NIAP Update

Dianne Hale

National Information Assurance Partnership

18 May 2017

NIAP Policy #5

- *“All cryptography in the TOE for which NIST provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components must be NIST validated (CAVP and/or CMVP). At minimum an appropriate NIST CAVP certificate is required before a NIAP CC Certificate will be awarded.”*

DoD mandates a CMVP (FIPS 140-2) certificate for products procured for use in DoD

NIAP and NIST CAVP/CMVP Relationship

- *CAVP/CMVP integral to NIAP certification - almost all COTS products in the market incorporate cryptographic functionality.*

- *NIST crypto standards are applicable to and used by private and public sectors.*

- *NIAP works with NIST to ensure CAVP/CMVP activities are incorporated into NIAP evaluations.*

- *Ensures all crypto functionality is evaluated to a consistent level of rigor.*

NIAP Recognition of CAVP/CMVP

- *Streamlines the NIAP evaluation process,*
- *Reduces cost, and*
- *Eliminates redundant activities – certain NIAP Assurance Activities are met by the CC Test Lab if that testing is conducted as part of a NIST CAVP or CMVP validation.*

NIAP Verification of CAVP/CMVP Certificates

- *Product Name*
- *Operational Environment (CAVP); HW/SW defined in Security Policy (CMVP)*
  - *Not always easy comparing what’s in the ST to the CAVP Operational Environment*
- *CAVP/CMVP Certificate numbers*
- *SFRs for which certificates apply*
- *All public facing documentation (ST, AAR, VR, PCL listing, Admin Guide)*

Documentation Review

- *Historical CAVP/CMVP lists are not valid (example, RNG transition).*

- *TSS must match SFR claims.*

- *The DRBG claimed in the ST must match the DRBG described in the Entropy Analysis Report.*

- *Misleading terms - If there are no CMVP claims they may not claim FIPS 140-2.*

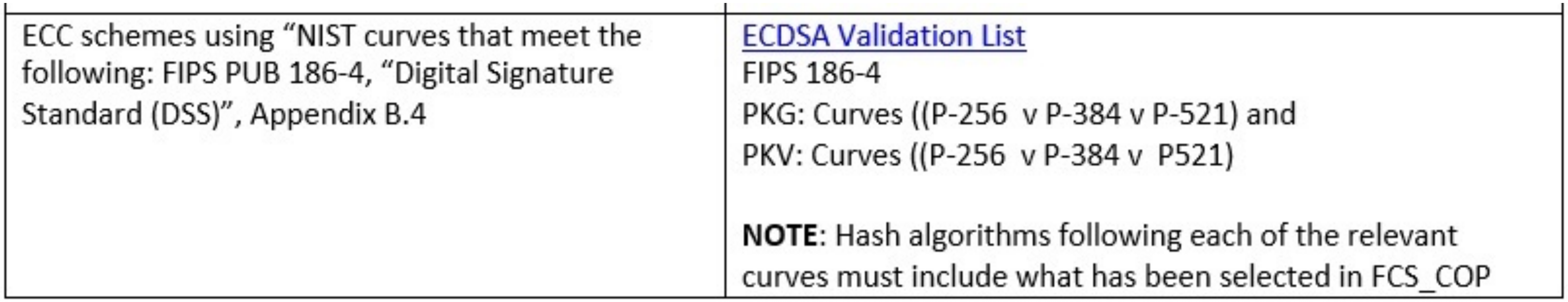
- *Claiming both CMVP and CAVP - the CAVP certificates must be included in the CMVP Security Policy.*

How do you know what to look for?

- *Some algorithms have different test methods, only some of which apply to the requirement.*
  - *RSA Key Generation*
  - *RSA Signature Generation*
  - *RSA Signature Verification*
- *Older certificates may be for older standards (186-2 vs. 186-4 for DSS).*
- *Multiple lists may seem to apply.*
  - *KAS, CVL for 800-56A*
- *Some requirements (for crypto) not obvious.*
  - *Algorithms used in Cryptographic Protocols*

CAVP Mapping Document, Version 1.0

- *Addresses all Crypto Requirements.*
  - *Details what CAVP validation lists to look at*
  - *Details what to look for on each list*



ECC schemes using "NIST curves that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	ECDSA Validation List FIPS 186-4 PKG: Curves ((P-256 v P-384 v P-521) and PKV: Curves ((P-256 v P-384 v P521) **NOTE**: Hash algorithms following each of the relevant curves must include what has been selected in FCS_COP

- *Requirements not addressed must be performed by CCTL.*

Current Efforts and Future Direction

- *NIAP supports the charter of the CMVP WG.*
- *Updating the CAVP mapping document for evaluators/validators to verify certificates are valid for requirements/assurance activities.*
  - *Addressing protocols*
  - *Adding new FIPS-approved and NIST-recommended cryptographic algorithms or components*
- *US continued support to the CC International Crypto WG to develop internationally-accepted cryptographic evaluation requirements and assurance activities.*

Current Efforts and Future Direction

- *SP800-56A*
  - *SP800-56A and DH Group 14 (see NDcPP 2.0 for interim solution until SP800-56rev3 is published).*

- *SP800-56B*
  - *SP800-56B – relooking into assurance activities and applicability of NIST certificates. NIST is revising after SP800-56Arev3 is complete. Once NIST has testing, certificate will be required.*

- *Mapping Document updates*
  - *Addressing protocols (TLS, IPSEC, SSH) – primitives and KDF (SP800-135).*
  - *Adding new FIPS-approved and NIST-recommended cryptographic algorithms or components*

Current Efforts and Future Direction

- *SP800-56C*
  - *Optional KDF which uses expansion and extraction method. Currently drafting AA and will be added to MDF. Once NIST has testing, certificate will be required.*

- *SP800-132*
  - *PBKDF for Storage Applications. Once NIST has testing, certificate will be required.*

Current Efforts and Future Direction

- *SHA-1*
  - *Currently allowed for non-digital signature applications. NIAP will be removing SHA-1 from PPs.*

- *SP800-131Ar1 – NIST Transitions*
  - *Beginning 2018, Key agreement and Key Transport must be SP800-56A or SP800-56B compliant. This does not affect NIAP as our PPs already require this already.*
- *CAVS*
  - *NIST will not be adding new tests to CAVS, therefore, no certificates will be available until the automated tool is ready (12+ months).*

Questions, Comments, Suggestions?

niap@niap-ccevs.org