Cryptographic Algorithm Validation Program

MPTS 2023: NIST Workshop on Multi-Party Threshold Schemes 2023
9/27/2023

Chris Celi, CAVP Program Manager, NIST
christopher.celi@nist.gov

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

FIPS 140-3

- Applies to all Federal agencies that use cryptography to protect sensitive information
- Requires that cryptographic modules undergo validation testing via the Cryptographic Module Validation Program (CMVP) in order to be used by the Federal government
- The Cryptographic Algorithm Validation Program (CAVP) exists as a branch of the CMVP to perform algorithm tests on cryptographic modules

Cryptographic Algorithm Validation Program

- **CAVP is a program within NIST**
- Validation consists of conformance testing to FIPS 140 “Security Requirements of Cryptographic Modules”
- Tested algorithms listed in SP 800-140 documents

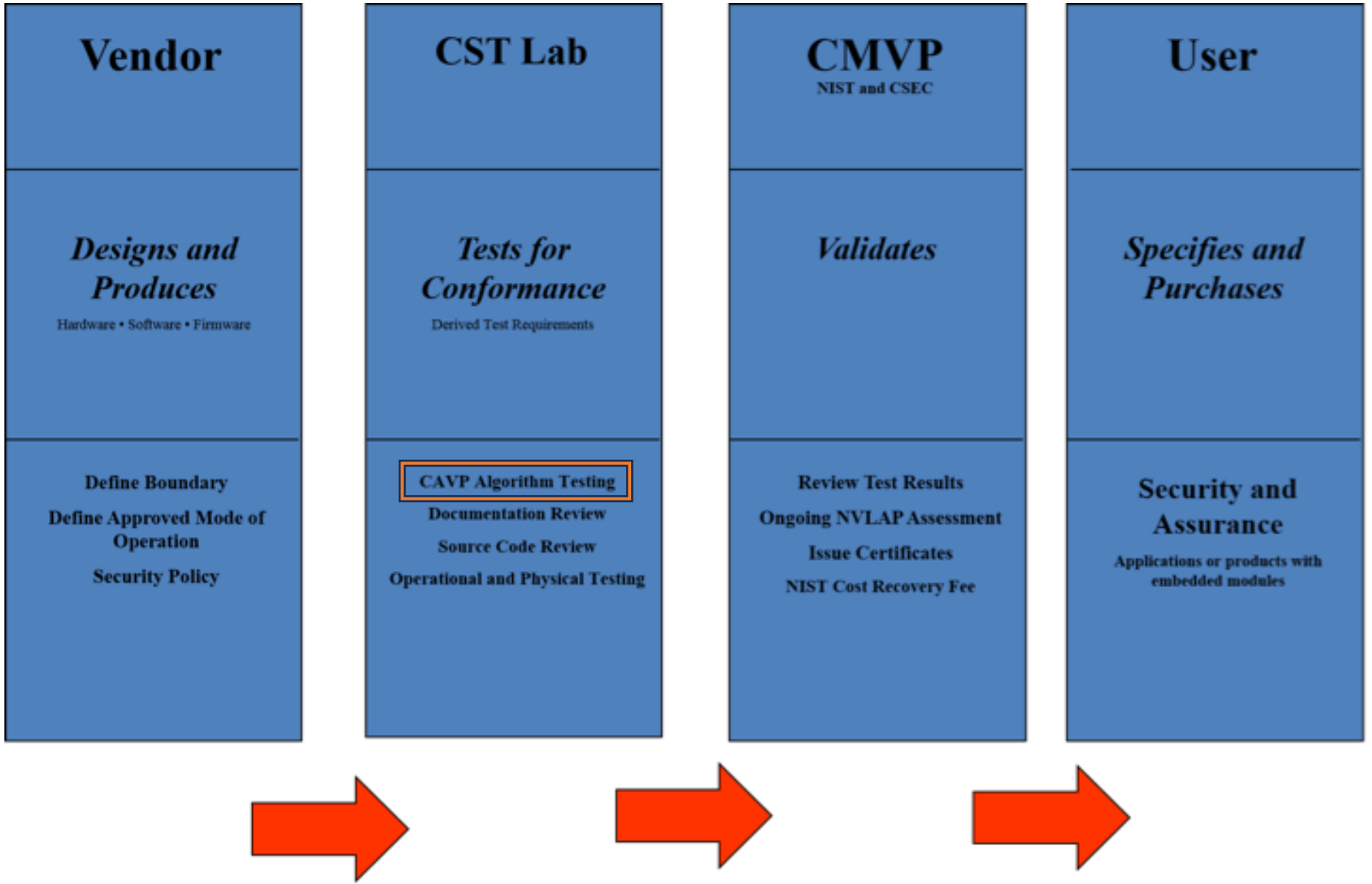
A cryptographic module is any software, hardware, hybrid, system, etc. that has at least one approved security function (cryptographic algorithm), such as encryption, authentication, digital signatures, key exchange…

