What is the Cryptographic Boundary?

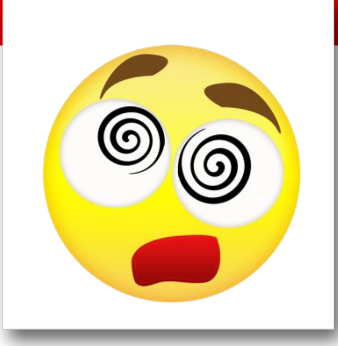
Ying-Chong "Hedy" Leung
Senior Consultant
atsec information security corp.
hedy@atsec.com

ICMC 2016, May 18-20, 2016, Shaw Centre Ottawa, Ontario

Why do we care?

- Requirement to specify the cryptographic boundary is the first bullet in the first section under the “Security Requirement” chapter of the FIPS 140-2 standard.
    - Define Module Type: Software? Firmware? Hardware? Hybrid?
    - Section 4.2 Cryptographic Module Ports and Interfaces
    - Section 4.3.2 Services
    - IG 7.7 Key Entry and Output
    - IG 7.14 Entropy CAVEATS
    - Section 4.9 Integrity Test, Software/Firmware Load Test
    - Section 4.10.1 Configuration Management
- Any change made within the boundary may cause RE-VALIDATION!

SO CONFUSING…



- “Physical boundary”
- “Defined boundary of the module”
- “Modules defined boundary”
- “Cryptographic module logical boundary”
- “Cryptographic module boundary”
- “Boundary of the cryptographic module”
- “Cryptographic boundary of the module”
- “Logical boundary”

