RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: ACB-R01

You, Me and FIPS 140-3: A Guide to the New Standard and Transition

Ryan Thomas

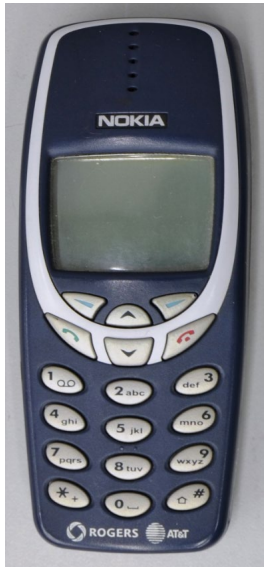
CST Laboratory Manager
Acumen Security
Twitter: @acumensec

FIPS 140-2 is *HOW* OLD?

- It’s hard to believe FIPS 140-2 turned 18 years old in May 2019 ….
- FIPS 140-2 is old enough to drive …
- In most countries it's old enough to vote or go to university!

Nothing much has changed since 2001, right?

Apple's 1st Gen iPod



Nokia 3360

Original xbox console

Objectives for this briefing

- What is this FIPS thing? Why is it important?
- Current challenges with “Dash-2”
- What took so long!?!
- New terms in “Dash-3”
- Key differences between “Dash-2” and “Dash-3”
- Key dates for the transition
- What will happen to existing FIPS 140-2 certificates?
- Apply: Acumen’s advice and tips to survive the transition

What is FIPS? Why is it important?

- Federal Information Processing Standard (FIPS) by U.S. Government
- Security Requirements for Cryptographic Modules
- For protection of “Sensitive But Unclassified information” (SBU)
- Dash “2” is the second iteration
- Mandated by U.S. and Canadian governments
- Established internationally as defacto benchmark for cyber security products that do crypto
- Minimum bar for whitelisting programs in regulated industries like finance, healthcare, legal and utilities

Who is the CMVP?

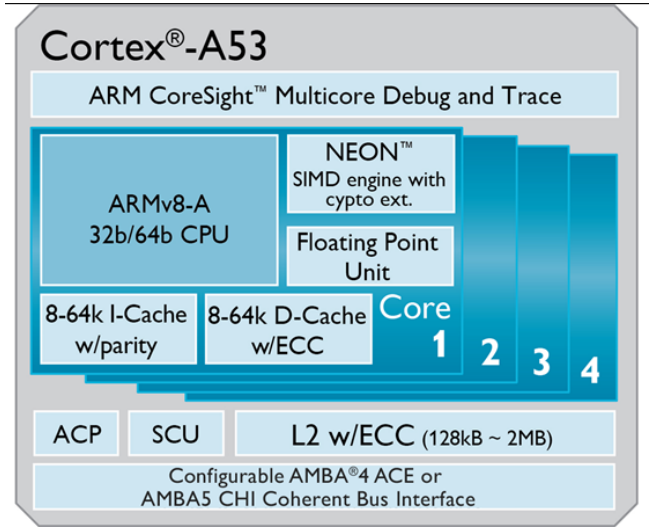
- Responsible for administration and oversight of FIPS 140-2 module validations
- Joint effort between U.S. National Institute of Standards and Technology (NIST) and Canada's Canadian Centre for Cyber Security (CCCS)
- Independent 3rd party testing labs (like Acumen) accredited by NVLAP
- Labs conduct FIPS functional testing and source review on CMVP's behalf
- CMVP ultimately validate submissions and issue FIPS validation certificates

RSAConference2020

Challenges with Dash-2

Challenges with FIPS 140-2 module validations

- 2001 standard wasn't written for SoCs, nested hypervisors, virtual HSMs or different cloud-based solutions etc.
- It has become ***SO*** difficult applying 18-year-old requirements and re-interpreting them for modern cyber security products and technologies!



FIPS lab customer feedback hotline …

Self-tests are no fun!

- Questionable value in some cases
- Ex. CRNGT on software RNGs?
- Each library instantiation must POST

Sledgehammer for Error Handling!

