atsec cst newsletter

2025-02

We are standing by our customers and preparing you for upcoming changes that may have an impact on your cryptographic modules, for example the changes to ISO/IEC 19790, which are expected to be published in March 2025. We will give an overview of those changes at the... *drum roll*...

FIPS 'n' Chips Crypto Module Bootcamp

After the overwhelming success of last year's bootcamp, atsec will host another free Crypto Module Bootcamp in collaboration with UT Austin on their campus on March 25th, 2025. This year we focus on the upcoming changes to ISO/IEC 1970 and what it means, especially for hardware vendors and chip manufacturers. Panel discussions and an impressive roster of experts from academia, government and the industry promise an interesting and informative day. We also have a dedicated time for networking and recruiting with the students from UT Austin's excellent Computer Science department.

See the agenda and the roster of speakers here: https://www.atsec.com/fips-n-chips/schedule.html
You can sign up for bootcamp here: https://forms.gle/NAPSKGjn6RWzk8nz8

The new year is here, and we have hit the ground running! This newsletter is intended to inform our customers about the recent updates that have been published or are currently in draft form, as well as general topics regarding the crypto module world.

CMVP Document Updates

- **FIPS 140-3 Management Manual version 2.3 (2024-12-17)**
  https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS-140-3-CMVP%20Management%20Manual.pdf

  Two new sections titled **4.3.3 Request for Transition Period Extension** and **7.1.2.1 Interim Validation** were added in this version.
  Please refer to the revision history for all changes to the document.

- **Transitioning the Use of Cryptographic Algorithms and Key Lengths**
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar3.ipd.pdf

  Some of the important changes include:

  - Section 1.2.2 expands the discussion on legacy use to include how users should consider the legacy-use status.
  - Section 1.2.3 is a new section that discusses the strategy for transitioning from a 112-bit security strength to a 128-bit security strength for block ciphers and hash functions or continuing the acceptability of the 112-bit security strength until further PQC guidance is provided for digital signatures and key establishment.
  - In Sec. 2, the Skipjack algorithm has been removed, TDEA is disallowed for applying cryptographic protection, and a subsection on the block cipher modes of operation has been added.
  - Appendix A has been added to discuss the continued use of AES when quantum computers become available.

CAVP Updates

The CAVP production server now supports ML-DSA and SLH-DSA sign and verify testing to include tests for the external interfaces defined in FIPS 204 Section 5 and FIPS 205 Section 10.

The updates also cover ML-DSA sign and verify testing to support externally computed μ as allowed in the FIPS 204 comments for Algorithm 7 (line 6) and Algorithm 8 (line 7).

FIPS 140-3 Implementation Guidance (IG)

The current version of the FIPS 140-3 IG was published on **December 20, 2024**, 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

C.M	Legacy Algorithms
Revised “Symmetric Algorithms Used for Decryption / Unwrapping” to break out rows for clarity and include unauthenticated AES. Minor clean up in other areas of the IG.	

CMVP Cost Recovery Fees

The CMVP updated the CR fees for cryptographic module validation and entropy source validation, effective on January 1st, 2025.
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	$2,500	$1,000
FIPS 140-3: UPDT Entropy: ESV	$5,500	$1,500
FIPS 140-3: FS		
Security Level 1:	$16,000	$3,000
Security Level 2:	$17,000	$4,000
Security Level 3:	$17,500	$4,000
Security Level 4:	$19,000	$4,000

International Cryptographic Module Conference (ICMC)

The next ICMC will be held in Toronto Canada from April 7-4 2025 and several of our colleagues will give presentations on several important topics. **We hope to see you at our booth!**

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

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://cmuf-workspace.org.