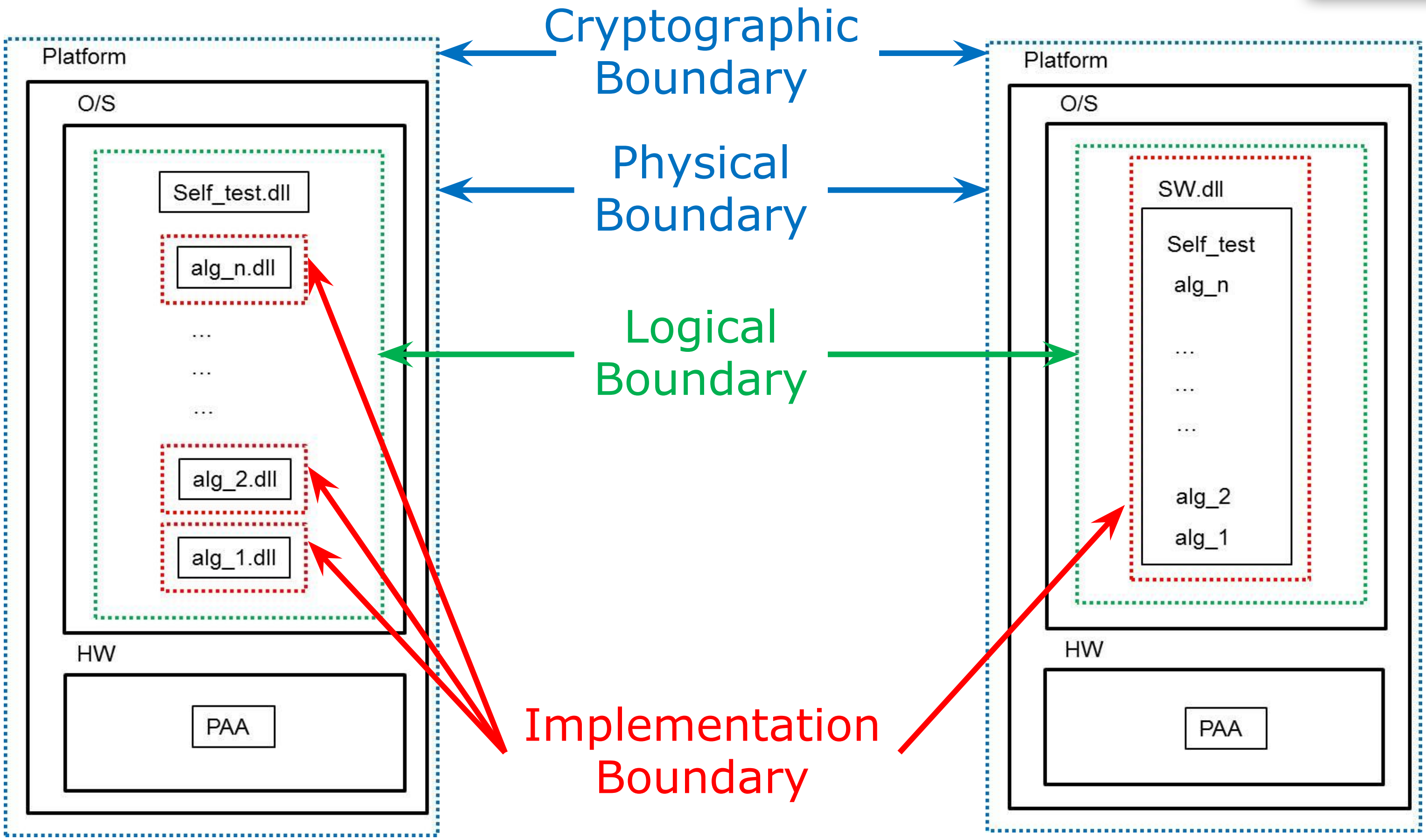
Terminology

- Cryptographic Boundary
  - FIPS 140-2 definition: “An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.”
- Cryptographic Algorithm Boundary
  - Or Implementation Boundary
  - The boundary of the algorithm implementation
  - This does not have to be the same as the cryptographic module boundary (CAVP FAQ GCM.3)

Terminology

- Physical Boundary
  - The platform on which the software/firmware [and operating system] reside
  - Same as Cryptographic Boundary
- Logical Boundary
  - The set of software/firmware components that implement the cryptographic mechanisms
  - “The logical boundary is wholly contained within the physical boundary. (IG 1.16, 1.17)”

