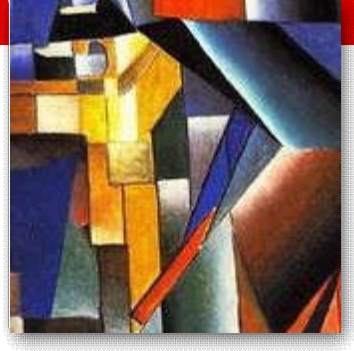
What does your FIPS Certificate say?

Swapneela Unkule
atsec information security corp.
Email: swapneela@atsec.com

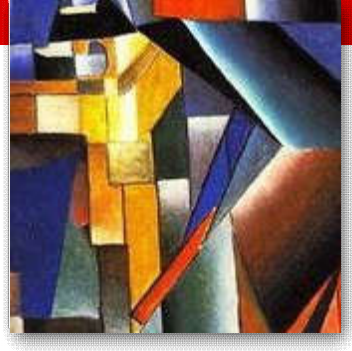
ICMC 2017, May 16-19, Westin Arlington Gateway, Washington, DC.

Topics Covered



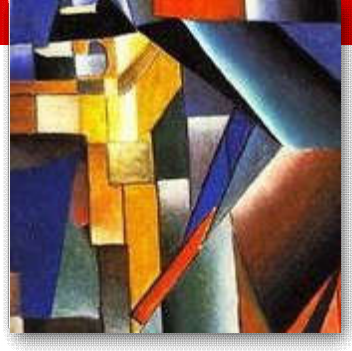
- Basic information of FIPS Certificate
- Certificate Differentiators
- A Complete Reading of FIPS Certificate

Basic information of FIPS Certificate



- Mandatory Fields on the Certificate
- Example Certificate

Mandatory Fields on the Certificate



1. Vendor Information — **Module Vendor**
2. Module Name, Version Number, Module Type
3. Validation and Sunset Date
4. Module security level

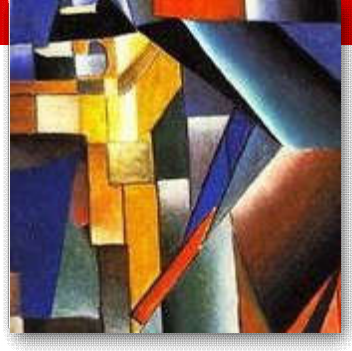
(2–4) — **About Module**

5. FIPS approved algorithms
6. Other Algorithms
7. Security Policy

(5–7) — **Module Details**

8. Tested Configuration — **Module Environment**

Example Certificate



Module Vendor

Validation & Sunset Date

Module Type

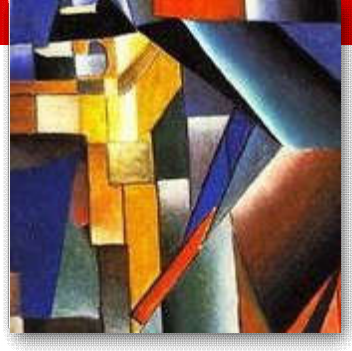
Vendor / CST Lab	Cryptographic Module	Module Type	Validation Date	Sunset Date	Level / Description
Hewlett Packard®, Enterprise 153 Taylor Street Littleton, MA 01460 USA Nagesh Kuriyavar TEL: 402-885-2812 FAX: 402-758-7332 Paul Rozeboom TEL: 402-885-2698 FAX: 402-758-7332 **CST Lab:** NVLAP 200658-0	**HP OpenCall HLR Cryptographic Module** (Software Version: I-HSS 01.08.01) Validated to FIPS 140-2 Consolidated Validation Certificate Security Policy Vendor Product Link	Software	12/22/2015	12/21/2020	*Overall Level:* 1 -Physical Security: N/A -Mitigation of Other Attacks: N/A -Tested Configuration(s): HP NonStop v J06.18 running on Integrity NonStop BladeSystem NB54000c (single-user mode) -*FIPS Approved algorithms:* AES (Cert. #3503); DRBG (Cert. #872); HMAC (Cert. #2237); SHS (Cert. #2890) -*Other algorithms:* N/A Multi-Chip Stand Alone "The HP OpenCall HLR Cryptographic Module provides cryptographic services that allows the HP OpenCall HLR to protect sensitive application and subscriber data at rest and during transit"

