Automated Crypto Validation Protocol

- Details of automated validations, assessment and the ACV Protocol
- Barry Fussell(Cisco), Christopher Celi(NIST)
- July 2018

Agenda

- How did we get here
- Application
- Architecture
- Runtime Assessment
- Demo
- What’s Next ?

Limitations of Traditional Conformance Testing

- **Long validation cycles**
  - Well beyond product development cycles
  - Hinder adoption of new technology by the Federal Agencies
- **Costly and rigid**
  - Difficult to obtain compliance assurance on platforms of actual use
  - Prevents agencies from fixing critical problems, e.g. CVE, without breaking compliance rules
- **Impossible to fix within the existing box**
  - Some improvements help but fall short of solving the problems agencies face today

CMVP Working Group

- Algorithm Test WG
  - Primary focus is on ACVP

- Software Module WG
  - Defines the sw module functional and failure testing

- Trusted Vendor WG
  - Defines Trusted Vendor acceptance and assurance criteria

- Hardware Module WG
  - Defines the hw module specific requirements

- Cloud WG
  - Defines any cloud specific requirements over and above sw and hw modules.

Automate as much as possible

- Reduce the validation cycle length
- Enable Just-In-Place validations
- Reduce the cost of validations
- Open access to international markets
- Provide a standardized way of performing runtime assessments

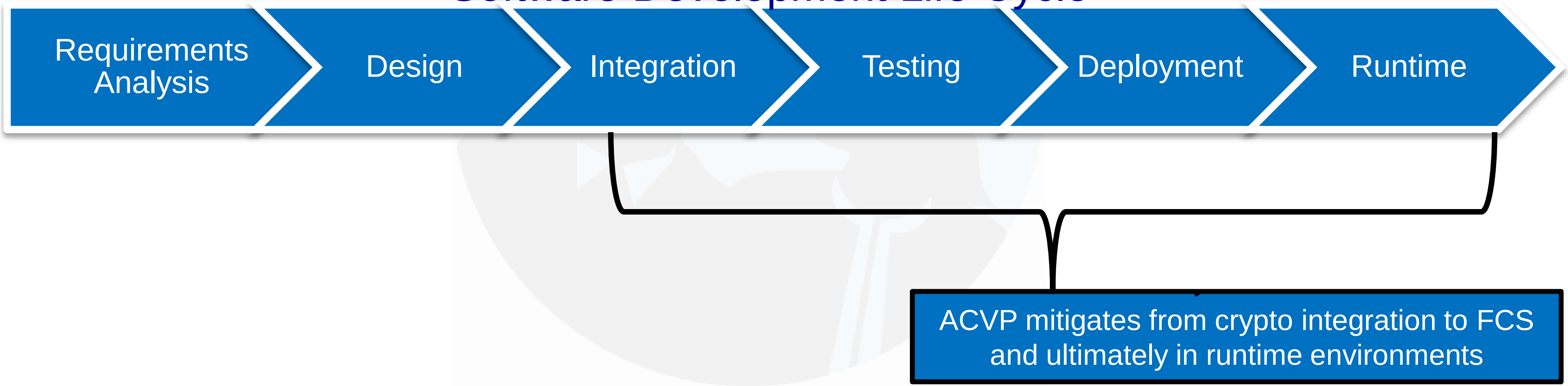
Powerful economic incentives for the industry

Applying ACVP

An attack can occur at any stage of the software life cycle

Mitigating attacks too early leaves you vulnerable in later stages

Software Development Life Cycle



Requirements Analysis

Design

Integration

Testing

Deployment

Runtime

ACVP mitigates from crypto integration to FCS and ultimately in runtime environments

“Lightweight standards track protocol built on top of existing standard protocols and encoding.”