Software and Firmware



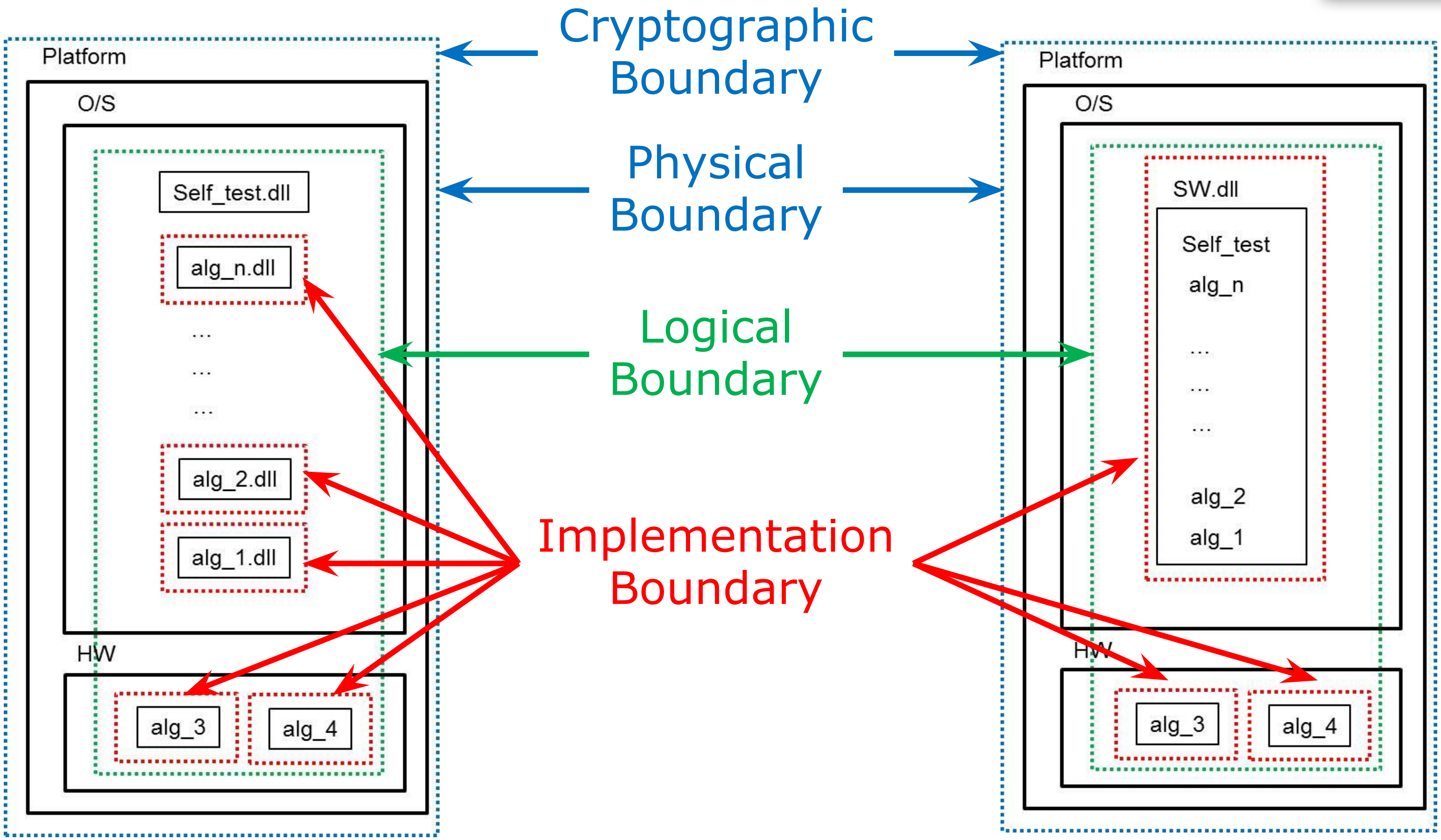
Cryptographic Boundary

Physical Boundary

Logical Boundary

Implementation Boundary

Software/Firmware-Hybrid



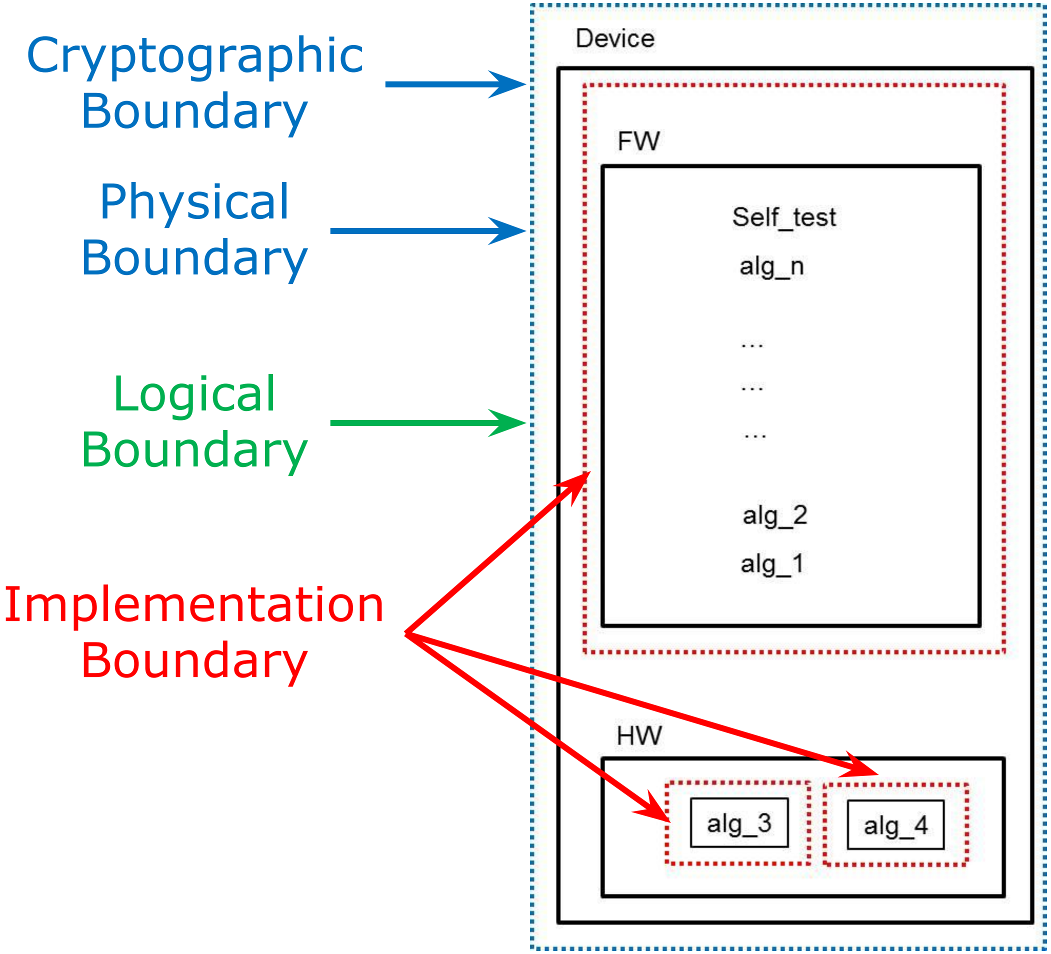
Cryptographic Boundary

Physical Boundary

