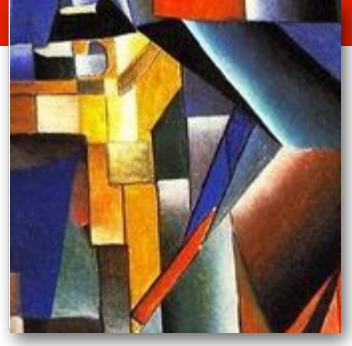
What is My Operational Environment?

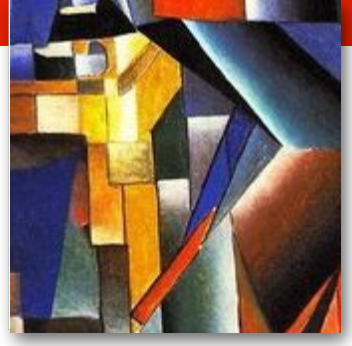
Swapneela Unkule

International Cryptographic Modules Conference
6 November 2015



Agenda

- Operational Environment (OE) for Algorithm Validation (CAVP)
- Operational Environment for Module validation (CMVP)
- OE Differences for Algorithm and Module Validation
- Guidance Required
- Conclusion



OE Specific Fields in CAVS Tool

Software Version: (*)

Part Number: (*)

Firmware Version: (*)

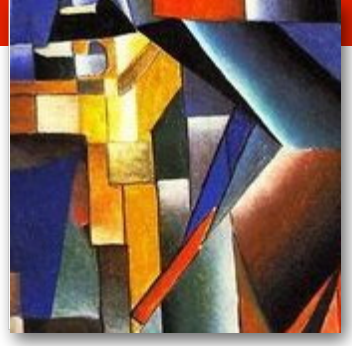
Implementation Type:

Software Firmware Hardware

Operating Environment for Testing Software/Firmware:

Processor

Operating System



OE listing in Algorithm Validation list

For CAVP, the OE consists of operating system and processor, on which the testing was conducted.

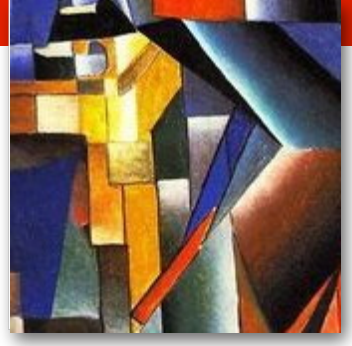
This applies to a single implementation, such as a single binary executable file or dynamic library

Example: Intel Core i5 w/ Windows 7 SP1 (64bit).
(AES Cert#3455)

For multiple implementations using a single source code base that can be compiled to target different OEs, each distinct implementation must be tested separately.

Example: Intel Core i7 w/ Windows 7; Intel Xeon E5-2650 w/ CentOS 7.1.1503
(AES Cert#3527)

OE for CAVP Based on Module Type



1. For Software Module

Processor: This identifies the Processor Family.

More specific information required if the s/w implementation executes differently within the same family.

Operating System: This identifies OS family or major version. More specific information required if the software implementation executes differently within the same OS family or major version number.

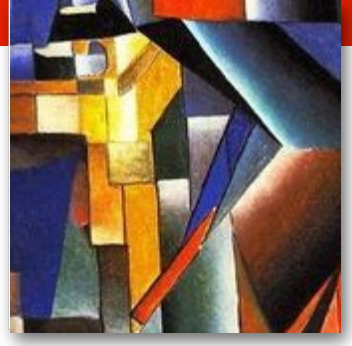
If any Virtual Machine (VM) is used during testing, it shall be listed in the OS field.

(CAVP FAQ GEN.17)

Example: When hypervisor runs directly on the hardware
"Intel Core 2 Duo w/ Windows XP on VMWare ESX 5"

When hypervisor runs on the host OS
"Intel Xeon w/ Windows 7 on Oracle VM VirtualBox on Oracle Solaris 11"

OE for CAVP Based on Module Type



2. For Firmware Module

Same requirement as software module. **Processor + Operating System**

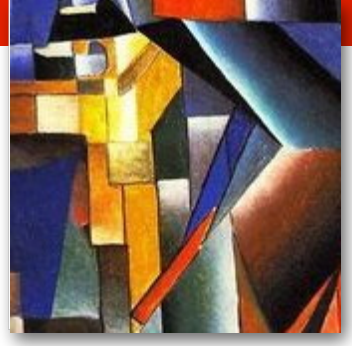
3. For Hardware Module - N/A

The environment is the actual hardware device, and implementation name along with hardware part number indicates the OE.

(CAVP FAQ GEN.17) If the algorithm can not be tested in HW then simulator can be used. Then implementation would be firmware and OE is simulator.

(IG 1.4) For HDL code, the algorithm implementation would be validated in the FPGA as hardware.