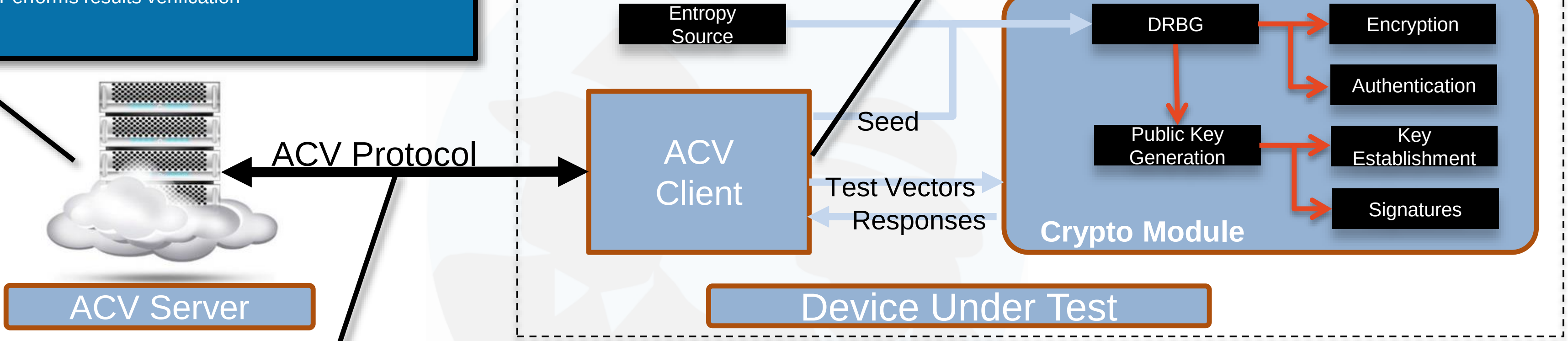
- TLS 1.2
- HTTPS
- Java Script Object Notation(JSON)
- JSON Web Token(JWT) Authorization
- 2 Factor authentication using TOTP
- Client and Protocol Specs open sourced via github

Base Architecture

Automated Cryptography Validation Protocol

ACV Server:
- Web hosted service
- Generates JSON test vectors
- Performs results verification

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



ACV Protocol:
- Standards-based protocol
- Developed in partnership w/ CMVP
- Extensible to mitigate additional vectors over time
- Open Source to enable independent verification

Proxy/Validation Authority Architecture

Automated Cryptographic Validation System

Validation Authority Server:

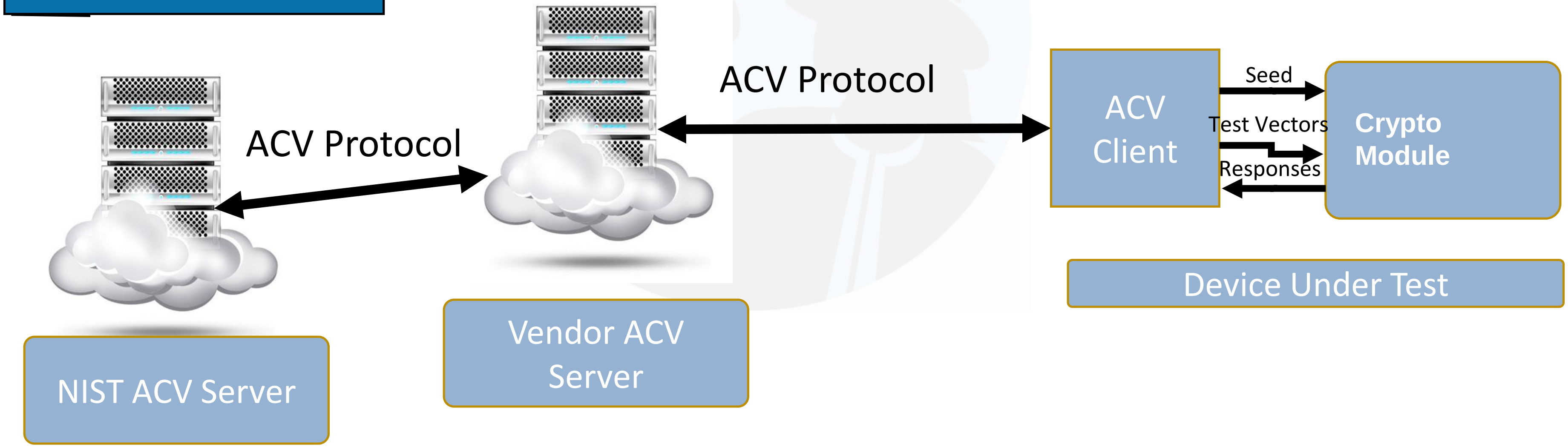
- Web hosted service w/ REST API
- Registers ACV Servers
- Generates JSON KAT vectors
- Validates JSON KAT results
- Publishes validation results from trusted vendor ACV Servers

ACV Proxy/Server:

