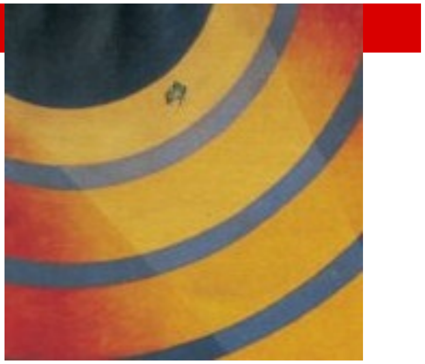
the information security provider

What type of module am I?

Yi Mao, Ph.D., CISSP
CST Lab Manager
atsec information security corp.
Email: yi@atsec.com

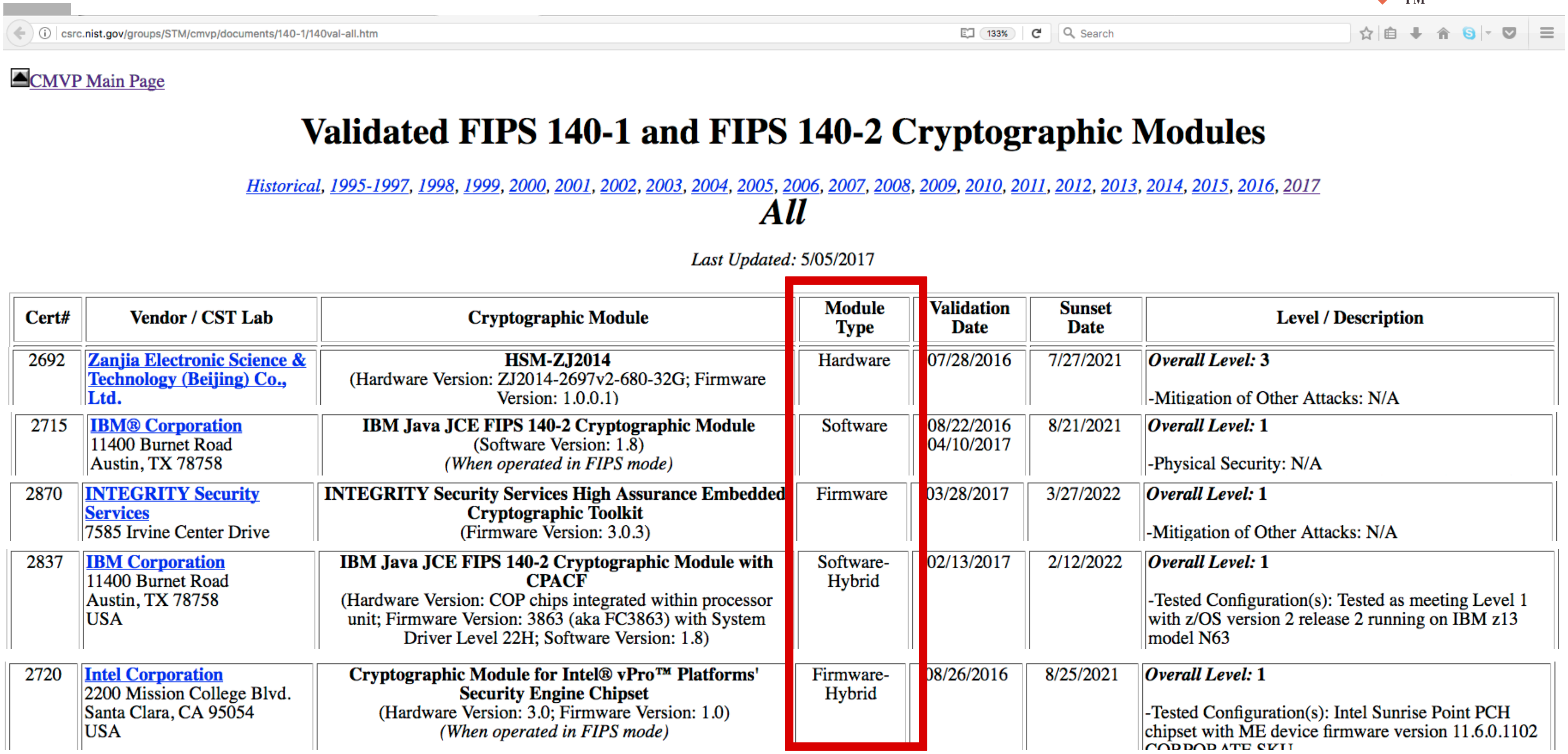
ICMC 2017, Westin Arlington Gateway, Washington DC, May 16-19, 2017

Agenda



- The Five types of modules in FIPS 140-2
- The troubles with hybrid modules
  (demonstrated by a video clip)
- The old IG 1.21 on Processor Algorithm Accelerator (PAA)
- The new IG 1.21 on Processor Algorithm Implementation (PAI)
- Suggestions to update IG 1.9
- Expecting a happy ending (video clip continued)