Logical Boundary

Implementation Boundary

Hardware



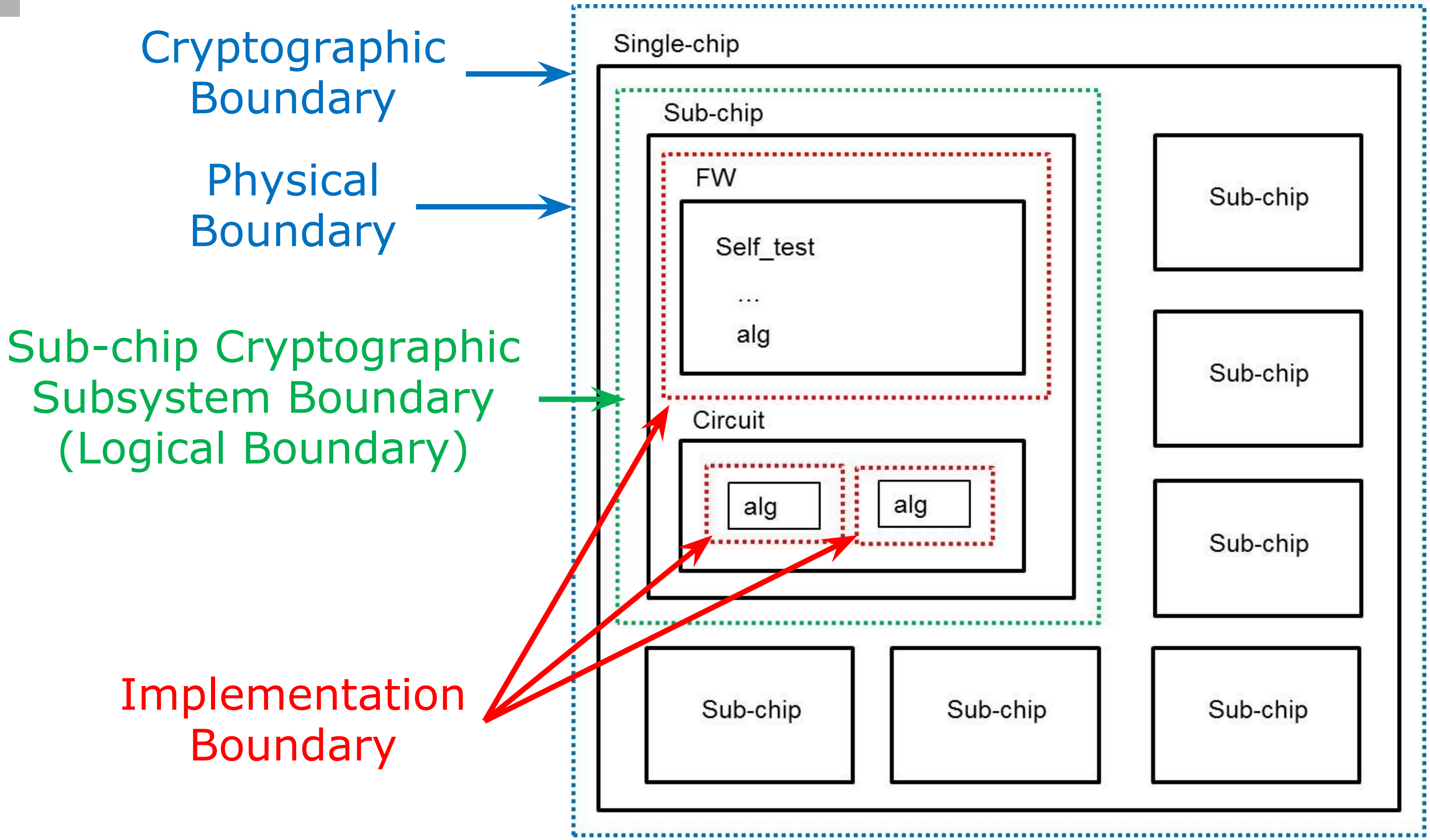
Cryptographic Boundary

Physical Boundary

Logical Boundary

Implementation Boundary

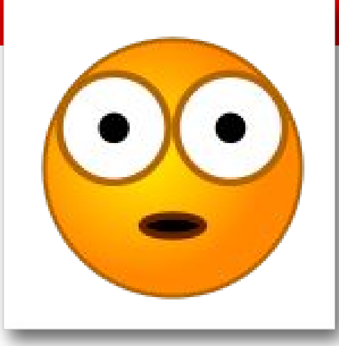
Hardware: Sub-chip Cryptographic Subsystem



