atsec CST Newsletter

2023-12

This newsletter is intended to inform our customers about the recent changes that have been published on the Cryptographic Module Validation Program (CMVP) website as well as upcoming changes. We are standing by our customers and preparing you for these changes that may have an impact on your cryptographic modules.

Documents

The CMVP published updated documents:

- **FIPS 140-3 Management Manual version 1.6 (2023-10-03)**
  https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual

- **SP800-140B Rev.1 (November 2023)**
  (CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140Br1.pdf

CMVP Transitions

January 1, 2024: Triple-DES (SP 800-67 Rev2)

The Triple-DES decryption, including its use in key unwrapping, will continue to be approved (for legacy use only) after December 31, 2023.
Already validated FIPS 140-2 modules that support Triple-DES Encryption in the Approved Mode will not be moved to the historical list.

January 1, 2024: Compliance to SP800-56BRev2

SP800-56B vendor affirmations submitted before December 30, 2020 remain approved until the end of 2023. Effective January 1, 2024, compliance to SP800-56BRev2 is required.

January 1, 2024: RSA PKCS based key wrapping

Any RSA-based key encapsulation/un-encapsulation algorithm using PKCS#1-v1.5 padding scheme were previously allowed to be used in approved mode. This allowance expires on December 31, 2023.
Already validated FIPS 140-2 modules will not be moved to the historical list.

January 1, 2024: SP 800-140Brev1 compliance

All FIPS 140-3 submissions need to comply with the SP 800-140Brev1. The Pilot project phase is ongoing and an overview can be found here
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/sp-800-140-series-supplemental-information/sp800-140b

February 5, 2024: FIPS 186-5 transition

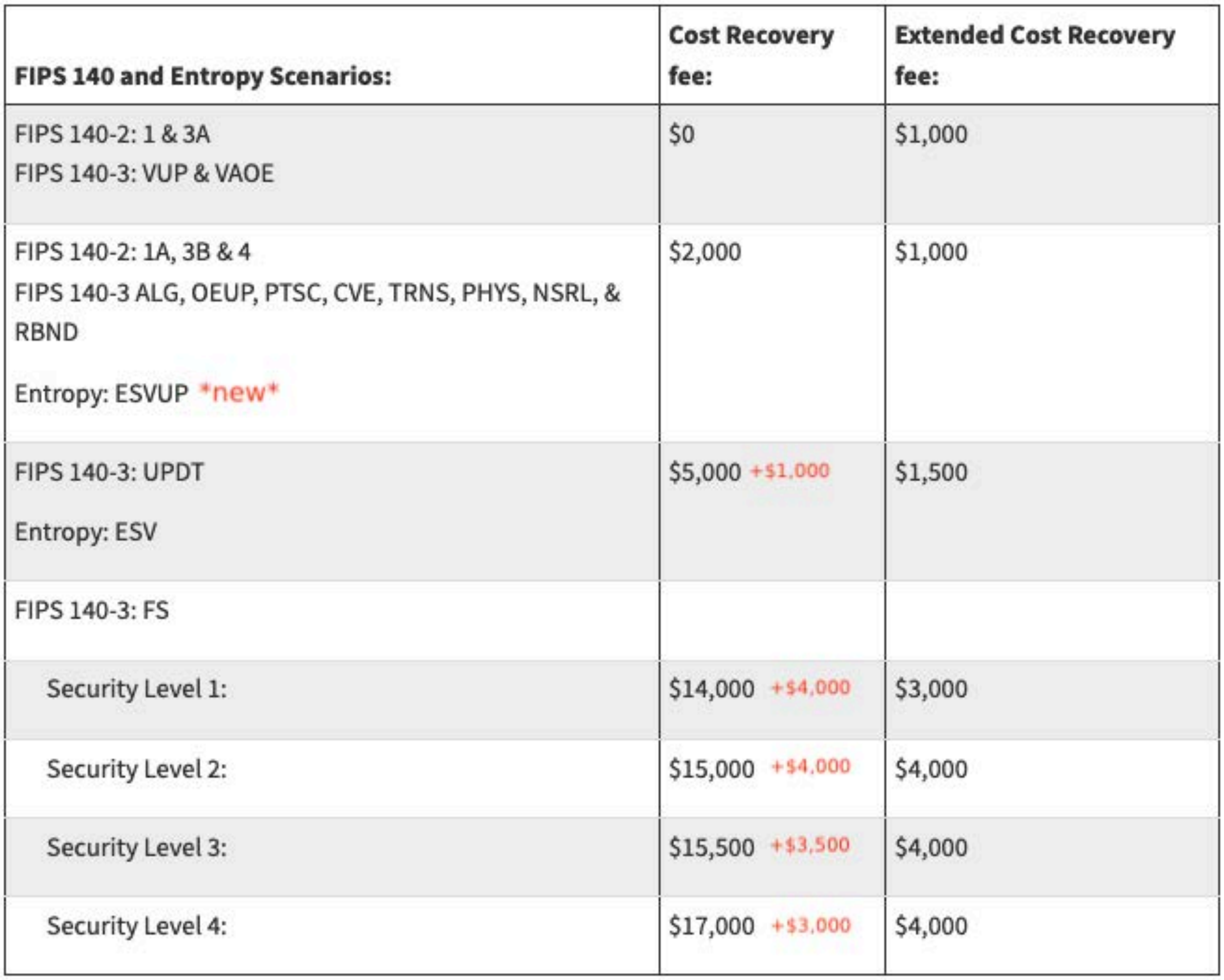
CMVP will no longer accept new submissions that implement DSA or RSA X9.31 in the approved mode, other than for signature verification, which is still approved for legacy purposes for both algorithms.
See FIPS 140-3 IG D.K for details.
Already validated or submitted modules will not be affected.