Module Types on Validation Lists



csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

CMVP Main Page

Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules

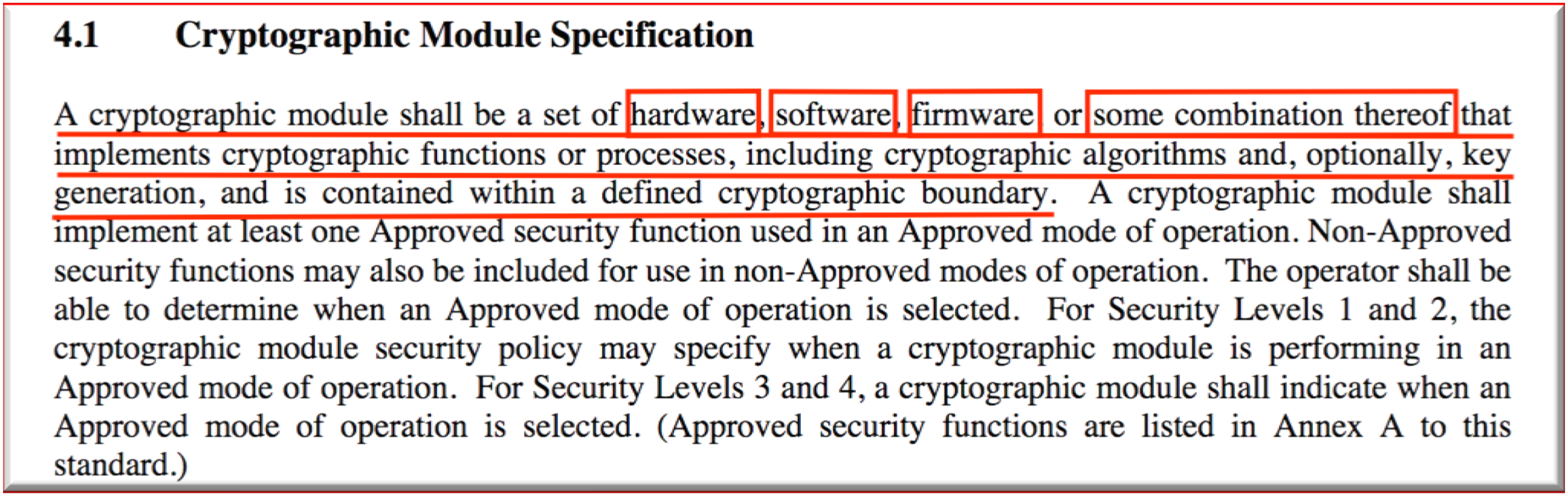
Historical, *1995-1997*, *1998*, *1999*, *2000*, *2001*, *2002*, *2003*, *2004*, *2005*, *2006*, *2007*, *2008*, *2009*, *2010*, *2011*, *2012*, *2013*, *2014*, *2015*, *2016*, *2017*

All

Last Updated: 5/05/2017

Cert#	Vendor / CST Lab	Cryptographic Module	Module Type	Validation Date	Sunset Date	Level / Description
2692	Zanjia Electronic Science & Technology (Beijing) Co., Ltd.	**HSM-ZJ2014** (Hardware Version: ZJ2014-2697v2-680-32G; Firmware Version: 1.0.0.1)	Hardware	07/28/2016	7/27/2021	***Overall Level:* 3** -Mitigation of Other Attacks: N/A
2715	IBM® Corporation 11400 Burnet Road Austin, TX 78758	**IBM Java JCE FIPS 140-2 Cryptographic Module** (Software Version: 1.8) *(When operated in FIPS mode)*	Software	08/22/2016 04/10/2017	8/21/2021	***Overall Level:* 1** -Physical Security: N/A
2870	INTEGRITY Security Services 7585 Irvine Center Drive	**INTEGRITY Security Services High Assurance Embedded Cryptographic Toolkit** (Firmware Version: 3.0.3)	Firmware	03/28/2017	3/27/2022	***Overall Level:* 1** -Mitigation of Other Attacks: N/A
2837	IBM Corporation 11400 Burnet Road Austin, TX 78758 USA	**IBM Java JCE FIPS 140-2 Cryptographic Module with CPACF** (Hardware Version: COP chips integrated within processor unit; Firmware Version: 3863 (aka FC3863) with System Driver Level 22H; Software Version: 1.8)	Software-Hybrid	02/13/2017	2/12/2022	***Overall Level:* 1** -Tested Configuration(s): Tested as meeting Level 1 with z/OS version 2 release 2 running on IBM z13 model N63
2720	Intel Corporation 2200 Mission College Blvd. Santa Clara, CA 95054 USA	**Cryptographic Module for Intel® vPro™ Platforms' Security Engine Chipset** (Hardware Version: 3.0; Firmware Version: 1.0) *(When operated in FIPS mode)*	Firmware-Hybrid	08/26/2016	8/25/2021	***Overall Level:* 1** -Tested Configuration(s): Intel Sunrise Point PCH chipset with ME device firmware version 11.6.0.1102 CORPORATE SKU

Cryptographic Module Specification in FIPS 140-2



4.1 Cryptographic Module Specification

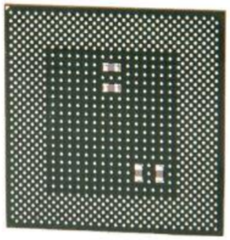
A cryptographic module shall be a set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary. A cryptographic module shall implement at least one Approved security function used in an Approved mode of operation. Non-Approved security functions may also be included for use in non-Approved modes of operation. The operator shall be able to determine when an Approved mode of operation is selected. For Security Levels 1 and 2, the cryptographic module security policy may specify when a cryptographic module is performing in an Approved mode of operation. For Security Levels 3 and 4, a cryptographic module shall indicate when an Approved mode of operation is selected. (Approved security functions are listed in Annex A to this standard.)

What is a Hardware module?

- On page 6, FIPS 140-2 defines:

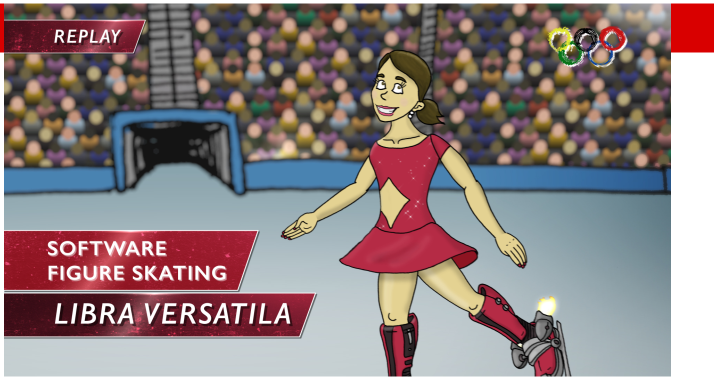
Hardware: the physical equipment within the cryptographic boundary used to process programs and data.

