Post-Quantum

Cryptography Conference

PQC in FIPS 140-3, status and roadmap

Summarize the current state of CMVP algorithm and module validation for PQC algorithms, briefly touch on CMVP plans to speed up module validation through automation, cover 140-3 requirements for PQC algorithms within module, and briefly highlight NSA's CNSA 2.0 as an example of government requirements for PQC beyond the minimum requirements of CMVP.

Jonathan Smith
Senior FIPS Tester at DEKRA

SSL.com PQ SHIELD HID KEYFACTOR ENTRUST

January 15 and 16, 2025 - Austin, TX (US) | Online

PKI Consortium

FIPS 140-3 and PQC

Jonathan Smith

A safe world

8 September, 2023

DEKRA

Introduction

- **Summary of FIPS 140-3**
- **Approved Algorithms & ACVP**
- **NIST/CMVP PQC algorithms**
- **Hybridization**
- **PQC in 140-3 requirement summary**
- **Additional Government / Customer requirements**
- **Queue & Automation**
- **Summary**

FIPS 140-3

- **Minimum requirements for protecting SBU information**
- **Validation authority - CMVP**
- **Incorporates ISO/IEC 19790:2012**
- **Approved algorithms for security**
  - **Annex C (SP 800-140C) *CMVP Approved Security Functions***
  - **Annex D (SP 800-140D) *CMVP Approved Sensitive Parameter Generation and Establishment Methods***
  - **SP 800-131 *Transitioning the Use of Cryptographic Algorithms and Key Lengths***

FIPS 140-3

- **Includes module and key lifecycles, roles & authentication, services, self-test, physical security, etc., in addition to just algorithms**
- **Requirements vary by level and module type**
- **Requirements split between:**
  - **ISO/IEC 19790:2012**
  - **ISO/IEC 24759:2017 (DTR)**
  - **SP 800-140**
  - **(IG) Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program**
  - **Annexes A - F**

Approved Algorithms

- **All are listed in Annexes C & D**
- **Algorithms separately validated through CAVP**
  - **“Black Box” algorithm testing through ACVP**
- **To provide security for 140-3 an Algorithm must be:**
  - **Approved (added to Annex C or D), and**
  - **Validated through ACVP or Vendor Affirmed per IG**
- **Algorithm use with 140-3 determined by the algorithm standard**

ACVP – Automated Cryptographic Validation Program

- **“Black Box” testing**
  - **Submit algorithm capability to NIST’s server**
  - **Receive test vectors**
  - **Algorithm processes test vectors into responses**
  - **Responses returned to NIST’s server**

- **Details on: https://github.com/usnistgov/ACVP#readme**

ACVP – Automated Cryptographic Validation Program

- **DEMO and PROD servers**
  - **DEMO**
    - **Open to all**
    - **For testing only**
    - **Includes some draft, non-approved algorithms**
    - **Trials new algorithm tests**
  - **PROD**
    - **Restricted to accredited CST or 17ACVT labs**
    - **Approved algorithms only**
    - **Issues CAVP algorithm validation certs**

NIST/CMVP PQC algorithms

Standardizing NIST PQC algorithms is ongoing

- **7 algorithms from 4 standards currently Approved**
- **1 standard in development (Falcon)**
- **4th round PQC (KEM) selection in progress**
- **“Onramp” additional signature algorithms being examined**

NIST/CMVP PQC algorithms

- **Current Standards**

NIST Standard	Algorithm	CAVP Algorithm Testing	CMVP Approved
FIPS 208 Stateful Hash-Based Signature Schemes	LMS	Yes	Yes
	HSS	Vendor Affirmed (IG C.O)	Yes
	XMSS	No	Yes*
	XMSS^{MT}	No	Yes*
FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard	ML-KEM (CRYSTALS-KYBER)	Yes	Yes
FIPS 204 Module-Lattice-Based Digital Signature Standard	ML-DSA (CRYSTALS-DILITHIUM)	Yes	Yes
FIPS 205 Stateless Hash-Based Digital Signature Standard	SLH-DSA (SPHINCS^{+})	Yes	Yes
FIPS 206 (Draft expected soon)	(FALCON)	No	No

* Approved but without not usable yet; lack ACVP or affirmation IG

NIST/CMVP PQC algorithms

- **Timeline**

Standard	Issued	CMVP Approved	ACVP testing	1st ACVP Cert
FIPS 208 (LMS)	Oct 29, 2020	May 2022	Apr 19, 2023	Jul 14, 2023
FIPS 208 (HMS)			-	-
FIPS 208 (XMSS)			-	-
FIPS 208 (XMSS^{MT})			-	-
FIPS 203 (ML-KEM)	Aug 13, 2024	Aug 13, 2024	Aug 13, 2024	Aug 13, 2024
FIPS 204 (ML-DSA)	Aug 13, 2024	Aug 13, 2024	Aug 13, 2024	Aug 13, 2024
FIPS 205 (SLH-DSA)	Aug 13, 2024	Aug 13, 2024	Aug 13, 2024	Aug 14, 2024