Next revision of the SHA standard

SHA-1 will be removed in the next revision of the SHA standard and a transition period will be provided. The target SHA-1 sunset date is December 31, 2030.

CMVP Cost Recovery Fees

The CMVP updated the CR fees for cryptographic module validation and entropy source validation, effective on January 1st, 2024. The increases are shown in red text below.
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees



FIPS 140 and Entropy Scenarios:	Cost Recovery fee:	Extended Cost Recovery fee:
FIPS 140-2: 1 & 3A FIPS 140-3: VUP & VAOE	$0	$1,000
FIPS 140-2: 1A, 3B & 4 FIPS 140-3 ALG, OEUP, PTSC, CVE, TRNS, PHYS, NSRL, & RBND Entropy: ESVUP *new*	$2,000	$1,000
FIPS 140-3: UPDT Entropy: ESV	$5,000 +$1,000	$1,500
FIPS 140-3: FS		
Security Level 1:	$14,000 +$4,000	$3,000
Security Level 2:	$15,000 +$4,000	$4,000
Security Level 3:	$15,500 +$3,500	$4,000
Security Level 4:	$17,000 +$3,000	$4,000

FIPS 140-3 Implementation Guidance (IG)

The current version of the IG was published on **November 22, 2023**, and is available at:
https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf

Updated Guidance

2.3.C	**Processor Algorithm Accelerators (PAA) and Processor Algorithm Implementation (PAI)**
Added a few Known PAAs.	
2.4.C	**Approved Security Service Indicator**

Clarified the API example in the Resolution and added a related Additional Comment 5.	
4.1.A	**Authorized Roles**
Added “[for CSPs only]” in Background. Clarified in a. the exception applies when hashing data, not SSPs. Added a paragraph after the exceptions connecting authorization to authentication.	
9.5.A	**SSP Establishment and SSP Entry and Output**
Slight modification to the SK legend under Table 2.	
C.C	**The Use and the Testing Requirements for the Family of Functions defined in FIPS 202**
Removed the outdated Additional Comments.	
C.H	**Key/IV Pair Uniqueness Requirements from SP 800-38D**
Changed “technique” to “scenario” in the beginning of the Resolution for consistency. Added leniency to the abort logic requirement in Scenario 3.	

FIPS 140-2 Implementation Guidance (IG)