- Examples of Hardware modules from the validation list:

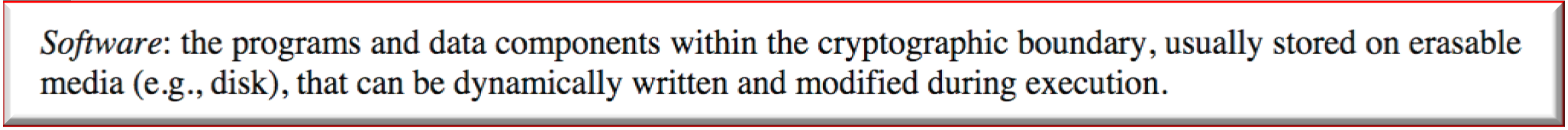


- Observed common features of hardware modules:
  - ✓ They have a physical enclosure.
  - ✓ The logical boundary is the same as physical boundary.
  - ✓ They may contain software and firmware components.
  - ✓ They implement not only cryptographic functions but also non-cryptographic functions.

What is a Software module?

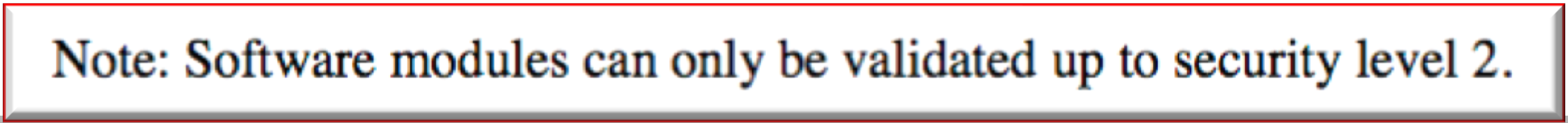


- On page 8, FIPS 140-2 defines:



Software: the programs and data components within the cryptographic boundary, usually stored on erasable media (e.g., disk), that can be dynamically written and modified during execution.

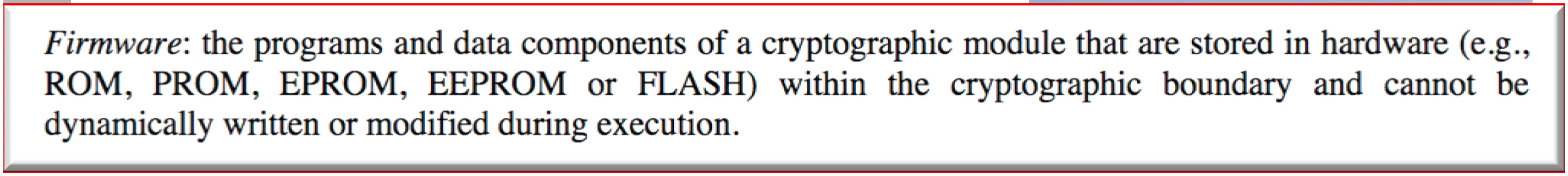
- **IG 1.16** provides interpretation for Software modules:
  - ✓ The physical boundary is the platform in which the software and OS reside.
  - ✓ The logical boundary is the software that implements the cryptographic functions.
  - ✓ The software load test is applicable.
  - ✓ **Physical security may not be applicable.**
  - ✓ **The power-on Approved integrity test (e.g. digital signature, keyed-hash) shall be performed.**
- Observed common features of Software modules:
  - ✓ **Their OE is modifiable.**
  - ✓ Their physical security and EMI/EMC compliance rely on their platform.
- FIPS 140-2 Annex B sets the limit of the FIPS validation level for Software modules



Note: Software modules can only be validated up to security level 2.

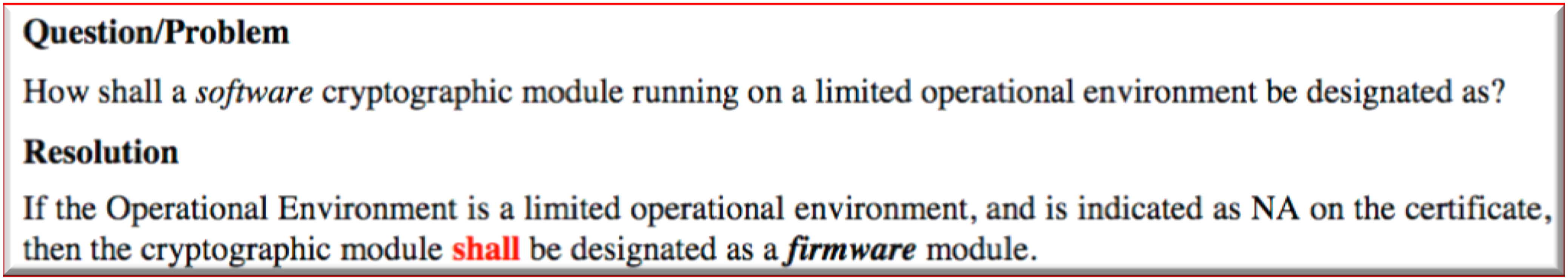
What is a Firmware module?

- On page 6, FIPS 140-2 defines:



Firmware: the programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

- **IG 1.3** defines the Firmware module designation:



Question/Problem

How shall a *software* cryptographic module running on a limited operational environment be designated as?

