ACVP – About

• Web-based protocol for cryptographic algorithm testing
• Testing is done via Vector Sets that describe the individual tests a client should perform
• All requests are initiated by the client
ACVP – Testing

1. Client sends *registration* to server. Describes module capabilities.

2. Server creates a vector set *prompt* for each algorithm listed in the capabilities.

3. Client retrieves any prompt, processes and submits *responses* to server.

4. Server lists the *disposition* for retrieval. Once the full Test Session is done, the client may Certify.
ACVP – Metadata

1. Metadata objects are created through the API, separate from the testing being performed.

2. An implementation has a vendor/organization and a person responsible for the validation.

3. An operating environment describes the platform the module was tested on: CPU, OS, etc.

4. A Certify combines a Test Session with an implementation and an OE.
ACVP – Status

- Exceeded capabilities of CAVS tool
- High throughput of validations
  - Most within a few minutes end to end
- Centralized model is easy to build upon
- Demo server for testing
- Prod server for validations
ACVP – Current Goals

1. **Remove Vendor Assertion**
   - Provide testing for all approved algorithms and modes
   - Expand capabilities to accommodate for special cases

2. **Upgrade Testing**
   - Address known vulnerabilities through testing
   - Explore formal methods

3. **“Query”-able Validations**
   - Allow queries against CSRC to obtain validation records in JSON for upstream use

4. **Support Upcoming Algorithms**
   - Post-Quantum
   - Lightweight
   - Hash-based signatures
ACVP – Get Involved

GitHub
https://www.github.com/usnistgov/acvp
https://www.github.com/usnistgov/acvp-server

Research

Clients
https://github.com/cisco/libacvp
https://github.com/smuellerDD/acvpp-roxy
https://github.com/smuellerDD/acvpp-parser

Chris Celi
christopher.celi@nist.gov