Module Name

Version Number

Security Level

Example Certificate



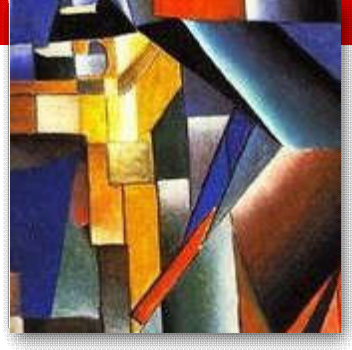
Vendor / CST Lab	Cryptographic Module	Module Type	Validation Date	Sunset Date	Level / Description
Hewlett Packard®, Enterprise 153 Taylor Street Littleton, MA 01460 USA Nagesh Kuriyavar TEL: 402-885-2812 FAX: 402-758-7332 Paul Rozeboom TEL: 402-885-2698 FAX: 402-758-7332 **CST Lab:** NVLAP 200658-0	**HP OpenCall HLR Cryptographic Module** (Software Version: I-HSS 01.08.01) Validated to FIPS 140-2 Consolidated Validation Certificate Security Policy ← SP Vendor Product Link	Software	12/22/2015	12/21/2020	***Overall Level:* 1** -Physical Security: N/A -Mitigation of Other Attacks: N/A -Tested Configuration(s): HP NonStop v J06.18 running on Integrity NonStop BladeSystem NB54000c (single-user mode) -*FIPS Approved algorithms:* AES (Cert. #3503); DRBG (Cert. #872); HMAC (Cert. #2237); SHS (Cert. #2890) -*Other algorithms:* N/A Multi-Chip Stand Alone "The HP OpenCall HLR Cryptographic Module provides cryptographic services that allows the HP OpenCall HLR to protect sensitive application and subscriber data at rest and during transit"

Module Environment →

Approved Algorithm →

Other Algorithm →

Example Certificate contd.



Certificate applicable to only this version

HP OpenCall HLR Cryptographic Module (Software Version: I-HSS 01.08.01) Validated to FIPS 140-2 Consolidated Validation Certificate Security Policy Vendor Product Link	Software	12/22/2015	12/21/2020	***Overall Level:*** **1** -Physical Security: N/A -Mitigation of Other Attacks: N/A -Tested Configuration(s): HP NonStop v J06.18 running on Integrity NonStop BladeSystem NB54000c (single-user mode) *-FIPS Approved algorithms:* AES (Cert. #3503); DRBG (Cert. #872); HMAC (Cert. #2237); SHS (Cert. #2890) *-Other algorithms:* N/A Multi-Chip Stand Alone

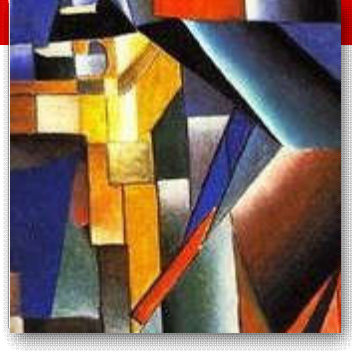
Applicable only to this specific platform& OS.

AES Certificate entry

3503	Hewlett Packard®, Enterprise 10810 Farnam Drive NBN02 Omaha, NE 68154	**OpenCall HLR Cryptographic Module** Version I-HSS 1.08.01	Intel Itanium 9300 w/ Non Stop OS J06.18

Exact same SW version and test platform used by CAVS

Certificate Differentiators



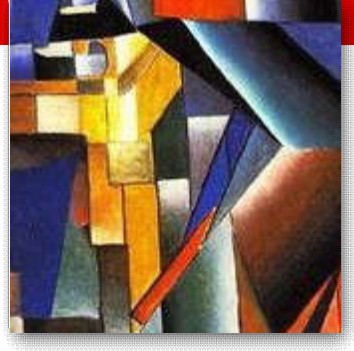
➢Caveats

1. Module operation caveat
2. Entropy caveat
3. Bound Module caveat

➢Extras beyond an overall FIPS level

1. Higher section level claimed
2. Tested with and without PAA
3. Mitigation of other attacks claimed

1. Module operation caveat



Caveat 1

(When operated in FIPS mode and with the tamper evident seals installed as indicated in the Security Policy.)

