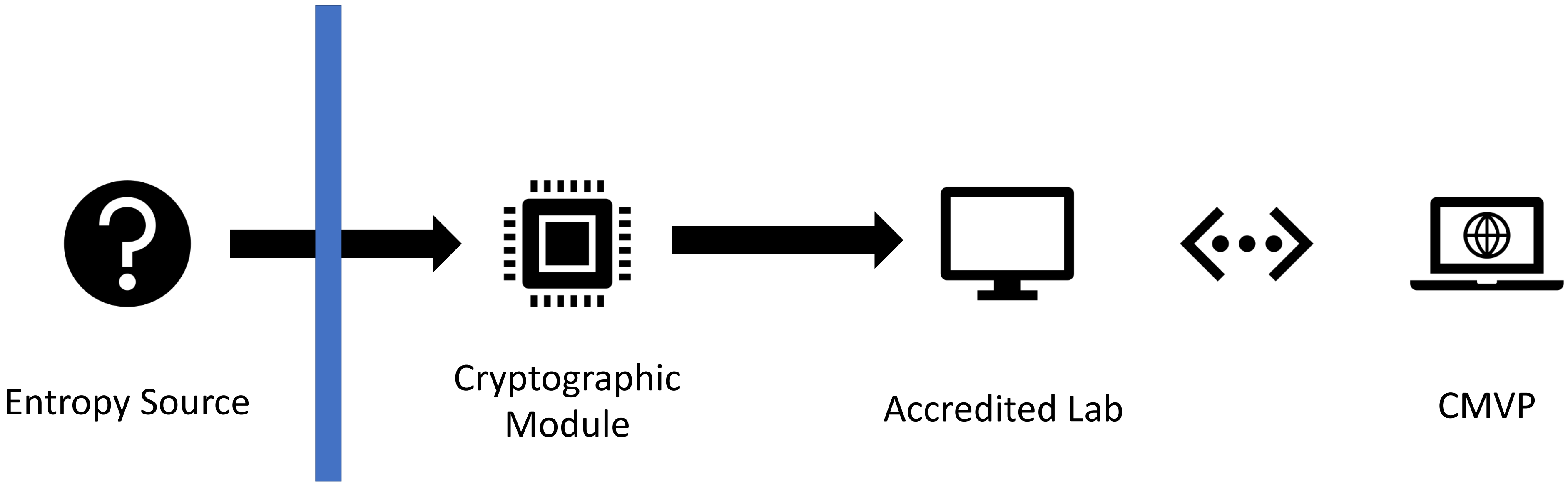
Entropy Source

Cryptographic Module

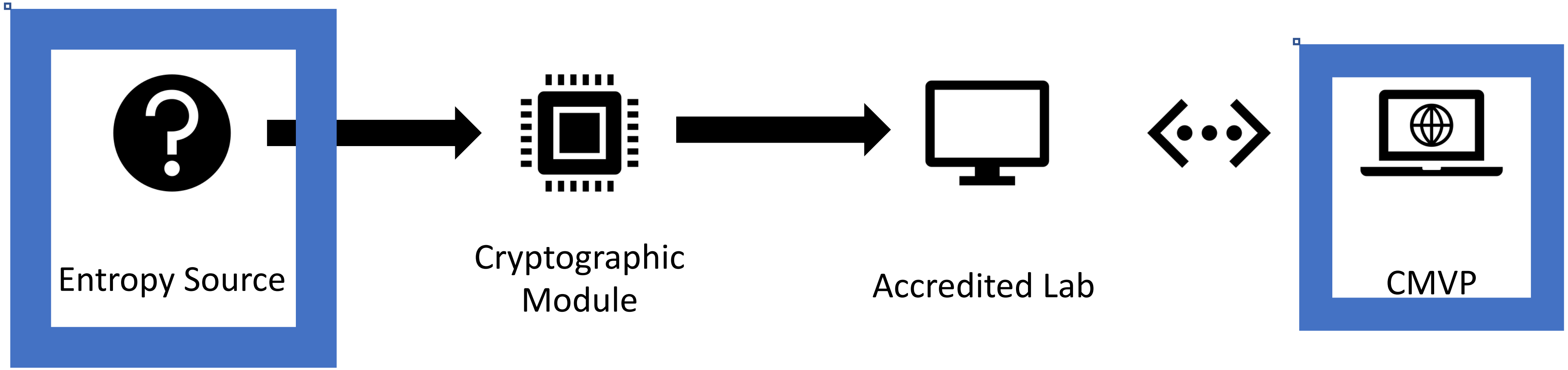
Accredited Lab

CMVP

Current Process



Current Process



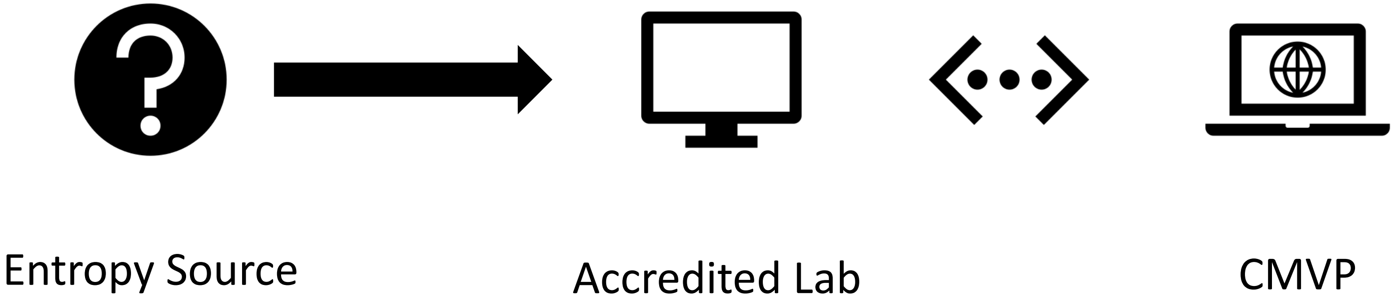
Current Process – End to End

- Lab or vendor collects data
  - SP800-90B Section 3.2.4
- Lab runs Entropy Assessment Tool
- Lab builds Entropy Assessment Report
  - Asks the vendor questions about the entropy source
- Entropy report is prepared along with module report package and algorithm testing
- Module is submitted to CMVP and all components are reviewed
- Lab interfaces with CMVP on follow-up discussions

New Process

- Depends on 17ESV NVLAP accreditation scope which outlines the requirements needed for a reviewer to submit a report
- Still going to the CMVP
- Allows for specific reviewers dedicated to entropy reports
- Not everything is certain about this process

New Process



New Process – Reports

- Entropy Assessment Reports may change shape
  - Mapping requirements to direct statements with a checklist or template
  - Different technologies may have different requirements
- Reviewers and submitters can agree on requirements and sufficient justification
- Reviewers can develop an understanding of the different technologies to consistently identify issues in a report