- All or nothing – no flexibility
- If self-tests fail traffic must be squelched!

Wut? Why no Cloud!?!

- Platform detail requirements
- Must specify tested hardware

So very, very Esoteric !!

- Additional help often necessary to navigate the FIPS “lore”
- Correct interpretations can be key!

How has CMVP coped with passage of time?

- Implementation Guidance document grown to 250 pages (it was ~65 pages in 2002)
- Many “shalls” and “shall nots”
- IGs published in isolation for many years (no industry feedback)
- Process is not agile, reactive, slowwwwwww

How have labs coped with challenges?

- My job on a day-to-day basis involves shoe-horning modern cyber security products into “FIPS-able” modules
- A lot of out of the box thinking and a pragmatic view of the requirements is needed to achieve FIPS validations

RSAConference2020

OK. What the *BLEEP* took So Long!?!

FIPS 140-3 ….. Vaporware?

- There were actually two successors to Dash-2
- Several reasons lead to the delay …
- Progress grinded to a halt …
- Talk of moving to FIPS 140-4!?!
- ~2012 ISO version gained a lot of traction
- Even after decision made … regime changes, red tape & bureaucracy delayed things further

RSAConference2020

FIPS 140-3: A NEW Hope

March 22nd, 2019 - FIPS 140-3 officially signed!

- Official confirmation of US decision to use ISO/IEC 19790:2012/Cor 1:2015 to replace FIPS 140-2
- ISO 24759:2017 will serve as the Derived Testing Requirements
- NIST SP 800-140 series serve as requirements for the CMVP
  - Clarify and replace ISO/IEC 19790 Annexes with SP 800-140A - F
  - Living documents that can be updated by CMVP
  - These are NEW DTRs!

NIST SP 800-140: Important Supplemental Docs

- SP 800-140 A - F replace current FIPS 140-2 Annexes A-D and supplement the ISO with additional CMVP requirements:
  - NIST SP 800-140 – CMVP updates to ISO/IEC 24759 DTR
    - Additional caveats, clarification and documentation requirements
  - NIST SP 800-140A – Vendor Documentation Requirements (ISO Annex A)
    - Focus on remediation of CVEs in the module
  - NIST SP 800-140B – Module Security Policy Requirements (ISO Annex B)
    - Module Security Policies to grow substantially (sigh….)

NIST SP 800-140: Important Supplemental Docs (cont'd)

- NIST SP 800-140C – Approved Security Functions (ISO Annex C)
  - References NIST publications – NIST SP 800-38A etc.
- NIST SP 800-140D – SSP (Key) Generation and SSP Key Establishment (ISO Annex D)
  - References NIST publications - NIST SP 800-90A, 56A etc.
- NIST SP 800-140E – Approved Authentication Methods (ISO Annex E)
  - ***NEW*** - Lots to digest here. Mostly aligns with NIST SP 800-63B
- NIST SP 800-140F - Approved non-invasive attack mitigation test metrics (ISO Annex F)
  - Some ISOs still in draft. Unclear if SL3 & SL4 available initially in 09/2020

What happens to the “duct tape”?

- There will be an IG, but it will be smaller (for now)
- Many technical IGs integrated “baked into” FIPS 140-3 and NIST SP 800-140 series already
- Programmatic related IGs will be moved to web-based CMVP Management Manual
- Plan to publish IG March 2020

RSAConference2020

FIPS 140-3: New Terms

New Terms: I Feel So Degraded …

- Normal vs. Degraded Mode of Operation
  - Normal Mode – All Tests PASS - entire set of algorithms, functions and services are available
  - Degraded Mode – Test FAILS - the module can still provide limited cryptographic services
- Example: Allow critical operations to continue after a single component failure

New Terms: SSPs, CSPs and PSPs

- Public Security Parameters (PSP)
  - Public keys, certificates etc.
- Critical Security Parameters (CSP)
  - Secret and private cryptographic keys, authentication data such as passwords, PINs etc.
- Sensitive Security Parameter (SSP)
  - Includes both PSPs and CSPs
- Confidentiality and integrity-related requirements associated with SSPs
- Only integrity-related requirements for PSPs.