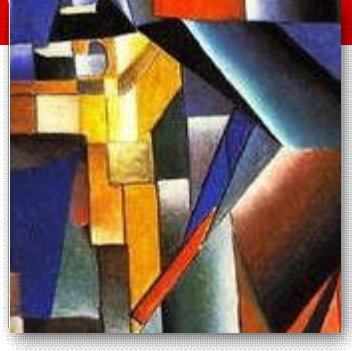
Caveat 2

Validated to FIPS 140-2

Consolidated Validation Certificate

Security Policy

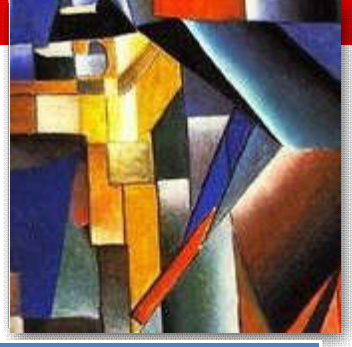
Certificate Differentiator



Module operation caveat	
(When operated in FIPS mode)	*-FIPS Approved algorithms:* AES (Cert. #3211); SHS (Cert. #2658); HMAC (Cert. #2024)
Validated to FIPS 140-2 Consolidated Validation Certificate	*-Other algorithms:* DES; CRC32

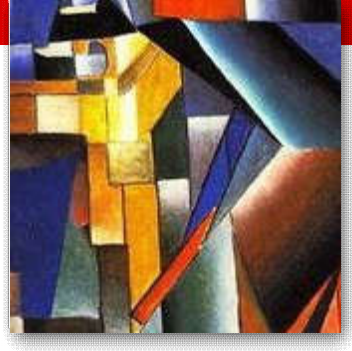
No module operation caveat	
(Software Version: I-HSS 01.08.01)	*-FIPS Approved algorithms:* AES (Cert. #3503); DRBG (Cert. #872); HMAC (Cert. #2237); SHS (Cert. #2890)
Validated to FIPS 140-2 Consolidated Validation Certificate	*-Other algorithms:* N/A

Certificate Differentiator contd.



Less Crypto Coverage	All Crypto Coverage
-*FIPS Approved algorithms:* AES (1) (Cert. #1436); SHS (Cert. #1301) -*Other algorithms:* AES (2) (non-compliant); RC4; MD5; SHS (non-compliant); RIPEMD; DES; Triple-DES (non-compliant); RC2-CBC, RC2-ECB, RC2-CFB64, RC2-OFB64; Blowfish; CAST; RSA (non-compliant); DSA (non-compliant); Diffie-Hellman; RNG (non-compliant)	-*FIPS Approved algorithms:* AES (Cert. #1493); DRBG (Cert. #61); ECDSA (Cert. #559); HMAC (Cert. #878); KAS (Cert. #16); RSA (Certs. #732 and #785); SHS (Cert. #1346); Triple-DES (Cert. #1122) -*Other algorithms:* NDRNG

2. Entropy caveat



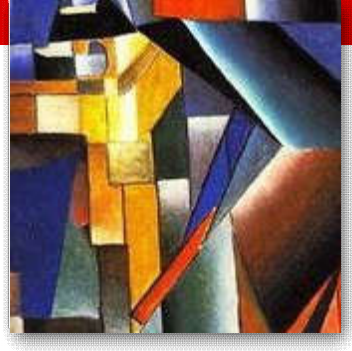
(When operated in FIPS mode. The module generates cryptographic keys whose strengths are modified by available entropy)