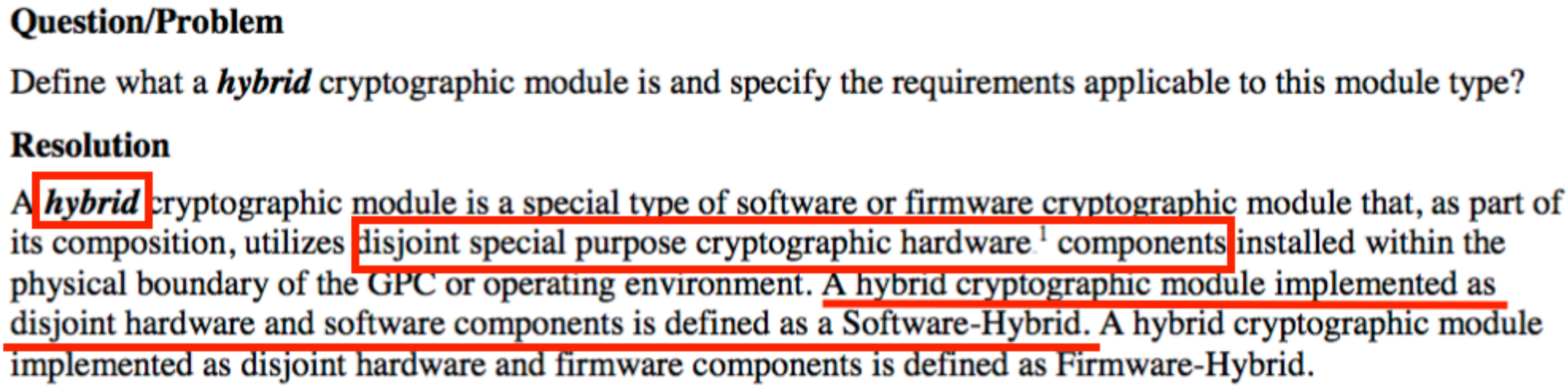
Resolution

If the Operational Environment is a limited operational environment, and is indicated as NA on the certificate, then the cryptographic module **shall** be designated as a ***firmware*** module.

- **IG 1.17** provides the following additional guidance:
  - ✓ The physical/logical boundary definition is the same as for a Software module.
  - ✓ The firmware load test is applicable.
  - ✓ **Physical security is applicable.**
  - ✓ **Error detection code (e.g. CRC 16) is allowed for the power-on integrity test.**
  - ✓ **Their OE is limited or non-modifiable.**

What is a Software-Hybrid module?

- **IG 1.9** defines a Software-Hybrid module:



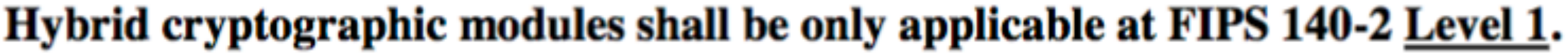
Question/Problem

Define what a ***hybrid*** cryptographic module is and specify the requirements applicable to this module type?

Resolution

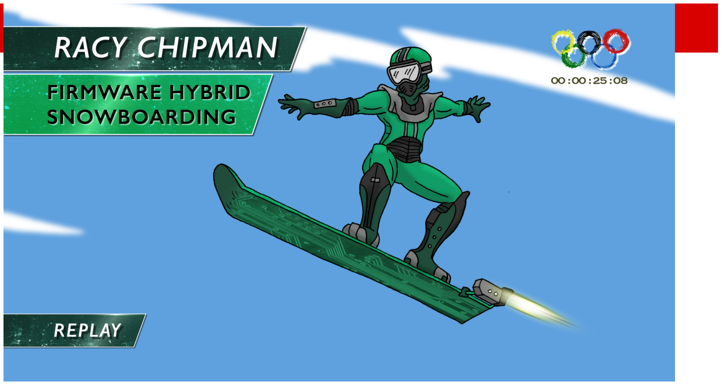
A ***hybrid*** cryptographic module is a special type of software or firmware cryptographic module that, as part of its composition, utilizes disjoint special purpose cryptographic hardware[1] components installed within the physical boundary of the GPC or operating environment. A hybrid cryptographic module implemented as disjoint hardware and software components is defined as a Software-Hybrid. A hybrid cryptographic module implemented as disjoint hardware and firmware components is defined as Firmware-Hybrid.

- Some key requirements in **IG 1.9** for Software-Hybrid module:
  - ✓ The software component logical interface is the external interface of the hybrid module.
  - ✓ **Physical security is applicable due to the hardware component.**
  - ✓ **A Software-Hybrid module has modifiable OS and OE requirements are applicable.**
  - ✓ **A strong integrity test shall be performed on the software component(s).**
  - ✓ **Keys/CSPs transferred between components of a hybrid module may be in plaintext.**

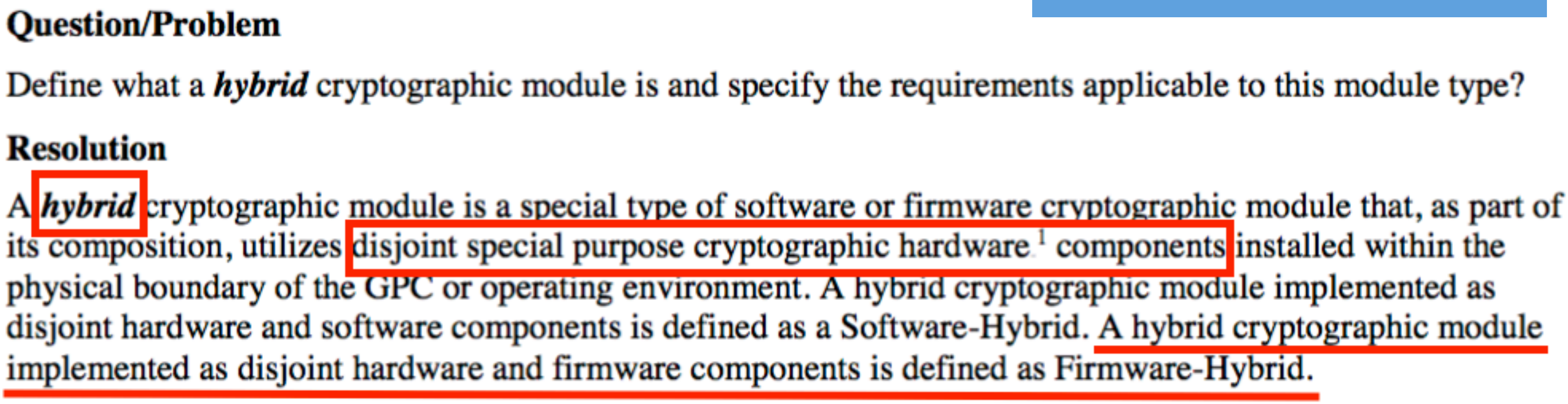


Hybrid cryptographic modules shall be only applicable at FIPS 140-2 Level 1.