Processor Algorithm Acceleration (PAA) part of the OE



Module has two AES implementations

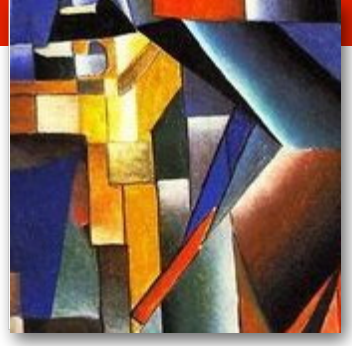
- One entirely in Software
- One in hardware using AES-NI instructions (if the processor supports it)

Algorithms shall be tested in both native execution and PAA execution

Intel Core i7-2600 with AES-NI w/ Microsoft Windows Server 2008 64-bit (AES Cert#2443)

Intel Core i7-2600 w/ Microsoft Windows Server 2008 64-bit (AES Cert#2439)

OE Porting (per IG 1.4)



- Processor bit size

- Algorithm tested on 64-bit platform with 32-bit version of the Module
- New platform changed to 32-bit
- If binary can not run w/o recompilation, implementations must be re-tested

- Processor architecture

- For Level 1 implementation tested on one processor,
- Claim can be made that the implementation also runs on a architecturally compatible processor running the same OS

Example: Apple A8 w/ iOS 8 running on IPhone 6 and IPhone 6Plus (Cert#2407)

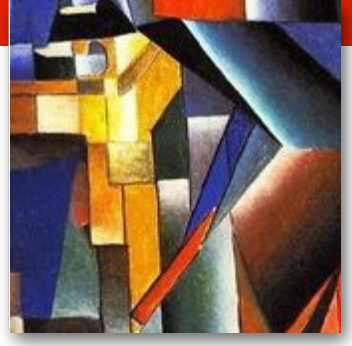
- Operating System

The algorithm implementation must have been tested on every OS claimed.

Example: Windows 2000, Windows 7

May re-use algorithm implementations between like operational environments.

Operational Environment for Module Validation



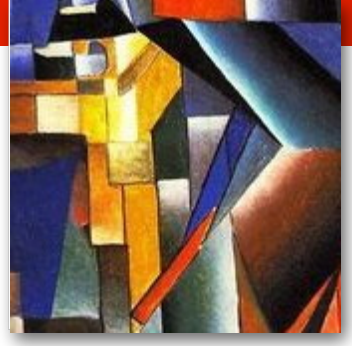
The OE of a cryptographic module refers to the management of the software, firmware, and/or hardware components required for the module to operate.

Types of OE (FIPS PUB 140-2)

- Non-modifiable: Example: firmware contained in ROM, or software contained in a computer with I/O devices disabled
- Limited: static non-modifiable virtual operational environment with no underlying general purpose OS.
  Example: JVM on a non-programmable PC card
- Modifiable: may be reconfigured to add/ delete/modify functionality, and/or may include general purpose operating system capabilities

  Example: computer O/S, configurable smart card O/S, or programmable firmware

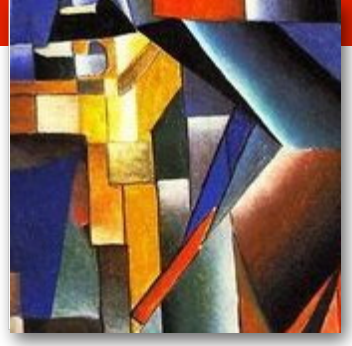
OE Listing for Module Validation



OE on validation certificate including according to (IG G.13)

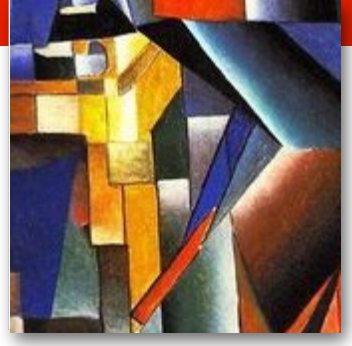
- Software Module
  e.g: Microsoft Windows XP with SP2 running on a Dell Optiplex Model 4567
- Software-Hybrid
  e.g: Debian GNU/Linux 4.0 (Linux kernel 2.6.17.13) running on
  4402-A ViPr DesktopTerminal
- Firmware, e.g. BlackBerry®7230 with BlackBerry OS® Versions 3.8
- F/W with Physical Security > Level 2 should include version info
  e.g: Crypto Unit (Hardware Version: 1.0) with Little OS® Version 3.7b
- For PAA (IG 1.21), Tested as meeting Level 1 with <OS> running on <platform> with PAA; <OS> running on <platform> without PAA

Software Level 2 Requirements for OE



- AS06.10: (Level 2) All cryptographic software and firmware, cryptographic keys and CSPs, and control and status information shall be under the control of an operating system that meets the functional requirements specified in the Protection Profiles listed in Annex B and is evaluated at the CC evaluation assurance level EAL2, or an equivalent evaluated trusted operating system.
- The Annex B only lists 'U.S. Government Approved Protection Profile - U.S. Government Protection Profile for General-Purpose Operating Systems in a Networked Environment' is sunset by NIAP in 2012.
- The NIAP PPs no longer have an assurance level such as EAL2.
- In this situation currently it is not possible to get a Level 2 validation for a software module.
- The CMVP is actively working on a solution for that. We expect that the Annex B will be updated soon.

