



NIST CMVP Automation Some Considerations

Stephan Mueller
<smueller@atsec.com>

Objective Data

- Automation implies that computers make decisions
 - In classical case: only fully objective data can be automatically analyzed
 - → Question is what is objective data in CMVP validations?
- 1 step: Identifying objective data in existing validations to automate:
 - CAVP certificates (TE.01.12.01) – CMVP can verify them against ACVP data base
 - List of KATs – CMVP can verify them against list of ciphers to comply with minimum requirements
 - Internal consistency check between CAVP certificates and list of ciphers
- 2 step: Partially or fully subjective data should be tackled later

Data Communication

- Rely on structure established with ACVP already
- One JSON hierarchy per test data
 - e.g. one hierarchy for KATs, one for CAVP certificates
 - Allow labs to skip test data entries
 - If test data entries are skipped – the old manual validation for respective test data needs to be applied
- Core goal: data structure **MUST** always be extensible without modifying existing definitions (like ACVP)
 - Each test data definition must have a version number
 - Change in test data definition must imply a change in version number

A?VP Structure

- One JSON hierarchy per A?VP test schemes
- Umbrella automation JSON structure wrapping test schemes
 - { {ACVP structure}, {AMVP structure}, {ENT structure}, ...}
 - Allow easy extensions with new schemes
 - All schemes are optional, all permutations of schemes are allowed, e.g.:
 - { {ACVP structure}}
 - { {ACVP structure}, {ENT structure}}
 - { {AMVP structure}}