What is a Firmware-Hybrid module?



- **IG 1.9** defines a Firmware-Hybrid module:



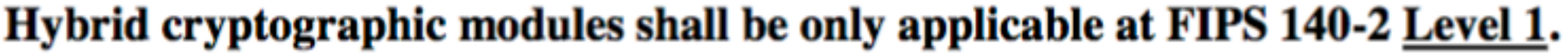
Question/Problem

Define what a ***hybrid*** cryptographic module is and specify the requirements applicable to this module type?

Resolution

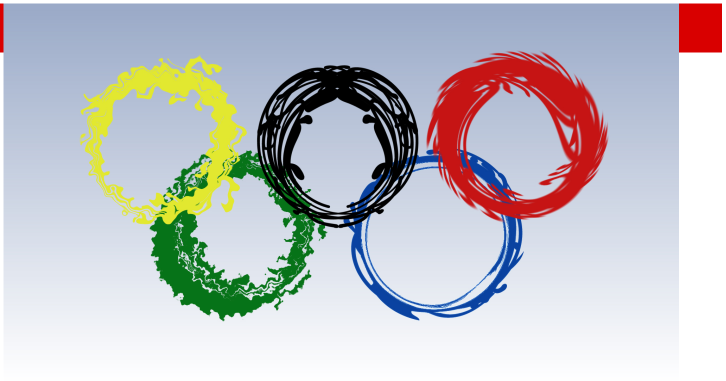
A ***hybrid*** cryptographic module is a special type of software or firmware cryptographic module that, as part of its composition, utilizes disjoint special purpose cryptographic hardware[1] components installed within the physical boundary of the GPC or operating environment. A hybrid cryptographic module implemented as disjoint hardware and software components is defined as a Software-Hybrid. A hybrid cryptographic module implemented as disjoint hardware and firmware components is defined as Firmware-Hybrid.

- Some key requirements in **IG 1.9** for Firmware-Hybrid module:
  - ✓ The firmware component logical interface is the external interface of the hybrid module.
  - ✓ **Physical security is applicable due to the hardware component.**
  - ✓ **A Firmware-Hybrid module has non-modifiable or limited OS.**
  - ✓ **Error detection code may be used for integrity test on the firmware component(s).**
  - ✓ **Keys/CSPs transferred between components of a hybrid module may be in plaintext.**



Hybrid cryptographic modules shall be only applicable at FIPS 140-2 Level 1.

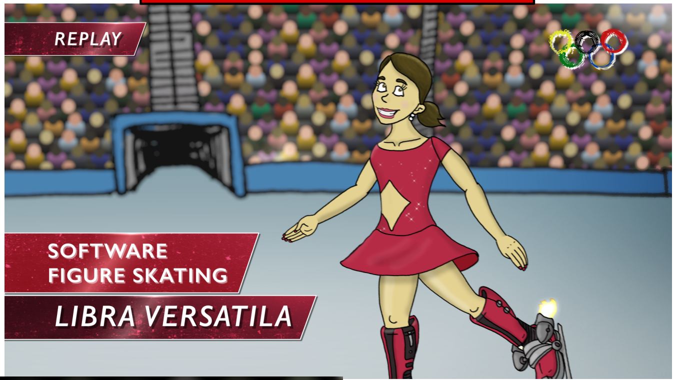
A “family picture” of modules

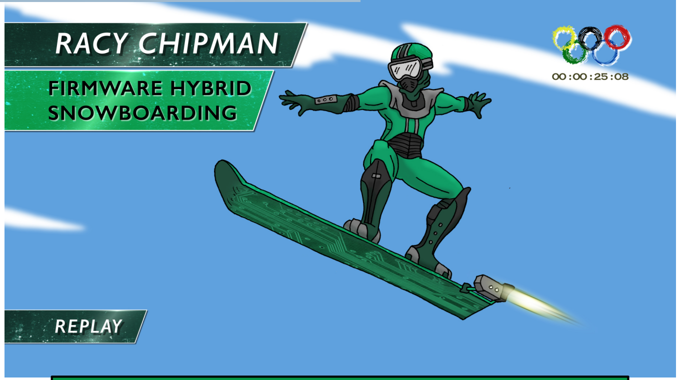


Firmware

Hardware

Software





Software-Hybrid

Software-Hybrid

Play the first half of the clip:
https://vimeo.com/217611269

What’s wrong with Libra’s skates?
Too advanced!

A software module has dependency on its Operational Environment:

- Processor
- Operating System

An advanced processor may have built-in acceleration functions:

- Simple mathematical construct
- Partial algorithm implementation
- Complete algorithm implementation

Here is where the trouble begins: the dividing line between software module and software-hardware hybrid module becomes blurred.

Why does Libra cry?
Different skates, different events!

Analogy:

- Libra: a software library module
- A pair of skates: a platform on which a software runs

Imaginary problem for Libra:

- Wearing less advanced skates she can compete in figure skating event.
- Wearing advanced skates she must compete in speed skating event.

Real-world problem for module validation:

- Running on a less advanced platform, the module is software.
- Running on an advance platform, the module is a hybrid.

Vendors cry:
Different platforms, different validations!