Hybridization

- **CMVP treating PQCs like any other approved algorithms**
  - **No mandatory hybridization**

- **Hybridization for key establishment**
  - **Permitted under SP 800-133**

- **Hybridization of signatures**
  - **Inherently permitted**

PQC in 140-3 requirement summary

FIPS 208 (LMS, HSS, XMSS, XMSS^{MT})

- **Private keys must reside in 140-3 level 3 or 4 hardware**
- **Algorithm SHALL NOT be usable in module's non-Approved mode**
- **No export, import, back-up, etc. of private keys**
- **IG 10.3.A self-tests**
  - **SigGen requires KeyGen**
  - **CAST also for KeyGen**
  - **PCT test following KeyGen limited to confirming same key identifier for new public & private key**

PQC in 140-3 requirement summary

FIPS 203 (ML-KEM)

- **Minimum RBG security strength depending on KEM used**
  - **128 bit for ML-KEM-512, 192 for ML-KEM-768, 256 for ML-KEM-1024**
- **Restrict access to internal functions**
- **ML-KEM SHALL NOT use floating-point math**
  - **IG 10.3.A self-tests**
    - **Encapsulation CAST using fixed *ek* and *m* values**
    - **Decapsulation CAST using fixed *dk* and *c* values; SHALL cover implicit rejection and non-rejection paths**
    - **KeyGen shall have a CAST using fixed random values**
    - **PCT SHALL encapsulate then decapsulate a shared secret**

PQC in 140-3 requirement summary

FIPS 204 (ML-DSA)

- **Minimum RBG security strength depending on DSA used**
  - **128 bit* for ML-DSA-44, 192 for ML-DSA-65, 256 for ML-DSA-87**
- **ML-DSA SHALL NOT use floating-point math**
  - **IG 10.3.A self-tests**
    - **Signing CAST using fixed *sk* and *M (and rnd, if applicable)* values**
    - **Signing CAST SHALL cover all applicable rejection sampling loop paths**
      - https://pages.nist.gov/ACVP/draft-celi-acvp-ml-dsa.html#name-known-answer-tests
    - **Verification CAST using known good signature**
    - **KeyGen shall have a CAST using fixed random values**
    - **PCT test following KeyGen is sign then verify some message**

*** Should be 192 bit, SHALL be 128 bit**

*

PQC in 140-3 requirement summary

FIPS 205 (SLH-DSA)

- **Minimum RBG security strength depending on DSA used**
  - **8*n* where n is defined by parameter set selected**
- **SLH-DSA SHALL NOT use floating-point math**
  - **IG 10.3.A self-tests**
    - **Signing CAST using fixed SK and *M* values; set opt_rand to PK.seed value**
    - **Verification CAST using known good signature**
    - **If SHA2 and SHAKE parameter sets both supported,**
      - **above CASTs SHALL each test one of each.**
    - **KeyGen shall have a CAST using fixed random values**
    - **PCT test following KeyGen limited to confirming same key identifier for new public & private key**

*** Should be 192 bit, SHALL be 128 bit**

Additional Government / Customer requirements

- **Determine additional requirements beyond 140-3**
  - **End users might want hybrid crypto (PQC + classic)**
  - **End users might want PQC aware protocols**
  - **NSA’s CNSA 2.0**
  - **Etc.**

Queue & NIST Automation

- **“Queue” between report submission and CMVP review: 1 year**

Automation

- **Attempting to speed up the currently slow process of review and approval**
- **Algorithm validation already automated through ACVP**
- **Entropy source validation already partially automated through ESV**
- **Module validation automation is being examined by NCCOE**
  - **Initial proposal expected at ICMC in April**
- **Security Policy Document review automation via SP 800-140Br1**

Summary

- **Labs ready for PQC 140-3 modules using**
  - **LMS, HSS, ML-KEM, ML-DSA, and/or SLH-DSA**
- **CAVP testing exists for LMS, ML-KEM, MK-DSA, SLH-DES**
  - **Certs already issued**
- **First 140-3 module w/ PQC likely validated summer/fall 2025**
- **More algorithms coming**
  - **ACVP for HSS (vendor approvable now), XMSS, XMSS^{MT}**
  - **FIPS 206 – based on Falcon**
  - **Fourth round KEM(s), etc.**

Questions?

Contact Information

Jonathan Smith - DEKRA

Jonathan.Smith@Dekra.com