Vendors, Labs, and CAVP

- Vendors of cryptographic modules use **NVLAP-accredited 17ACVT laboratories** to test their algorithms.
- First-party labs may also be **NVLAP-accredited** to **17ACVT**
- All testing happens on the NIST-hosted Automated Cryptographic Validation Test System (ACVTS)

💻 https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

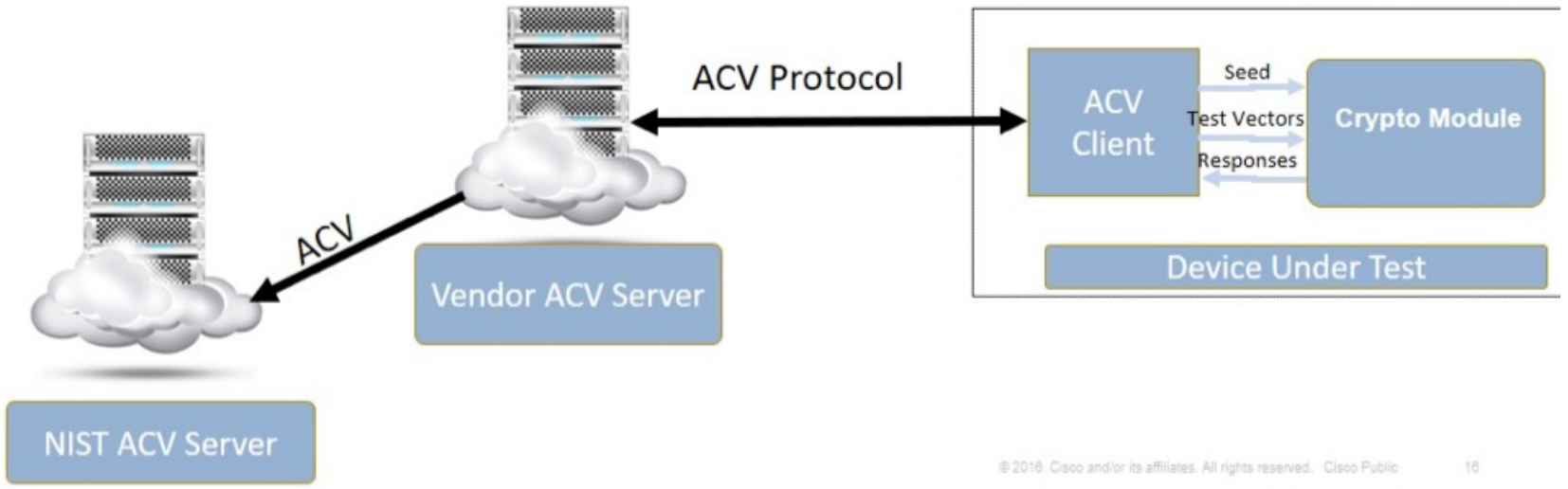
Validation Process



Algorithm Validation Process

Proxy/Validation Authority Architecture

Automated Cryptographic Validation System



Algorithm Validation Process

- NIST-hosted server called Automated Cryptographic Validation Test System (ACVTS) provides algorithm test vectors
- JSON-based communication over an API
- Tests (almost) all NIST-approved cryptographic algorithms
- Server provides inputs to a client that returns the outputs for verification