Validated to FIPS 140-2
Consolidated Validation Certificate

Security Policy

Vendor Product Link

Certificate Differentiator



Security strength met in some cases

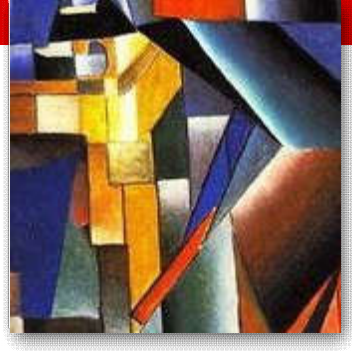
(Software Version: 1.0)
(When operated in FIPS mode. The module generates cryptographic keys whose strengths are modified by available entropy)

Security strength met always

(Software Version: 1.0)
(When operated in FIPS mode)

Validated to FIPS 140-2

Certificate Differentiator contd.



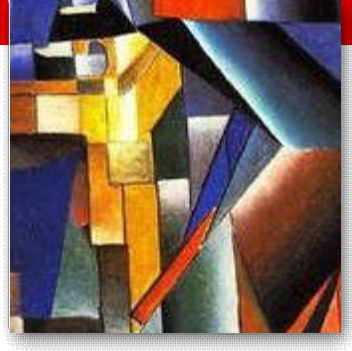
Assurance in some cases

(Software Version: 1.0)
(When operated in FIPS mode. The module generates cryptographic keys whose strengths are modified by available entropy)

No assurance in all cases

(Software Version: 1.0)
(When operated in FIPS mode. No assurance of the minimum strength of generated keys.)

3. Bound Module caveat



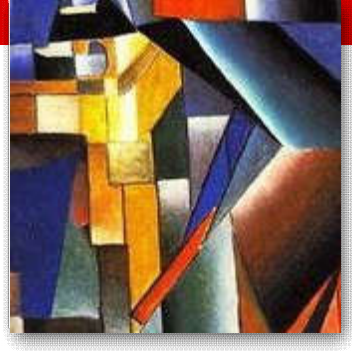
(When operated in FIPS mode with module IBM(R) z/OS(R) Version 2 Release 1 Security Server RACF(R) Signature Verification Module version 1.0 validated to FIPS 140-2 under Cert. #2691 operating in FIPS mode)

Validated to FIPS 140-2

Consolidated Validation Certificate

Security Policy

Certificate Differentiator



Module dependent on other module

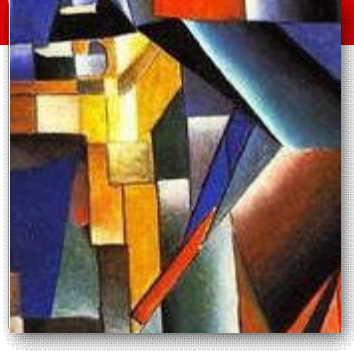
(When operated in FIPS mode with module IBM(R) z/OS(R) Version 2 Release 1 Security Server RACF(R) Signature Verification Module version 1.0 validated to FIPS 140-2 under Cert. #2691 operating in FIPS mode)

No module dependency

(When operated in FIPS mode)

Validated to FIPS 140-2

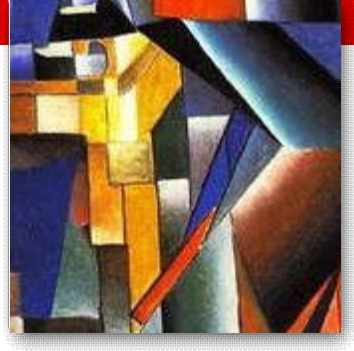
4. Higher section level claimed



Overall Level: 2

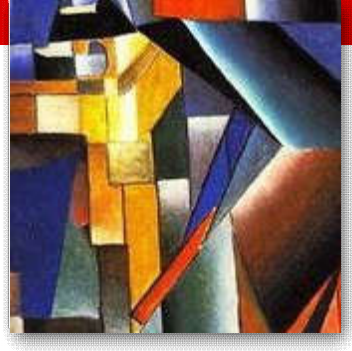
-Roles, Services, and Authentication: Level 3
-Physical Security: Level 3
-EMI/EMC: Level 3