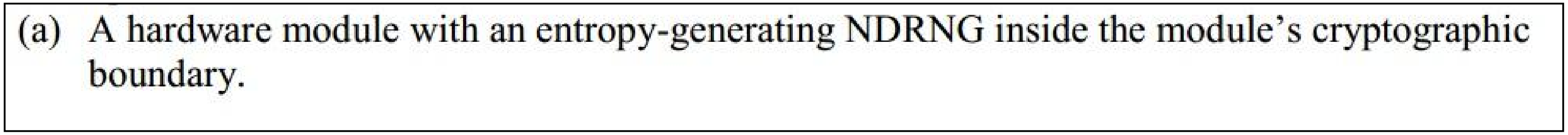
Defining a small boundary, and a small validation scope…

- CMVP
  - FIPS 140-2 states, "A cryptographic module shall implement at least one Approved security function used in an Approved mode of operation."
  - FIPS 140-2 IG 1.1 2004-02-27 states regarding a Cryptographic Module Name, "It is not acceptable to provide a module name that represents a module that has more components than the modules defined boundary. "
- CAVP
  - CAVP FAQ TDES.2, "Tighten the algorithmic boundary."

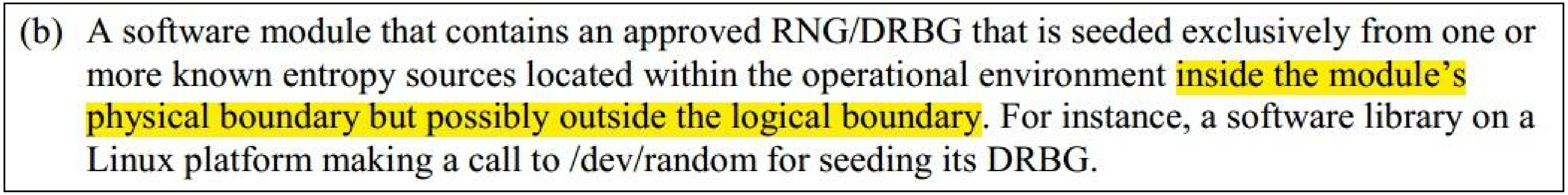
Recently…



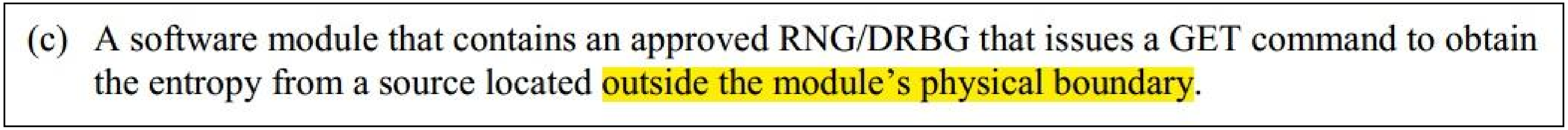
- FIPS 140-2 IG 7.14 2015-11-12



(a) A hardware module with an entropy-generating NDRNG inside the module’s cryptographic boundary.



(b) A software module that contains an approved RNG/DRBG that is seeded exclusively from one or more known entropy sources located within the operational environment inside the module’s physical boundary but possibly outside the logical boundary. For instance, a software library on a Linux platform making a call to /dev/random for seeding its DRBG.

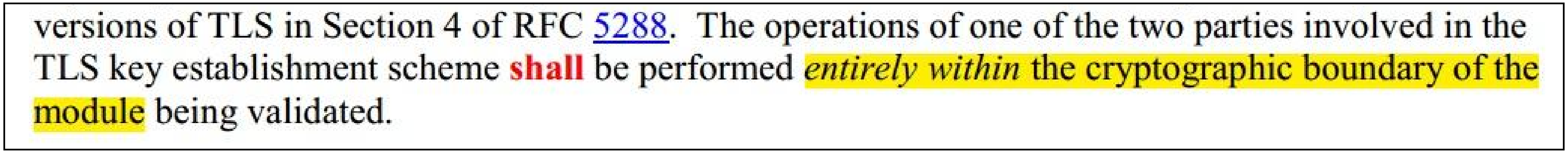


(c) A software module that contains an approved RNG/DRBG that issues a GET command to obtain the entropy from a source located outside the module’s physical boundary.