- Web hosted service
- Interacts with NIST ACV Server to obtain JSON KAT data
- Optionally generates JSON test vectors
- Optionally performs results verification
- Reports JSON KAT results to NIST ACV Server

ACV Client:

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

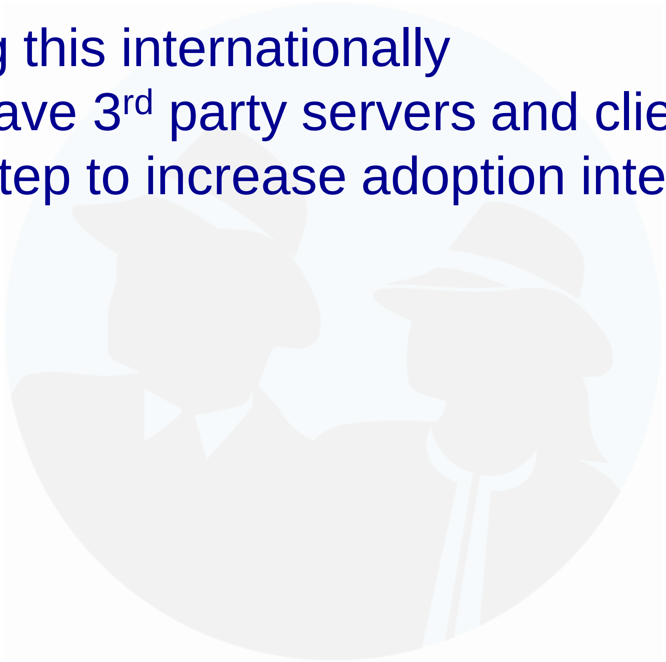


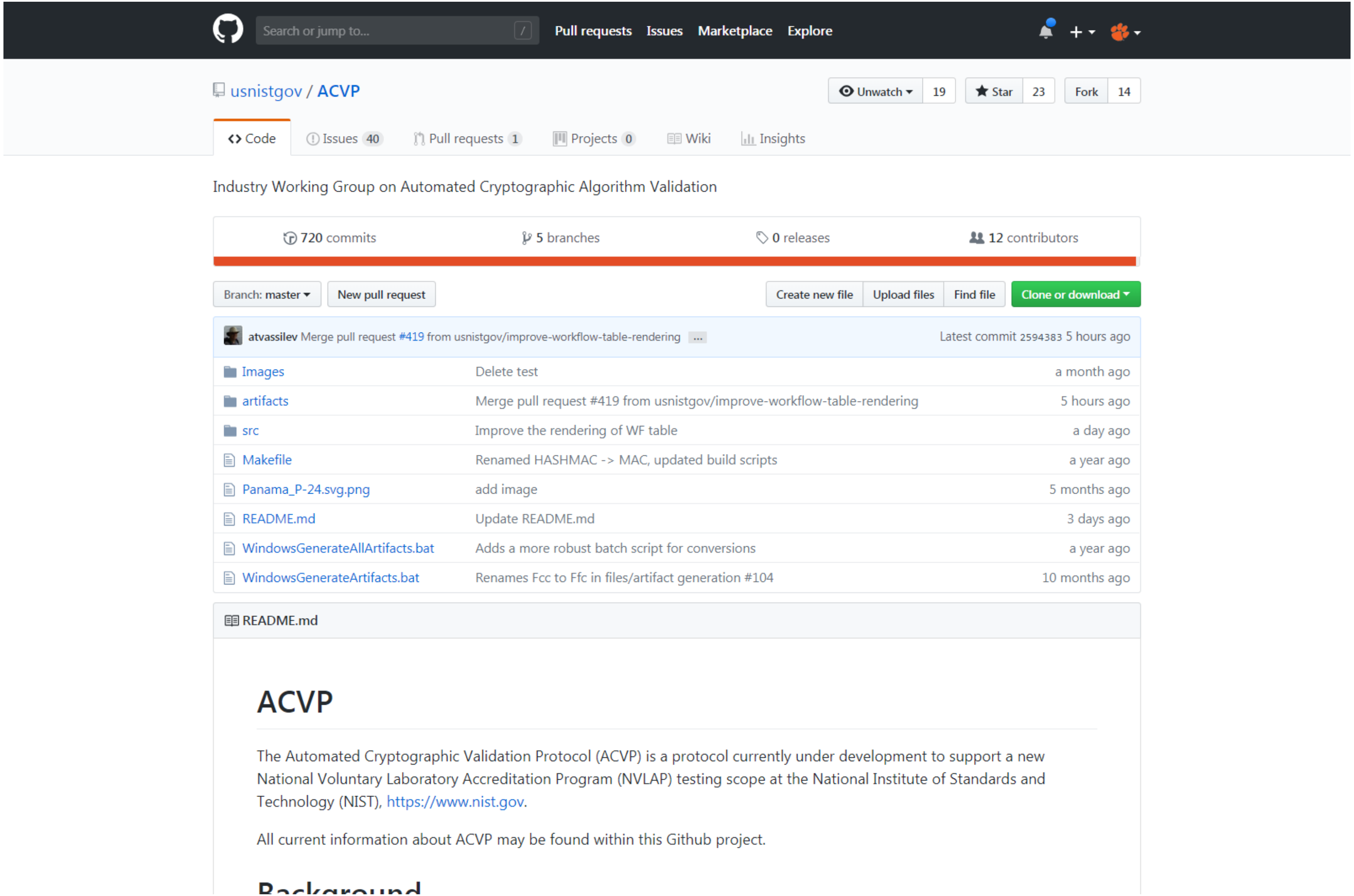
Runtime Cryptographic Assessment

- How long since your crypto has been assessed ?
- Power On Self Tests(POST) are typically run once and never again.
- How effective are POSTs anyway ?
- What can we test at runtime ?

International Acceptance

- NIST is promoting this internationally
- The desire is to have 3rd party servers and clients
- IETF is the next step to increase adoption internationally





Industry Working Group on Automated Cryptographic Algorithm Validation

atvassilev Merge pull request #419 from usnistgov/improve-workflow-table-rendering … Latest commit 2594383 5 hours ago

Images	Delete test	a month ago
artifacts	Merge pull request #419 from usnistgov/improve-workflow-table-rendering	5 hours ago
src	Improve the rendering of WF table	a day ago
Makefile	Renamed HASHMAC -> MAC, updated build scripts	a year ago
Panama_P-24.svg.png	add image	5 months ago
README.md	Update README.md	3 days ago
WindowsGenerateAllArtifacts.bat	Adds a more robust batch script for conversions	a year ago
WindowsGenerateArtifacts.bat	Renames Fcc to Ffc in files/artifact generation #104	10 months ago