Certificate Differentiator



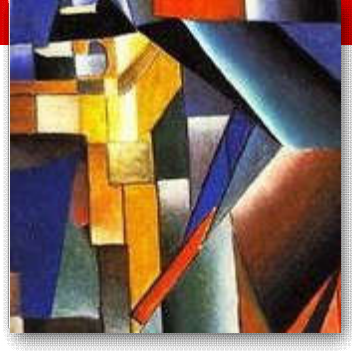
Level 1 met	Level 1 met and Authentication Present
Overall Level: **1** -Mitigation of Other Attacks: N/A -Tested Configuration(s): N/A	***Overall Level:*** **1** -Roles, Services, and Authentication: Level 2 -Mitigation of Other Attacks: N/A -Tested Configuration(s): N/A

Certificate Differentiator contd.



Level 1 met and Authentication Present	Level 1 met and Authentication & Identification Present
Overall Level: **1** -Roles, Services, and Authentication: Level 2 -Mitigation of Other Attacks: N/A -Tested Configuration(s): N/A	***Overall Level:*** **1** -Roles, Services, and Authentication: Level 3 -Design Assurance: Level 3

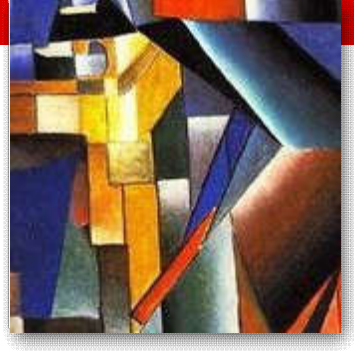
5. Tested with and without PAA



***Overall Level:* 1**

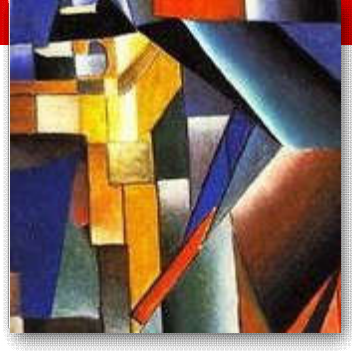
-Physical Security: N/A
-Mitigation of Other Attacks: N/A
-Tested Configuration(s): Tested as meeting Level 1 with Red Hat Enterprise Linux 7.1 running on HP ProLiant DL380p Gen8 with PAA
Red Hat Enterprise Linux 7.1 running on HP ProLiant DL380p Gen8 without PAA

Certificate Differentiator



Tested Configuration	Tested Configuration with and without PAA
Red Hat Enterprise Linux 7.1 running on IBM Power8 Little Endian 8286-41A	Red Hat Linux Enterprise Server 7.0 BE 64-bit running on an IBM 8286-42A POWER8 with PAA Red Hat Linux Enterprise Server 7.0 BE 64-bit running on an IBM 8286-42A POWER8 without PAA

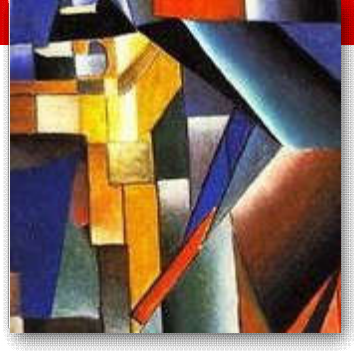
6. Mitigation of other attacks claimed



***Overall Level:* 1**

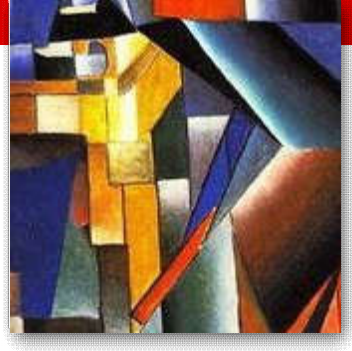
-Tested Configuration(s): Tested as meeting Level 1 with z/OS version 2 release 2 running on IBM z13 model N63
Red Hat Enterprise Linux Server release 7.2 running on IBM z13 model N63 (single-user mode)