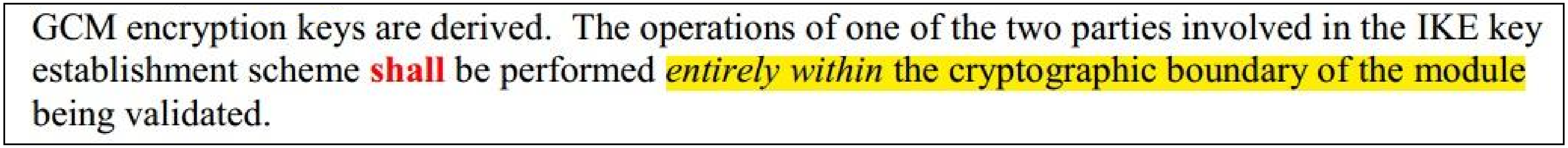
- Entropy strength estimation is provided by the vendor!
- Entropy Analysis Report is provided by the lab for submission!

Apparently…

- FIPS 140-2 IG A.5 2015-08-07



versions of TLS in Section 4 of RFC 5288. The operations of one of the two parties involved in the TLS key establishment scheme **shall** be performed *entirely within* the cryptographic boundary of the module being validated.



GCM encryption keys are derived. The operations of one of the two parties involved in the IKE key establishment scheme **shall** be performed *entirely within* the cryptographic boundary of the module being validated.

- What does “the cryptographic boundary of the module” refer to? The Logical Boundary (LB) or Physical Boundary (PB)?
  - Within the PB and outside the LB, why do we need to review source code and verify the out of scope components?
  - Within the PB and LB, enlarge the Logical Boundary!

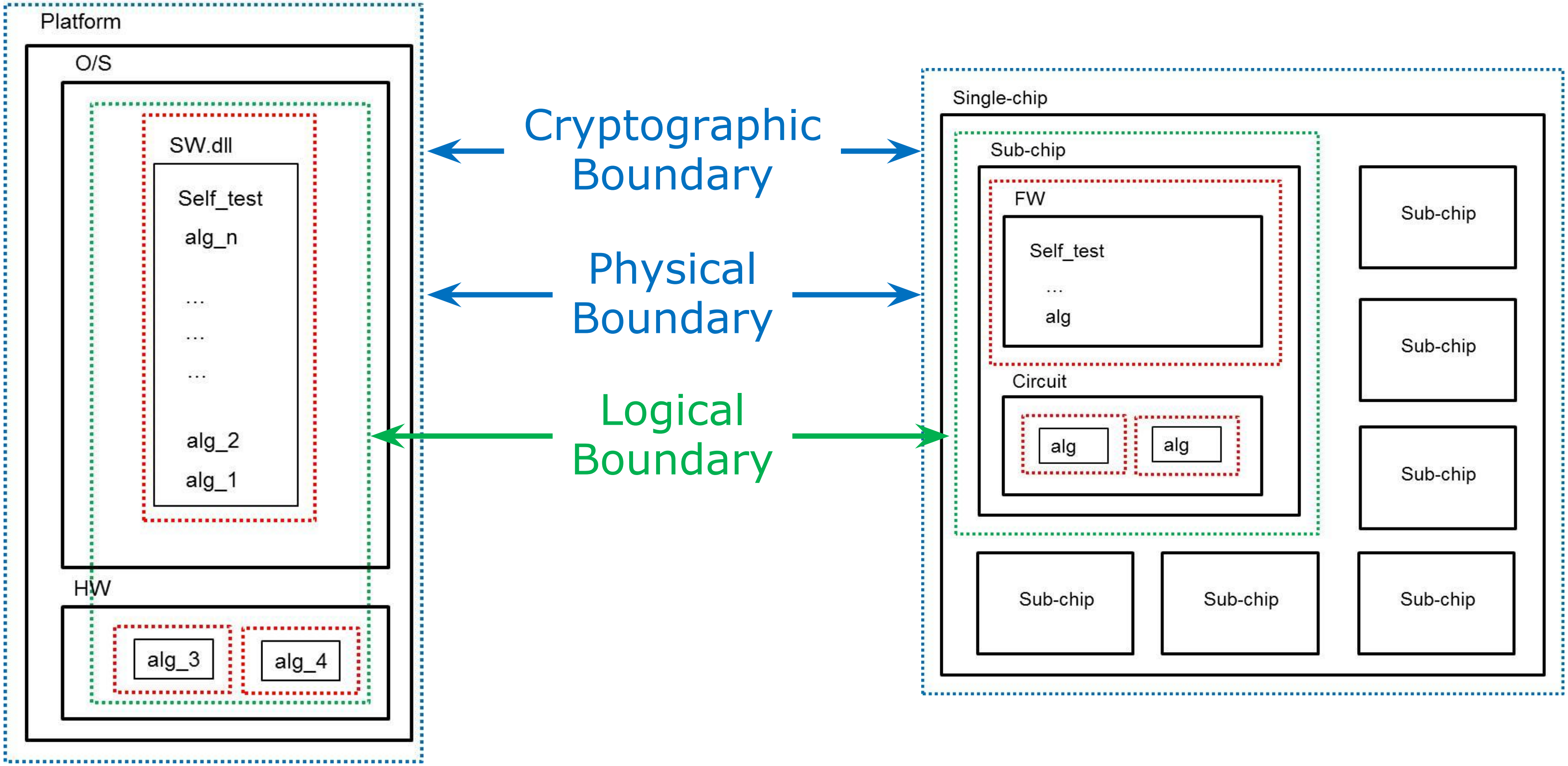
Impact of enlarging the validation scope