New Terms: Self-Test Categories

- Pre-Operational self-tests
  - Previously a Power-On Self-Test (ie. POST)
- Periodic self-tests
  - SL 1 same as “classic” FIPS 140-2 on-demand self-test.
  - SL 3 & 4 specific self-tests must be performed upon a defined time period
  - Logic needs to be built-in!
- Conditional fault test
  - If a fault detected in cryptographic algorithm the self-test must fail

Example: DRBG Health Checking

New Terms: New Output Types Defined

- Control Output Interface
  - Commands sent to instruct another component or
  - Commands which indicate state of operation of a module

  Example: Control and provisioning commands sent from wireless controller to wireless AP

- Self-initiated Cryptographic Output
  - Ability to perform crypto operations or management functions without external operator request

  Example: Module configured to automatically establish an IPsec tunnel to another device upon startup

New Terms: Vendor Testing, Low-Level Testing & EoL

- Vendor Testing (All levels)
  - Vendors shall use “current” automated security diagnostic tools

  Example: Static code analysis tools such as Coverity or Fortify etc.

- Low-level Testing (SL 3 & SL 4)
  - Written, detailed test cases for functionality with expected outcomes

- End of Life
  - SL 1 requires procedure for secure sanitization of the module
  - SL 3 & 4 requires procedures for secure destruction of the module

RSAConference2020

FIPS 140-3: What's the Diff?

- Hold on to your hats we'll be going pretty fast here
- For a detailed "Diff" visit the Acumen Security blog

The Diff: Dash-2 vs. Dash-3 Snapshot

FIPS 140-2

1.Cryptographic Module Specification
2.Cryptographic Module Ports and Interfaces
3.Roles, Services, and Authentication
4.Finite State Model
5.Physical Security
6.Operational Environment
7.Cryptographic Key Management
8.EMI/EMC requirements
9.Self Tests
10.Design Assurance
11.Mitigation of Other Attacks

Appendix C – Security Policy

Annex A – Approved Security Functions

Annex B – Approved Protection Profiles

Annex C – Approved RNGs

Annex D – Approved Key Establishment

ISO/IEC 19790

1.Cryptographic module specification
2.Cryptographic module interfaces
3.Roles, services, and authentication
4.Software/Firmware security
5.Operational environment
6.Physical security
7.Non-invasive security
8.Sensitive security parameter management
9.Self Tests
10.Life-cycle assurance
11.Mitigation of other attacks

Annex A – Documentation requirements

Annex B – Cryptographic module security policy

Annex C – Approved Security Functions

Annex D – Approved sensitive security parameter generation and establishment

Annex E – Approved authentication mechanisms

Annex F – Approved non-invasive attack mitigating test metrics

The Diff: Gimmie the TL;DR

- Conceptually a lot is the same …
- References to EALs and Common Criteria removed
- Many clarifications and explanations from CMVP's "lessons learned" during Dash-2
- Explicitly addresses Hybrid modules and entropy
- Physical Security changes at SL 3 & 4
- Strong Authentication requirements at SL 2 and up
- Module Development and Lifecycle requirements
- Module Delivery and "First use" requirements
- Finite State Model gets folded into Design Assurance
- Actual Non-Invasive Security Requirements
  - SL 3 & SL 4 Mitigation Testing using Test metrics defined in (future) SP 800-140F
- Prescriptive Security Policy requirements

The Diff: Those Dang Self-tests

- Updated: Pre-Operational Self-tests
  - Software/firmware integrity test
  - Bypass test
  - Critical functions test
- EDC Integrity test for HW modules only at SL 1
- New: Conditional Cryptographic Algorithm Self-tests
  - Performed prior to first use – BIG CHANGE HERE
  - Can be Known Answer Test, Comparison Test or Fault-detection Test

The Diff: Those Dang Self-tests (continued)