Certificate Differentiator



Level 3 met	Level 3 met and Mitigation claimed
Overall Level: 3 -Mitigation of Other Attacks: N/A -Tested Configuration(s): N/A	***Overall Level: 3*** **Missing** -Tested Configuration(s): N/A

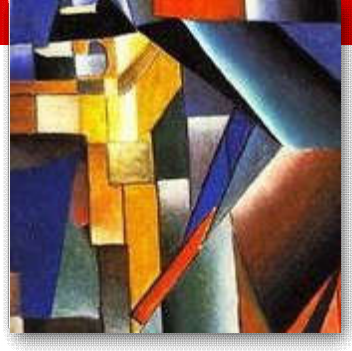
A Complete Reading of FIPS Certificate



- Vendor Approach--what kind of certificate we want to get?

- User Approach--what kind of certificate we want to use?

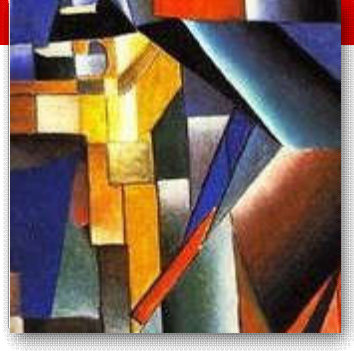
A Complete Reading of FIPS Certificate contd.



Certificate Field	Vendor	User
Module Name, Version Number, Module Type	Focus CRYPTO in product. Multiple validation to cover entire product.	Check for module coverage and versions when using the product.
Validation and Sunset Date	Consider revalidation/ rebranding before sunset.	Check for the remaining lifetime of the module.
FIPS approved algorithms and Other Algorithms	Consider testing all the approved algorithms to get broader crypto coverage.	Look for the crypto algorithm you want to use.
Security Policy	Provide insight to the module with possible use case of the module wrt to entire product.	Refer for module details, user guidance and intended use.

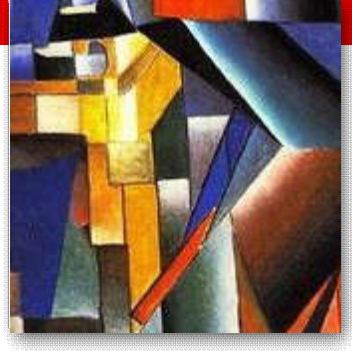
A Complete Reading of FIPS Certificate

contd.

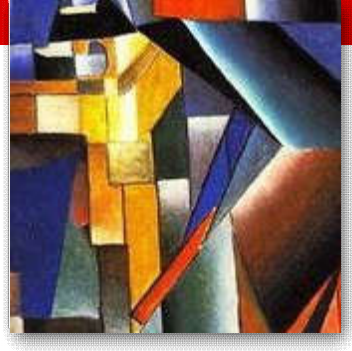


Certificate Field	Vendor	User
Tested Configuration	Choose representative platforms.	Match to your requirement or request to Vendor (1sub)
Module operation caveat	Specify the intended operating condition	Pay attention to this while using the module.
Entropy caveat	Avoid - pay attention to Entropy details.	Read the caveat carefully.
Bound Module caveat	Avoid - dependency among the modules.	Check for dependency of the module.
Higher section level, Mitigation of other attacks, PAA	Claim areas of the module exceeding the requirement.	Look for these fields when want to get extra beyond an overall FIPS level.

Concluding Remarks



- Plan your validation visualizing the certificate entry.
- Give some thought on Entropy to avoid caveat.
- Choose the Test configuration wisely.
- Plan your module with certificate differentiators in mind.
- Vendors, plan the certificate carefully!
- Users, read the certificate carefully!



Thank You !

Questions ?