ACVTS

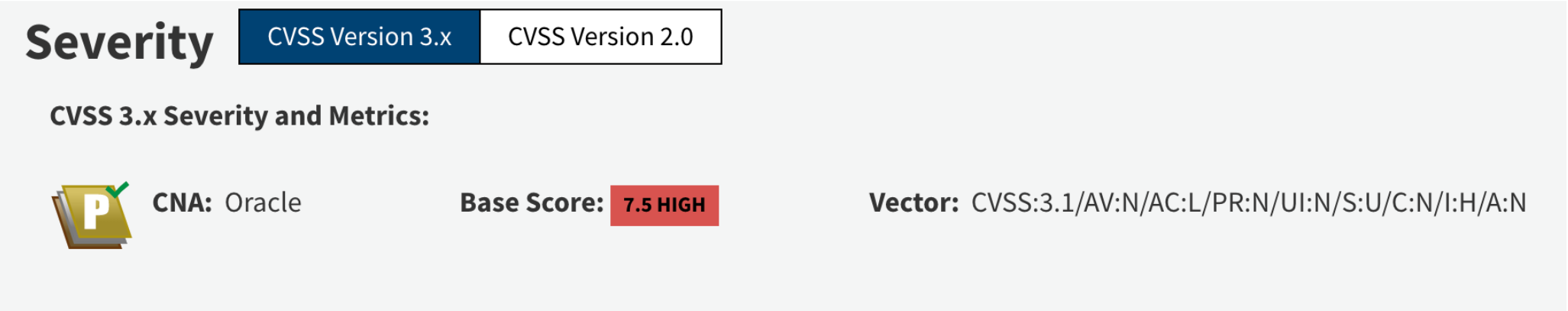
- Production Server active since 2019
  - Access limited to NVLAP-accredited 17ACVT labs
  - Pay per vector set (or unlimited for one year)

- Demo Server active since 2017
  - Access open to those who request
  - No costs
  - See https://github.com/usnistgov/ACVP for more information

- Over 1,850,000 vector sets served!

Improved Algorithm Testing

- Interested in developing tests based on CVEs
- Help the industry learn from mistakes
- CVE-2022-21449 affecting Java 15+ ECDSA signatures



Improved Algorithm Testing

- ECDSA Signatures where r = 0, and/or s = 0 would *always* pass signature verification


```
{
    "d": "28085D750F374847891B5146856923E658CC2A9EF2AA0AA6",
    "qx": "185FF9ADA4F583023CC0C4623F247761AF701F8B17391C3B",
    "qy": "282661CDE3AE6F1260EABB87CD7564C0634FCF99DD3BB44B",

    "r": "F83FAAEE8410F7FD9C8ED11461EBEA85A5D7ECDB055D4055",
    "s": "1C465A398E293C2D097CFF09EBDCD8307C207A6B515EF491"
}
```

Improved Algorithm Testing

- ECDSA Signatures where r = 0, and/or s = 0 would *always* pass signature verification

```
{
    "d": "28085D750F374847891B5146856923E658CC2A9EF2AA0AA6",
    "qx": "185FF9ADA4F583023CC0C4623F247761AF701F8B17391C3B",
    "qy": "282661CDE3AE6F1260EABB87CD7564C0634FCF99DD3BB44B",

    "r": "00",
    "s": "00"
}
```

Other Technical Details

- Can serve all algorithms very quickly, including SP 800-208 algorithms
- Cluster-based back-end is able to process many vector set requests simultaneously
- Pool system allows the cluster to continue working when no requests are present to pre-generate “harder” items so they are ready when a request comes in
- C# codebase, all generation code is open-source, including cryptographic implementations!

Conclusion

Questions?

See our GitHub
https://github.com/usnistgov/ACVP-Server

CAVP Program Manager

Chris Celi

christopher.celi@nist.gov