This is a serious problem:

- CMVP Rule:
  Different types of modules cannot be certified in one validation.
- Consequence:
  The same software module running on multiple platforms
  must be validated separately for different platforms, which implies:
  - ➢ more NIST fees
  - ➢ more lab fee
  - ➢ longer certification time
  - ➢ multiplied effort for future re-validations

Old IG 1.21 Processor Algorithm Accelerators (PAA) (Last Modified Date: 03/02/2015)

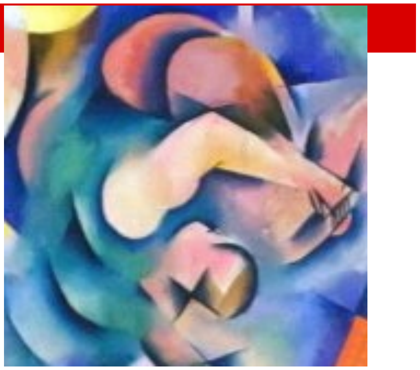
- Background section made a distinction between:
  - a mathematical construct (PAA function), and
  - a complete cryptographic algorithm (not a PAA function).

  If the processor function is deemed not a PAA, then the processor is security-specific hardware and hence the module becomes software-hardware hybrid.

Bad news for a non-PAA function: complete documentation of the entire component (i.e. processor), including HDL, shall be submitted to the testing laboratory when under test.

Good news for PAA function: no extra documentation required.

Old IG 1.21 Processor Algorithm Accelerators (PAA) Cont'd



- Question/Problem
  - What are known processors providing PAA functions?
  - How to indicate the use of PAA functions on the validation certificate?

- Resolution
  - Modified definition of hybrid module utilizing PAA functions
  - Annotations on the FIPS certificate
  - A list of known PAAs

Definition of Hybrid module in old IG 1.21

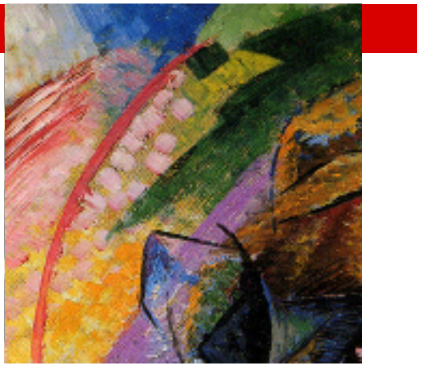
- **Software/Firmware-Hybrid Module:** If the software or firmware component of the hybrid can only support a cryptographic algorithm by exclusively utilizing the PAA capability, then the module **shall** be defined as a Software/Firmware-Hybrid Module Embodiment (IG 1.9)

- **Software/Firmware Module:** If the software or firmware component of the module can support a cryptographic algorithm natively or by utilizing the PAA capability if available, then the module shall be defined as a Software/Firmware module Embodiment, unless there are other reasons to designate the module as hybrid.

Annotations on the FIPS certificate for PAA

- **Software/Firmware-Hybrid Module:**
  - **Module versioning** information shall include the part number or version of the processor chip.
  - **Operational Environment:** Tested as meeting Level 1 with <OS> running on <platform> with PAA.
- **Software/Firmware Module:**
  - **Algorithm certificates:** the accelerated algorithms shall be tested in both native execution and PAA execution.
  - **Operational Environment:** Tested as meeting Level 1 with <OS> running on <platform> with PAA; <OS> running on <platform> without PAA.

Known PAAs in old IG 1.21



- Intel: Processors Xeon, Core i5 or i7: PAA = AES-NI
  - Accelerator sub-functions for AES implementations
- Oracle; Oracle SPARC processors based on SPARC Core S3 and later (e.g., SPARC T4, T5, M5, M6)
  - Accelerator sub-functions for AES, DES, SHA-1, SHA-256, SHA-512 and RSA

Additional Comments

NOTE 5: Please contact the CMVP to address new PAA implementations and make a determination of whether it is a full cryptographic function or not.

The granularity of PAA functions

- The classification of PAA functions and non-PAA functions are binary in IG 1.21, but just like fifty shades of grey, the complexity of the functions that different processors provide may be gradual:

simple math construct simple PAA PAA complex PAA PAI

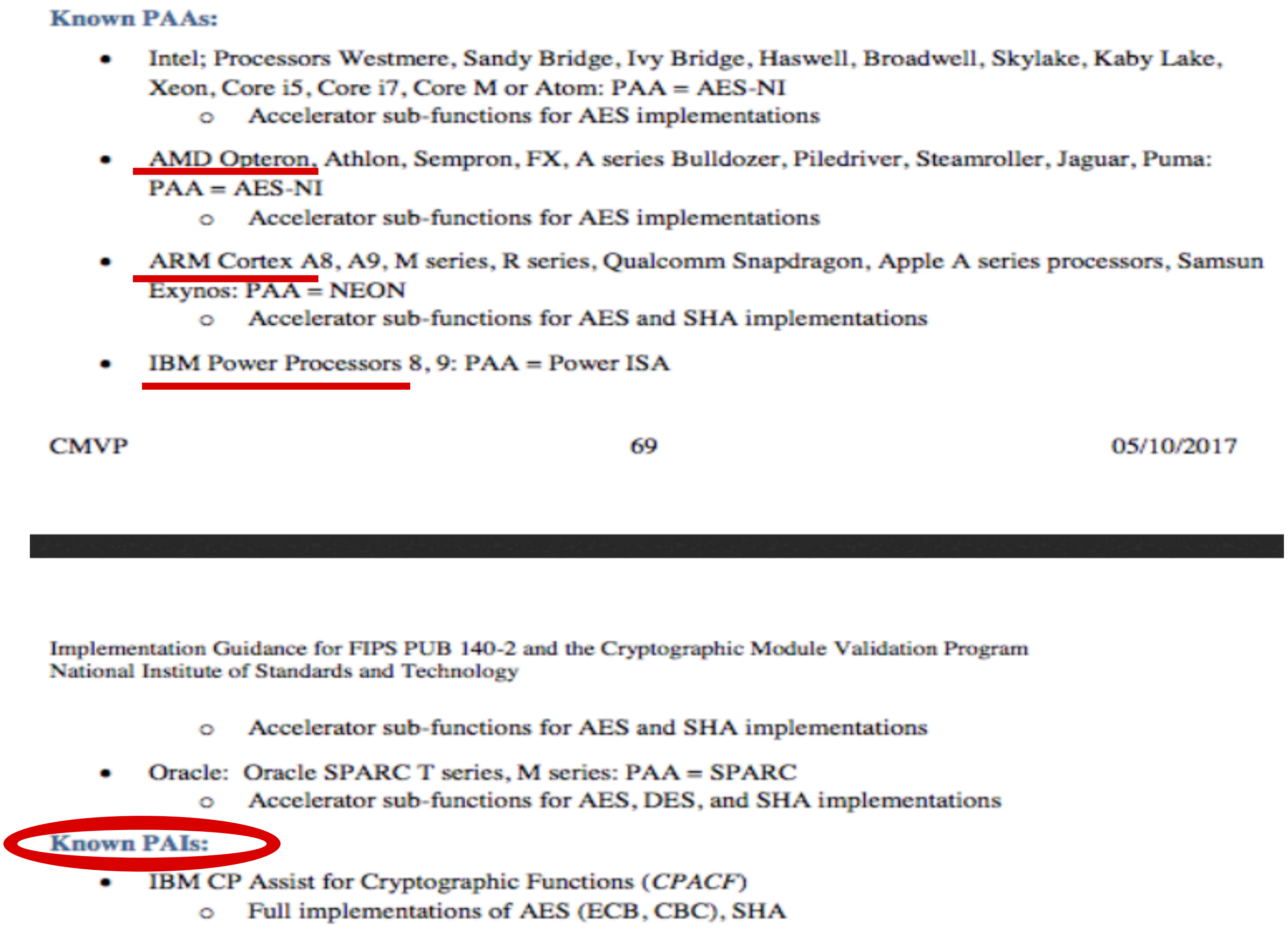
- PAI: complete processor algorithm implementation

Updated definition of Hybrid module in new IG 1.21 (Last Modified Date: 04/17/2017)

- **Software/Firmware-Hybrid Module:** If the software or firmware component of the hybrid can only support a cryptographic algorithm by exclusively utilizing the PAA or PAI capability, then the module **shall** be defined as a Software/Firmware-Hybrid Module Embodiment (IG 1.9)

- **Software/Firmware Module:** If the software or firmware component of the module can support a cryptographic algorithm natively or by utilizing the PAA or PAI capability if available, then the module shall be defined as a Software/Firmware module Embodiment, unless there are other reasons to designate the module as hybrid.

A longer list of PAAs and a new list of PAI in new IG 1.21



Known PAAs:

- Intel; Processors Westmere, Sandy Bridge, Ivy Bridge, Haswell, Broadwell, Skylake, Kaby Lake, Xeon, Core i5, Core i7, Core M or Atom: PAA = AES-NI
  - o Accelerator sub-functions for AES implementations
- AMD Opteron, Athlon, Sempron, FX, A series Bulldozer, Piledriver, Steamroller, Jaguar, Puma: PAA = AES-NI
  - o Accelerator sub-functions for AES implementations
- ARM Cortex A8, A9, M series, R series, Qualcomm Snapdragon, Apple A series processors, Samsun Exynos: PAA = NEON
  - o Accelerator sub-functions for AES and SHA implementations
- IBM Power Processors 8, 9: PAA = Power ISA

CMVP 69 05/10/2017

Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
National Institute of Standards and Technology

  - o Accelerator sub-functions for AES and SHA implementations
- Oracle: Oracle SPARC T series, M series: PAA = SPARC
  - o Accelerator sub-functions for AES, DES, and SHA implementations

Known PAIs:

- IBM CP Assist for Cryptographic Functions (*CPACF*)
  - o Full implementations of AES (ECB, CBC), SHA

What if a hardware component …

with the dedicated purpose for cryptographic functions (e.g. cryptographic hardware accelerator cards, cryptographic hardware chips):

- can be utilized by a software module in a plug-n-play fashion, and
- is often provided by a third party.

Will a software module runs on a platform with such a hardware component turn into a Hybrid module?

The root cause of the problem

- In IG 1.21 (old and new), whether or not the processor provides PAA and/or PAI in the module's operational environment overweighs the architectural design of the module itself.
  - *First* question should be: Is the module designed to have self-contained security functions and does it run correctly without any processor acceleration?
  - *Second* question can be: Is the module designed to utilize processor acceleration if available?