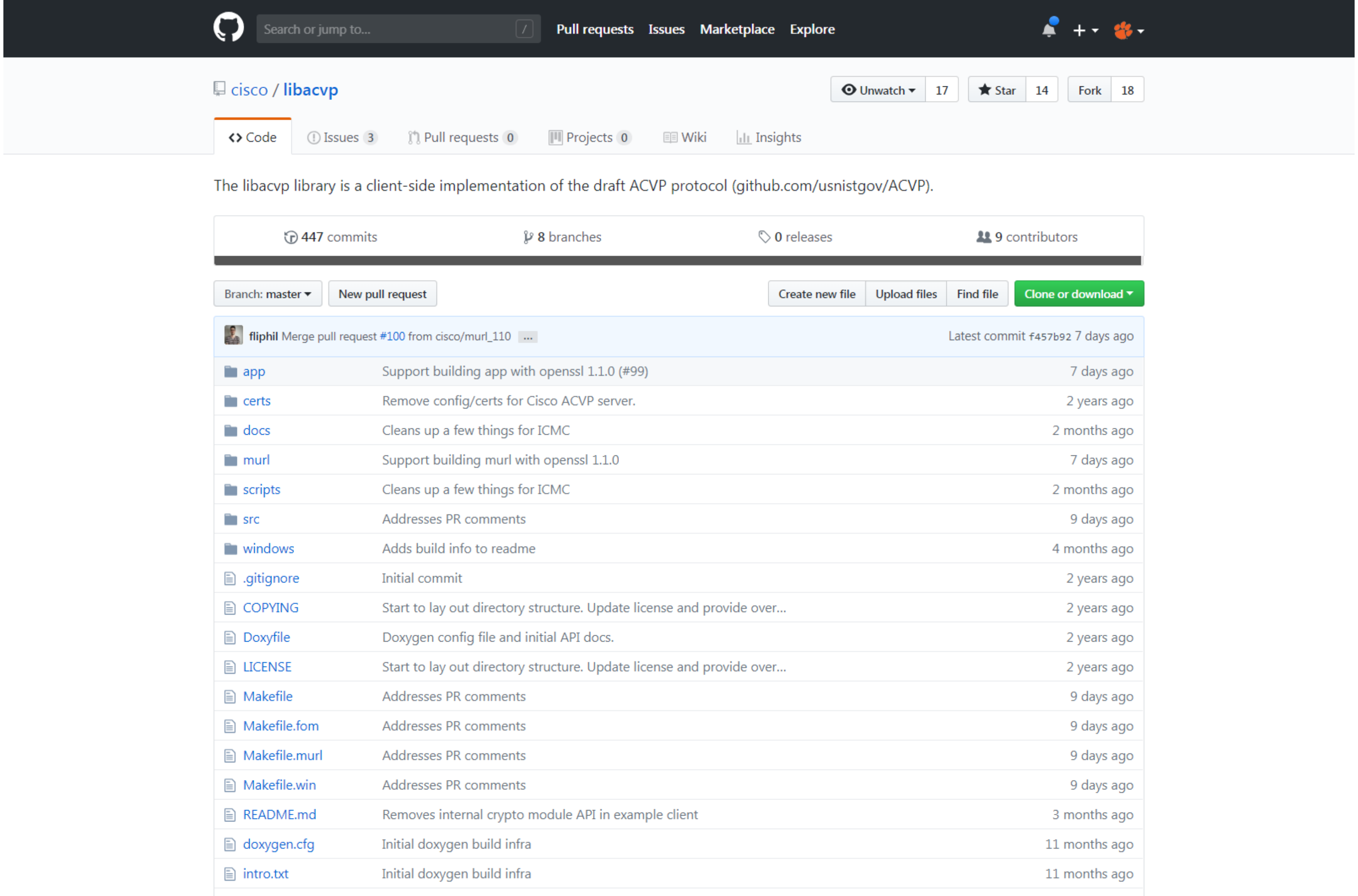
README.md

ACVP

The Automated Cryptographic Validation Protocol (ACVP) is a protocol currently under development to support a new National Voluntary Laboratory Accreditation Program (NVLAP) testing scope at the National Institute of Standards and Technology (NIST), https://www.nist.gov.

All current information about ACVP may be found within this Github project.

Background



The libacvp library is a client-side implementation of the draft ACVP protocol (github.com/usnistgov/ACVP).

fliphil Merge pull request #100 from cisco/murl_110 … Latest commit f457b92 7 days ago

app	Support building app with openssl 1.1.0 (#99)	7 days ago
certs	Remove config/certs for Cisco ACVP server.	2 years ago
docs	Cleans up a few things for ICMC	2 months ago
murl	Support building murl with openssl 1.1.0	7 days ago
scripts	Cleans up a few things for ICMC	2 months ago
src	Addresses PR comments	9 days ago
windows	Adds build info to readme	4 months ago
.gitignore	Initial commit	2 years ago
COPYING	Start to lay out directory structure. Update license and provide over...	2 years ago
Doxyfile	Doxygen config file and initial API docs.	2 years ago
LICENSE	Start to lay out directory structure. Update license and provide over...	2 years ago
Makefile	Addresses PR comments	9 days ago
Makefile.fom	Addresses PR comments	9 days ago
Makefile.murl	Addresses PR comments	9 days ago
Makefile.win	Addresses PR comments	9 days ago
README.md	Removes internal crypto module API in example client	3 months ago
doxygen.cfg	Initial doxygen build infra	11 months ago
intro.txt	Initial doxygen build infra	11 months ago

How to get involved

https://github.com/usnistgov/ACVP

https://github.com/cisco/libacvp

algotest@list.nist.gov

acvp@ietf.org

Contacts:

Barry Fussell(Cisco)
David McGrew(Cisco)
Ellie Daw(Cisco)
Philip Perricone(Cisco)
Sam Farthing(Cisco)
Apostol Vassilev(NIST)
Christopher Celi(NIST)
Harold Booth(NIST)

DEMO

Summary of our goals

- Address the needs of the validation authority community
- Extensible to increase testing coverage
- Gain additional industry participation
- Standardize to grow international acceptance
- Promote and encourage adoption

Next Steps

- Where would the best place to get additional participation ?
- Best way to move this forward ?
- How do we accomplish this within the IETF framework ?