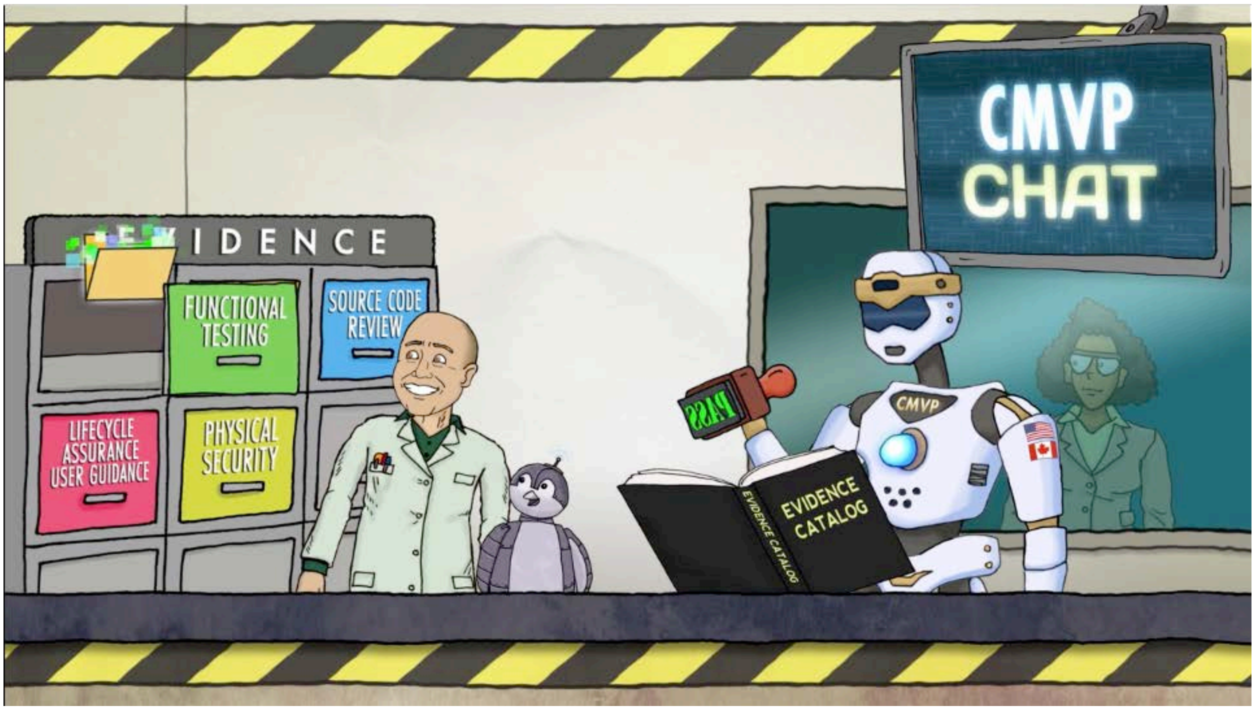
The current version of the IG was published on **October 30, 2023**, and is available at: https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-program/documents/fips140-2/FIPS1402IG.pdf

Updated Guidance

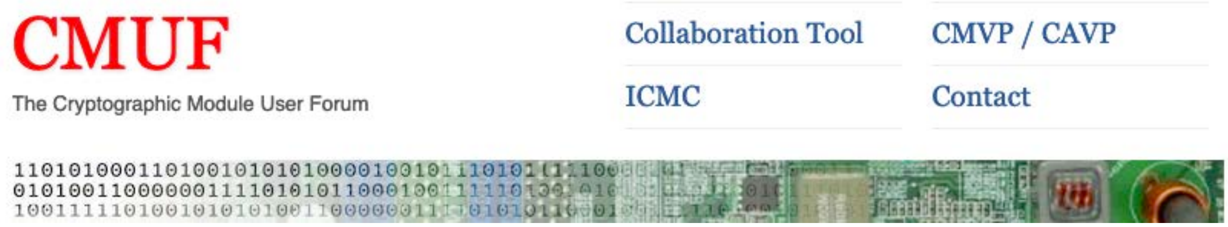
G.8	**Revalidation Requirements**
Added requirements in Scenario 3B for a table indicating which certificate fields have been updated.	
G.17	**Remote Testing for Modules**
Updated to be consistent with the FIPS 140-3 remote testing guidance.	
D.4	**Requirements for Vendor Affirmation of SP 800-56B**
Removed reference to the December 31, 2023 transition.	
D.9	**Key Transport Methods**
Updated the language on the December 31, 2023 transitions.	

Shortening the FIPS Queue through Automation

atsec has been working with the National Cybersecurity Center of Excellence (NCCoE) on ways to shorten the FIPS 140-3 module submission queue. We produced a video to give a light-hearted overview of the effort (https://vimeo.com/864916383).



The Cryptographic Module User Forum


CMUF

The Cryptographic Module User Forum

We invite you to take a look at the CMUF website at https://cmuf.org/ and join the CMUF Collaboration Forum at https://cmuserforum.onlyoffice.com.