New Process – End to End

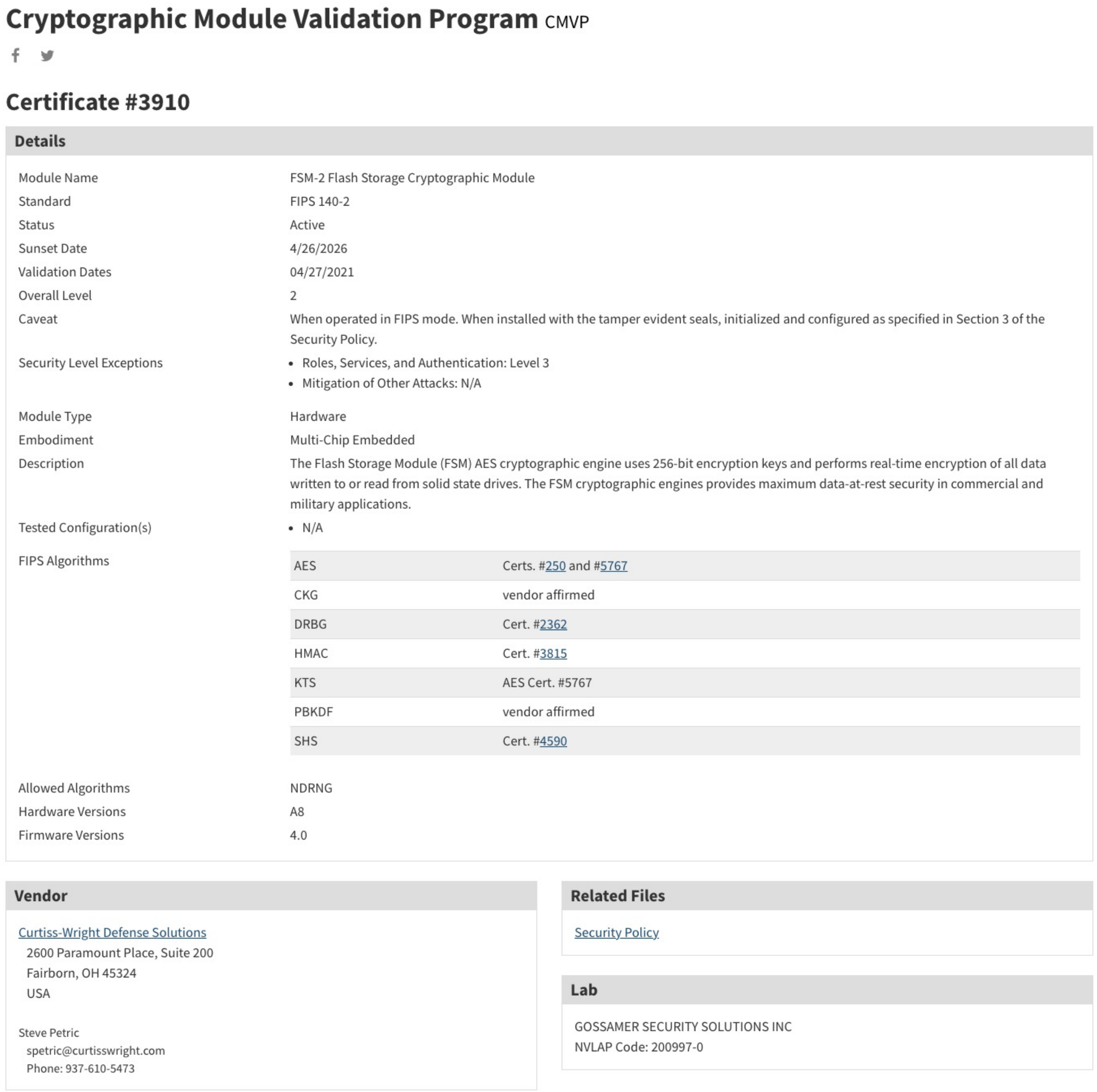
- Entropy source developer works with lab to prepare tests and documentation
- CAVP validation testing may occur through the lab
- Lab submits to CMVP through ESVTS
- CMVP reviews the report and may have questions
- Approved submissions are listed on a new Entropy Validation List with a validation number
- Validation number can be referenced during module review

New Process – Certificates

- Entropy Validation List

- Information about the entropy source
- Information about the developer
- Imagine a current module listing

New Process – Certificates



Cryptographic Module Validation Program CMVP

Certificate #3910

Details

Module Name	FSM-2 Flash Storage Cryptographic Module
Standard	FIPS 140-2
Status	Active
Sunset Date	4/26/2026
Validation Dates	04/27/2021
Overall Level	2
Caveat	When operated in FIPS mode. When installed with the tamper evident seals, initialized and configured as specified in Section 3 of the Security Policy.
Security Level Exceptions	• Roles, Services, and Authentication: Level 3 • Mitigation of Other Attacks: N/A
Module Type	Hardware
Embodiment	Multi-Chip Embedded
Description	The Flash Storage Module (FSM) AES cryptographic engine uses 256-bit encryption keys and performs real-time encryption of all data written to or read from solid state drives. The FSM cryptographic engines provides maximum data-at-rest security in commercial and military applications.
Tested Configuration(s)	• N/A

FIPS Algorithms

AES	Certs. #250 and #5767
CKG	vendor affirmed
DRBG	Cert. #2362
HMAC	Cert. #3815
KTS	AES Cert. #5767
PBKDF	vendor affirmed
SHS	Cert. #4590

Allowed Algorithms	NDRNG
Hardware Versions	A8
Firmware Versions	4.0

Vendor

Curtiss-Wright Defense Solutions
2600 Paramount Place, Suite 200
Fairborn, OH 45324
USA

Steve Petric
spetric@curtisswright.com
Phone: 937-610-5473

Related Files

Security Policy

Lab

GOSSAMER SECURITY SOLUTIONS INC
NVLAP Code: 200997-0

New Process – Module Consumption

- New considerations for modules consuming entropy validations
- Health tests must be performed and acknowledged
- Supported operating conditions must be maintained
- If the module starts up the entropy source, power-on self-tests are required for components of the entropy source
- These must be documented as part of the module validation process

Questions?