- Updated: Conditional Bypass Test requirements
  - Must use Approved Integrity technique
  - Module must implement logic for the check immediately before and after changes
- New: Conditional Fault-Detection Test
  - Fault detection mechanisms integrated in algorithm
  - When a fault is detected, the cryptographic algorithm test must fail
- SL 3 and 4 error logging required on self-test failure

The Diff: Those Dang Self-tests (continued)

- Updated: Explicit Pairwise Consistency Test (PCT) requirements for:
  - Digital signature generation/verification
  - SSP agreement (underlying algorithms used for DH or EC DH)
  - Approved key transport (RSA and DLC schemes)

  This would affect modules generating asymmetric keys or digital certs

- Integrity Test - Disjoint Signatures vs Encompassing Signatures :
  - Disjoint - One or more signatures covering entire set of module code (multiple binaries)
  - Encompassing - Single signature for entire set of code

The Diff: Roles, Services and Authentication

- Only Crypto-Officer role is required (User role optional)
- “Show Version” Service
  - Allowing the module version information to be verified
- SL 2 Authentication mechanisms must be enforced by the module
  - Cannot rely on procedural enforcement
- Other requirements (password size etc.) detailed in ***SP 800-140E***
- Default Authentication data/credentials (initial use) must be changed
- SL 4 requires multi-factor authentication

The Diff: Let's get physical (Physical Security)

- Changes mostly at SL 3 and SL 4
- Added temperature relationship to hard coating or potting materials
- SL 3 Tamper Evident seals require numbering or other unique identifier
- SL 3 requires EFP (Environmental Failure Protection) or EFT (Environmental Failure Testing)
- SL 4 requires EFP for temperature and voltage
- SL 4 requires protection from Fault Induction (changes due to voltage/laser/radiation techniques)

The Diff: Software/Firmware and OS Security

- Software modules now can achieve SL 2 without Common Criteria dependency
- SL 2 OS requirements for RBAC, I&A and detailed audit logging (similar to Common Criteria OSPP)
- SL 2 shall only include code in executable form (no source, object code or scripts!)
- No SL 3 for Software modules
- EDC (like a 16-bit CRC) no longer acceptable for firmware

The Diff: Actual Non-Invasive Security Requirements

- Non-Invasive (side-channel) Attacks
  - Attacks performed with no direct physical contact
  - Do not alter or change the state of the module
- Differential Power Analysis (DPA)
  - Analysis of electrical power consumption variation
- Simple Power Analysis (SPA)
  - Analysis of instruction execution patterns in relation to power consumption
- Not mandatory at SL 1 or SL 2
- SL 3 & SL 4 - Test metrics to be defined in ***SP 800-140F***

The Diff: It's "Zeroisation", Not "Zeroization"!

- SL 2 (+) module must implement zeroisation logic (cannot be procedural)
- Status output indicator when zeroisation is complete
- Must overwrite SSPs with 0's, 1's or random data
- Temporary SSPs zeroised when no longer needed
- SL 4 SSP zeroisation immediate & non-interruptible
- SL 4 zeroise all SSPs and return to factory state

The Diff: So long, and thanks for all the Fish!

- Bye, Bye “RNG” – Now called ***RBG***
- See you later “NDRNG”- Now called ***Entropy***
- Adios “CRNGT”!
- Cya! to the EMI/EMC stuff – No FCC Class A and B requirements!
- Sayonara “Z” - No Formal Modeling requirements at SL 4 in FIPS 140-3!