Vendor Affirmation



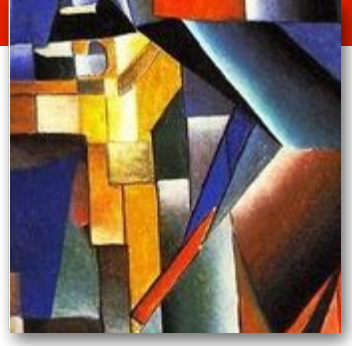
My product runs on many platforms should I test all?

If the module is recompiled/ported on a new platform, no code change

Vendor Affirmation Possible!

- (IG G.5) CMVP allows porting and re-compilation of a validated software, firmware or hybrid CM if porting rules are followed.
- Validation status maintained without retesting
- Vendor affirmed OE included in SP not on Certificate!
- Statement in the SP:

  The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys.



OE Porting Rules IG G.5

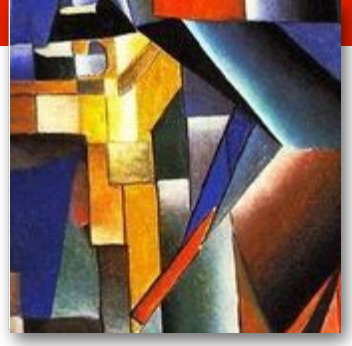
- Software Module (No Code change)

Level 1: remains compliant, when operating on GPC & uses

- specified single user OS /mode specified on the validation certificate Or another compatible single user operating system

Level 2: remains compliant, when operating on GPC provided,

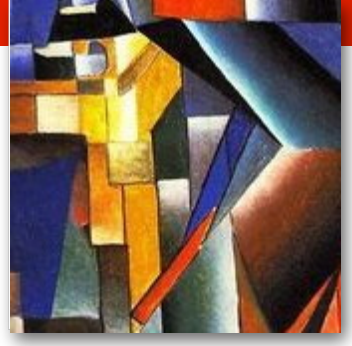
- GPC incorporates the specified CC evaluated EAL2 (or equivalent) OS/mode/ operational settings Protection Profiles listed in Annex B and is evaluated at the CC evaluation assurance level EAL2 Or another compatible CC evaluated EAL2 (or equivalent) OS with like mode and operational settings



OE Porting Rules IG G.5

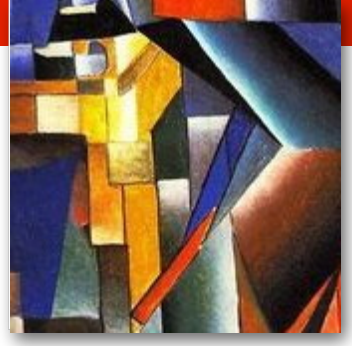
- ❖ Firmware modules
  - No Code change for recompilation
  - Tested operating system unchanged (i.e. same version or revision number)
- ❖ Hybrid modules
  - No software or firmware code change for recompilation
  - Tested operating system unchanged (i.e. same version or revision number)
  - Hardware components utilized by the controlling s/w or h/w are not modified

OE Differences for Algorithm and Module Validation



	Algorithm Validation	Module Validation
OE Components	Processor and OS	Platform(including Processor) and OS
OE selection influences	Algorithm implementation	Algorithm, Key Management functionality, Physical Security
Security Level Requirements	Same for all levels	OE and Physical security requirement for OE changes depending on security level chosen

Guidance Required



- According to IG 1.3, JAVA virtual machine on a non-programmable PC card is an example of a limited OE.

For a general-purpose hypervisor (e.g. VMware) should it be considered as a **non-modifiable or limited OE?**

- According to IG 1.4 you may re-use algorithm implementations between **like** operational environments.

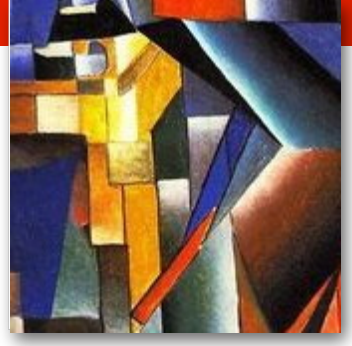
What can be considered as like OE?

Example: Windows 7 SP1 and Windows 7 SP2

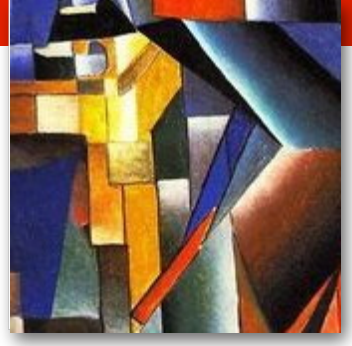
- Software module validation at Level 2

We expect that the Annex B will be updated soon.

Conclusion



- The OE plays an important role for Algorithm and Module validation.
- For certification, the testing needs to be performed on each OE.
- Changes to the OE can trigger revalidation.
- Vendor affirmation is possible for a validated module on a new OE (if there is no code change and porting rules were followed).
- More guidance will be helpful for virtualized OEs and software level 2 validation



Thank You