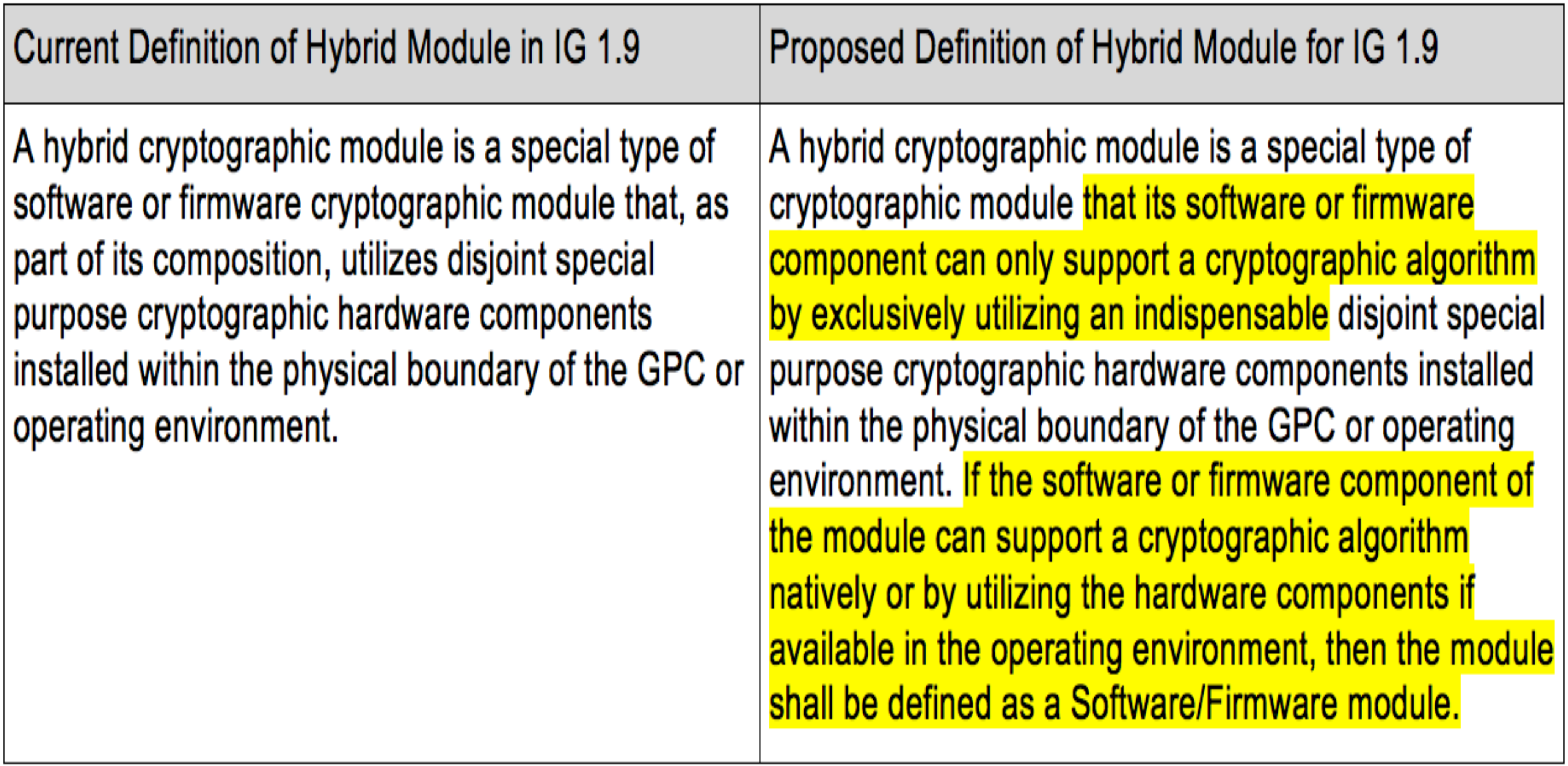
The order of these two questions was reversed in IG 1.21.

Proposing a fix

- Generalizing the thoughts from IG 1.21:
  - Software/Firmware-Hybrid Module: If the software or firmware component of the hybrid can only support a cryptographic algorithm by exclusively utilizing the ~~PAA or PAI~~ capability, then the module shall be defined as a Software/Firmware-Hybrid Module Embodiment (IG 1.9)
  - If the software or firmware component of the module can support a cryptographic algorithm natively or by utilizing the ~~PAA or PAI~~ capability if available, then the module shall be defined as a Software/Firmware module Embodiment, unless there are other reasons to designate the module as hybrid.

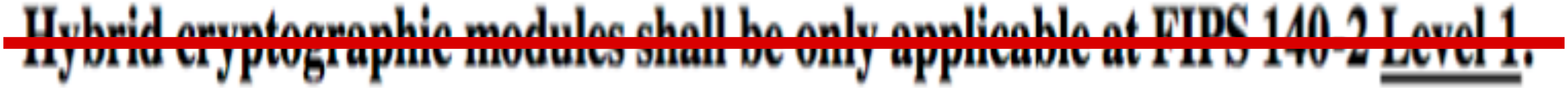
Hardware Crypto Accelerator

Updating the definition of Hybrid module in IG 1.9



Current Definition of Hybrid Module in IG 1.9	Proposed Definition of Hybrid Module for IG 1.9
A hybrid cryptographic module is a special type of software or firmware cryptographic module that, as part of its composition, utilizes disjoint special purpose cryptographic hardware components installed within the physical boundary of the GPC or operating environment.	A hybrid cryptographic module is a special type of cryptographic module that its software or firmware component can only support a cryptographic algorithm by exclusively utilizing an indispensable disjoint special purpose cryptographic hardware components installed within the physical boundary of the GPC or operating environment. If the software or firmware component of the module can support a cryptographic algorithm natively or by utilizing the hardware components if available in the operating environment, then the module shall be defined as a Software/Firmware module.

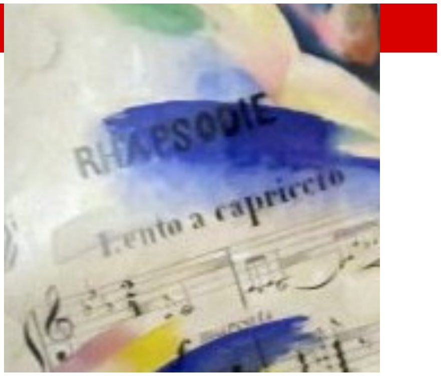
Suggesting one more change to IG 1.9



~~Hybrid cryptographic modules shall be only applicable at FIPS 140-2 Level 1.~~

- Since a software module can be validated up to level 2, there is no obvious reason why a software-hybrid module cannot be validated at level 2.
- Whether or not a hybrid module can be validated at level 2 or higher (in the case of a Firmware-Hybrid), it should be determined by the fact of whether the module meets the requirements at the desired levels.

Play the second half of the clip:
https://vimeo.com/217611269



Thank you for your attention!