RSAConference2020

FIPS 140-3: Key Dates

FIPS 140-3 transition: Important dates

- **March 22nd, 2020** – IG and SP 800-140 series published
- **~March 2020** - CMVP management manual & programmatic guidance (for labs) published
- **September 22nd, 2020** - CMVP will accept 140-3 submissions
- **September 22nd, 2021** – FIPS 140-2 submissions no longer accepted by CMVP

NIST FIPS 140-3 Website: https://csrc.nist.gov/projects/fips-140-3-development#sp800-140

RSAConference2020

“APPLY”

Our Advice: Tips To Survive the Transition

Apply: Take a breath -2 certs aren't going anywhere

- FIPS 140-2 module validations are still valid for **5 years**
- A FIPS 140-2 validation certificate awarded August 15th, 2021 - would be valid until **August 15th, 2026**!
- CMVP will not be revoking FIPS 140-2 certificates as part of the FIPS 140-3 transition
- U.S. federal agencies (and others) may continue to purchase products on the FIPS 140-2 CMVP validated modules list

Apply: Can I achieve BOTH FIPS 140-2 and FIPS 140-3?

- Cautiously, I say *YES (@ SL 1 & 2) – but alas, the devil is in the details!*
- Much could change based on NIST SP 800-140X and IG (March 2020)
- May not be practical to begin testing until the middle of 2020
- Some uncertainty on correct interpretation of ambiguous terminology
- Early adopters will face challenges on how to test certain requirements
- Evaluate your business requirements

Apply: Things (we think) you can do today (without forking code)

- Implement automated security tool testing (ie. SCA tools)
- Implement FIPS 140-3 Design Assurance requirements (mostly procedural & docs)
- Require default authentication data to be changed during initial setup
- Enforce strong authentication mechanisms (NIST SP 800-63B, a CC OSPP or NDcPP)
- Do ALL self-tests at power-up (per FIPS 140-2 requirements) this meets FIPS pre-op 140-3 requirements
- Dependent on the desired level and module type:
  - Implement FIPS 140-3 Zeroisation requirements now
  - Implement FIPS 140-3 Bypass self-test requirements now

Apply: Where can I get “FIPS 140-3”?

- NIST have arranged for 2000 free licenses to researchers, academics and small organizations
  - Request applications @ https://csrc.nist.gov/Projects/FIPS-140-3-Transition-Effort/Transition-to-FIPS-140-3

- ISO/IEC 19790:2012/Cor 1:2015 – $108 USD
- ISO/IEC 24759:2017 - $200 USD
  - *Note: ISO/IEC 19790:2012/Cor 1:2015 – Make sure you are using this version!

Apply: In closing, points to remember …

- Move to FIPS 140-3 is a good thing!
- Labs and CMVP reviewers will need some feeling out time
- Still ambiguity especially at SL 3 & SL 4
- FIPS 140-2 is the "*devil we know*" … interpretations are clear – short term easier & faster (cheaper)
- FIPS 140-2 certs are valid for 5 years (buy yourself some time)
- A "diff" of FIPS 140-3 is ***NOT*** complete unless it includes SP 800-140X series
- Again, evaluate your business requirements – most stakeholders want a cert ***A$AP***
- Algorithms not directly affected by FIPS 140-3 (See NIST SP 800-131Ar2)
- Free copies of the ISO are available

Apply: Other changes that should be on your radar

- August 2020 – "Classic" CAVP testing retired. ACVTS only!
- September 2020 – RSA transition – FIPS 186-4 only
- November 2020 – Full SP 800-90B (Entropy) compliance required
- January 2021 – Non-SP 800-56A Key Agreement schemes disallowed (per SP 800-131Ar2)
- ~2022 - NIST Post-Quantum Crypto Standardization Process
  - SP 800-131Ar2 – Recognizes RSA and DH/ED DH Key agreement are at risk
- January 2023 – Triple-DES encryption disallowed (SP 800-131Ar2)

Apply: How to stay in the loop?

- NIST FIPS 140-3 project site (https://csrc.nist.gov/Projects/FIPS-140-3-Development#schedule)
- Check our blog for detailed diff analysis (https://blog.acumensecurity.net/)
- Join the Acumen mailing list for all CMVP updates (ping me)
- Join the FIPS 140-3 CMUF Working Group
- ICMC Conference, April 2020 - Washington DC

RSAConference2020

Q & A Time

Ryan Thomas

CST Lab Manager

rthomas@acumensecurity.net

intertek acumen security