International Cryptographic Module Conference (ICMC)

The ICMC 2023 was held from September 20 to 22 in Ottawa, Canada.
Please see our blog article for a summary:
https://atsec-information-security.blogspot.com/2023/09/the-11th-international-cryptographic.html

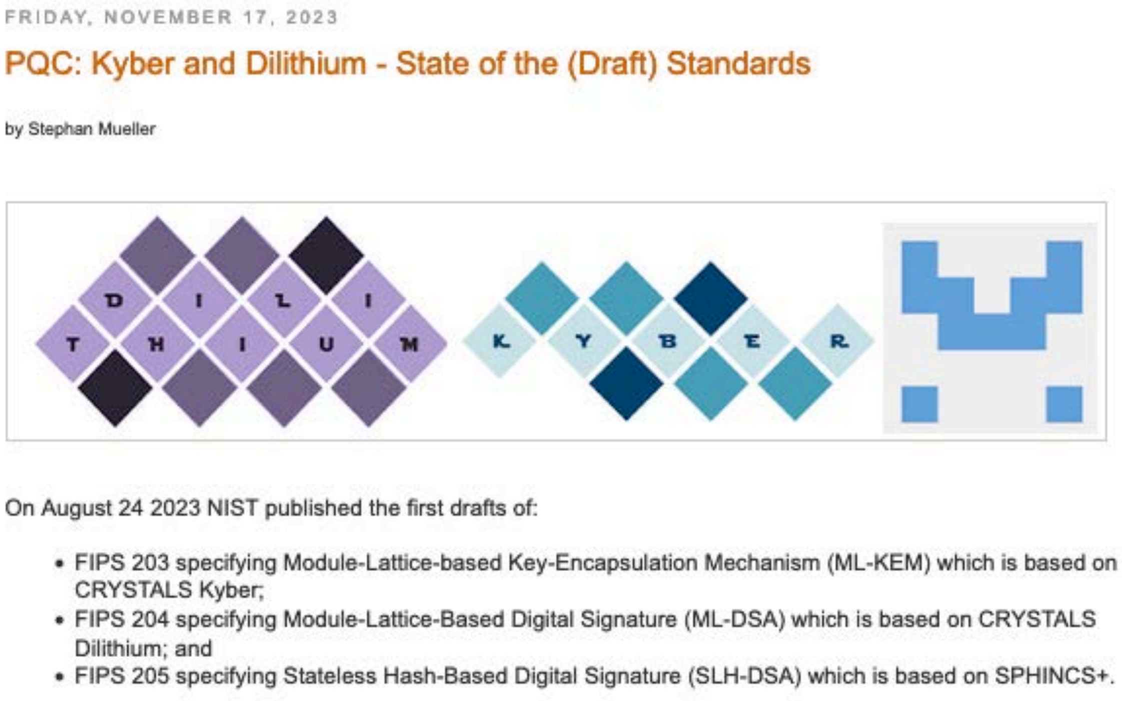
For more information on the ICMC, please visit https://icmconference.org/.

Crypto Module Boot Camp – February 27th 2024

atsec information security has partnered with Concordia University in Austin, Texas for a day-long in-person or remote boot camp on cryptography, AI and Cyberspace, cryptographic algorithms, entropy and NIST's cryptographic module validation program (CMVP). Attendance is free and includes lunch and a tour of the nature preserve at the end of the day. Donations to the Dr. Bertrand du Castel Scholarship for Concordia students are highly encouraged and appreciated. We will send out additional information about the event soon.

PQC: Kyber and Dilithium - State of the (Draft) Standards

Our colleague, Stephan Mueller, published a blog article on the topic of quantum safe algorithms: https://atsec-information-security.blogspot.com/2023/11/pqc-kyber-and-dilithium-state-of-draft.html



FRIDAY, NOVEMBER 17, 2023

PQC: Kyber and Dilithium - State of the (Draft) Standards

by Stephan Mueller

On August 24 2023 NIST published the first drafts of:

- FIPS 203 specifying Module-Lattice-based Key-Encapsulation Mechanism (ML-KEM) which is based on CRYSTALS Kyber;
- FIPS 204 specifying Module-Lattice-Based Digital Signature (ML-DSA) which is based on CRYSTALS Dilithium; and
- FIPS 205 specifying Stateless Hash-Based Digital Signature (SLH-DSA) which is based on SPHINCS+.

Happy Holidays and Happy New Year

The whole atsec team wishes our colleagues, customers, partners, and suppliers Merry Christmas and a Happy New Year.

Please see our seasonal greetings here: https://atsec-information-security.blogspot.com/