We want a small scope, and a small boundary…

I want to know everything inside and out of your module, no matter if you developed it or not! You are responsible!

- Impact of Enlarging the Logical Boundary
  - Section 4.2 Cryptographic Module Ports and Interfaces
  - Section 4.9 Integrity Test, Software/Firmware Load Test
  - Section 4.10.1 Configuration Management
  - Revalidation may exceed 30% code change

More Issues…

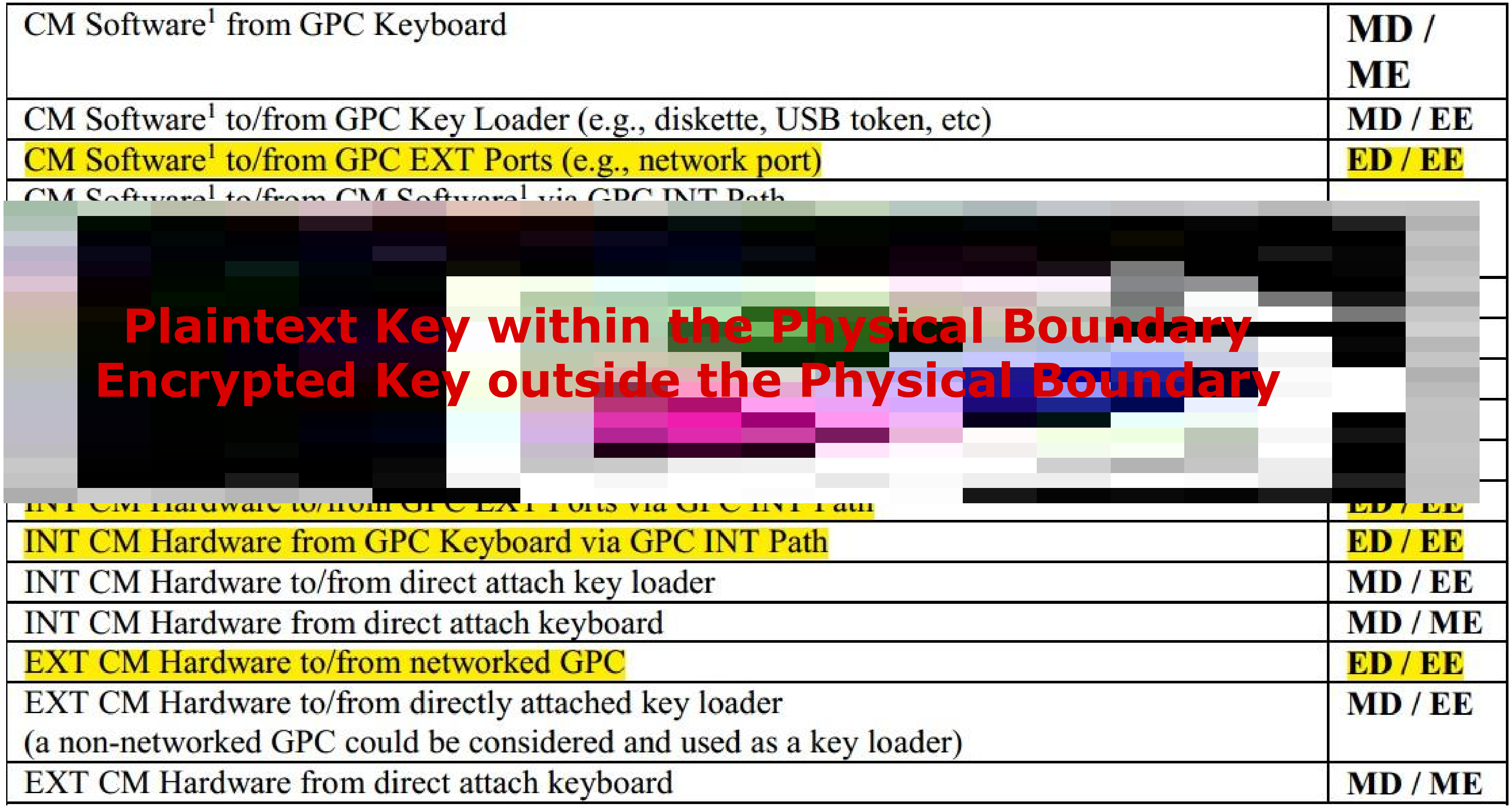


Cryptographic Boundary

Physical Boundary

Logical Boundary

IG 7.7

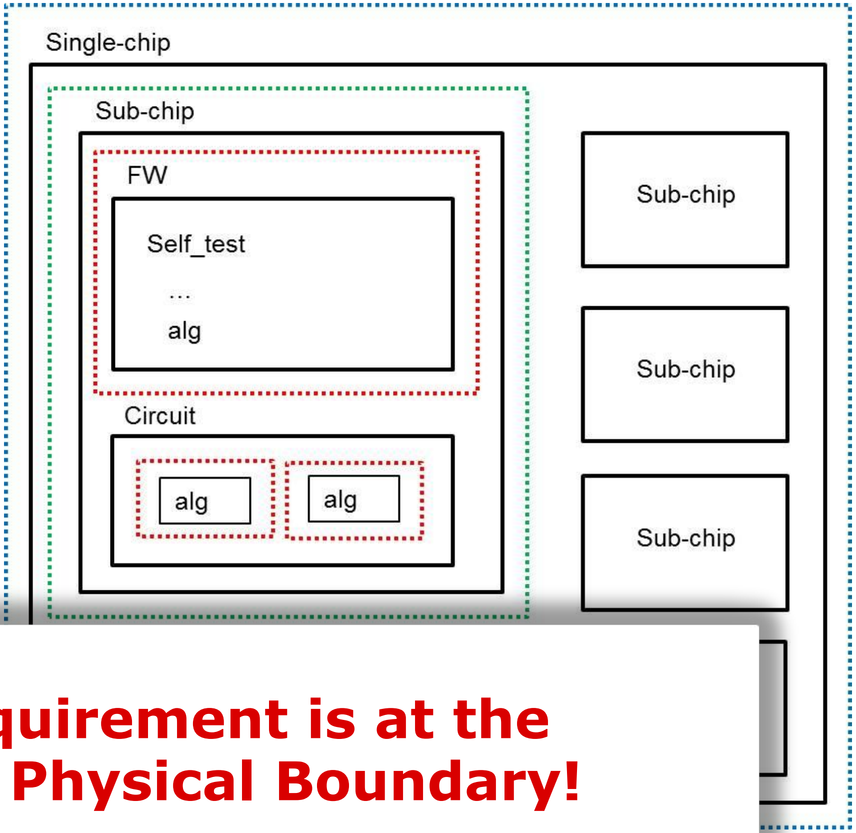


CM Software[1] from GPC Keyboard	**MD / ME**
CM Software[1] to/from GPC Key Loader (e.g., diskette, USB token, etc)	**MD / EE**
CM Software[1] to/from GPC EXT Ports (e.g., network port)	**ED / EE**
[redacted]	[redacted]
INT CM Hardware from GPC Keyboard via GPC INT Path	**ED / EE**
INT CM Hardware to/from direct attach key loader	**MD / EE**
INT CM Hardware from direct attach keyboard	**MD / ME**
EXT CM Hardware to/from networked GPC	**ED / EE**
EXT CM Hardware to/from directly attached key loader (a non-networked GPC could be considered and used as a key loader)	**MD / EE**
EXT CM Hardware from direct attach keyboard	**MD / ME**

Plaintext Key within the Physical Boundary
Encrypted Key outside the Physical Boundary

Sub-Chip Cryptographic Subsystem (IG 1.20)

- Encrypted Key entry or output at the sub-chip cryptographic subsystem boundary, except when:
  - Transferring CSPs between two disjointed sub-chip cryptographic subsystems via a Trusted Path.



Key Entry and Output requirement is at the Logical Boundary, not the Physical Boundary!

Conclusion

- Many different terms refer to the module’s boundary in the IG. It’s complicated.
- The vendor should define the module’s boundary carefully and properly, and engage the lab at an early stage of development.
- Be aware that the CMVP has a tendency to enlarge the validation scope and the module’s boundary.
- There is asymmetric treatment for Key Entry and Output between software and sub-chip cryptographic subsystem.

Thank You