#SHAREorg

SHARE
Technology · Connections · Results

Understanding FIPS (Federal Information Processing Standard) 140-2 and z/OS System SSL (Secure Socket Layer)

Alyson Comer
IBM Corporation
z/OS System SSL Development
Endicott, NY
Email: comera@us.ibm.com

February 8th, 2013
Session 12536

SHARE in San Francisco 2013

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

IBM®
MVS
RACF®
z/OS®
zEnterprise

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

•All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Session Abstract

This session will give an overview of FIPS (Federal Information Processing Standard) 140-2 and z/OS System SSL (Secure Socket Layer). The session will start with an overview of what is FIPS 140-2, what was entailed in getting z/OS System SSL certified at FIPS 140-2 level 1 and how to utilize z/OS System SSL in a FIPS 140-2 manner.

Agenda

- **Overview of FIPS 140-2**
  - What is FIPS 140-2
  - FIPS 140-2 Requirements
  - FIPS 140-2 Security Levels
  - FIPS 140-2 Validation Types
  - Security Policy
  - Validation Process Flow
- **Using z/OS System SSL in FIPS mode**
  - Requirements/Configuration
  - Application changes
  - Enabling AT-TLS for FIPS

What is FIPS 140

- **FIPS (Federal Information Processing Standard)** defines standards and guidelines utilized by the US government and other regulated industries (ie. Financial and health-care)

- **FIPS 140** defines the security requirements for products that contain cryptographic functionality.

  - **FIPS 140-1 issued in January 1994**
  - **FIPS 140-2 issued in May 2001**
  - **FIPS 140-3 under development – draft December 2009**

What is FIPS 140-2

- Validations require conforming implementations to be formally validated through the **Cryptographic Module Validation Program (CMVP).**

- **NIST** (National Institute of Standards and Technology) and Communications Security Establishment of the Government of Canada (**CSEC**) jointly operate the **Cryptographic Module Validation Program (CMVP)**

- Each product works with accredited **Cryptographic and Security Testing (CST) laboratory**. Product provides required documentation/test platforms and CST Lab evaluates product and builds submission package to be submitted to NIST. Interaction with NIST is done by CST Lab.
  - 20+ accredited labs
  - Worldwide
  - http://csrc.nist.gov/groups/STM/testing_labs/index.html

FIPS 140-2 Terms

- ***Cryptographic boundary***: 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 module***: the set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

- ***Approved security function****: a* security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either
  - a) specified in an Approved standard,
  - b) adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard, or
  - c) specified in the list of Approved security functions.

- ***Approved mode of operation***: a mode of the cryptographic module that employs only Approved security functions (ie. Triple DES, AES).

- ***Critical security parameter (CSP)***: security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module.

FIPS 140-2 Requirements

- *FIPS 140-2 Security Requirements for Cryptographic Module publication*

  http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

  *defines **11** requirements a cryptographic module must meet.*

  - *Annex A:* Approved Security Functions for FIPS PUB 140-2
    - Symmetric, asymmetric and message digests
  - Annex B: Approved Protection Profiles for FIPS PUB 140-2
    - Common Criteria
  - Annex C: Approved Random Number Generation for FIPS 140-2
  - Annex D: Approved Key establishment Techniques for FIPS 140-2
    - RSA, ECDSA etc

FIPS 140-2 Security Levels

Within the FIPS 140-2 standard 4 security levels are defined.

```
Lowest    Security Level 1
          Security Level 2
          Security Level 3
Highest   Security Level 4
```

FIPS 140-2 Requirements

1	***Cryptographic module specification***	•Specifications of cryptographic module including information about what is included in the cryptographic module boundary (hardware, software, firmware). •Approved cryptographic algorithms and modes. •Statement of module security policy. •Detailed information about the software/hardware/firmware levels
2	***Cryptographic module ports and interfaces***	Data and control information that flows in and out of the module and how it must be presented
3	***Roles, services and authentication***	•Role Type–user, officer, maintenance (users of the cryptographic module) and how it is enforced •Services, operations, or functions that can be performed •Show Status, Perform Self-Tests, Perform Approved Security Function - at least one is required
4	***Finite state model***	•high-level module states and how control transitions from one state to another

FIPS 140-2 Requirements cont'd

5	***Physical security***	Production grade components; tamper detection/response; tamper resistance
6	***Operational environment***	•Management of the software, firmware, and/or hardware components required for the module to operate •Operating system manages system software and firmware as well as processes and threads. •How module is utilized – APIs, proper installation and configuration of components
7	***Cryptographic key management***	•Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization. •Plaintext or encrypted keys
8	**EMI/EMC**	•Federal Communications Commission requirement against hardware components of the cryptographic boundary

FIPS 140-2 Requirements cont'd

9	***Self-test***	Tests to ensure module is functioning properly • Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. • On-demand tests • Conditional tests: pair-wise consistency test, continuous random number generation test
10	***Design assurance***	Documentation which supports that the module has been well designed and implemented
11	***Mitigation of other attacks***	Specification of mitigation of attacks for which no testable requirements are currently available.

How do the Requirements map to FIPS 140-2 security levels (example)

	Level 1	Level 2	Level 3	Level 4
Specifications	Specifications of cryptographic module and module boundary. Approved cryptographic algorithms and modes. Statement of module security policy. Description of all hardware, software, and firmware.			
Ports & Interfaces	Specifications for all interfaces and input/output ports.		Logical or physical separation of ports used for unprotected security parameters.	
Authentication and access control	Logical separation of required and optional roles.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Key Management	Keys established using manual methods may be entered or output in cleartext form.		Keys established using manual methods must be entered and output either encrypted or using split knowledge procedures.	
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response.	Tamper detection and response envelope.

Algorithm Validation Requirement

- **Cryptographic Algorithm Validation Program** is the validation testing for FIPS approved and NIST recommended cryptographic algorithms and components of algorithms.
- Prerequisite to the Cryptographic Module Validation Program (CMVP)
- Algorithms
  - Symmetric Algorithms – Triple DES, AES etc
  - Asymmetric Algorithms – RSA, DSA, ECDSA etc
  - SHS
  - HMAC
  - RNG
  - etc
- CAVP tool provided to accredited labs. Labs generate test vectors, Vendors execute algorithms using test vectors and labs validate results
- http://csrc.nist.gov/groups/STM/cavp/index.html
- Website contains information about the algorithms and sample test vectors
- Validation List - http://csrc.nist.gov/groups/STM/cavp/validation.html

Types of Validations

- **Software**
  - Provides products the ability to certify software algorithm implementations
- **Hybrid**
  - Provides products the ability to certify a mixture of software and hardware algorithm implementation.
- **Hardware**
  - Provides products the ability to certify pure hardware algorithm implementations (ie. Cryptographic cards)

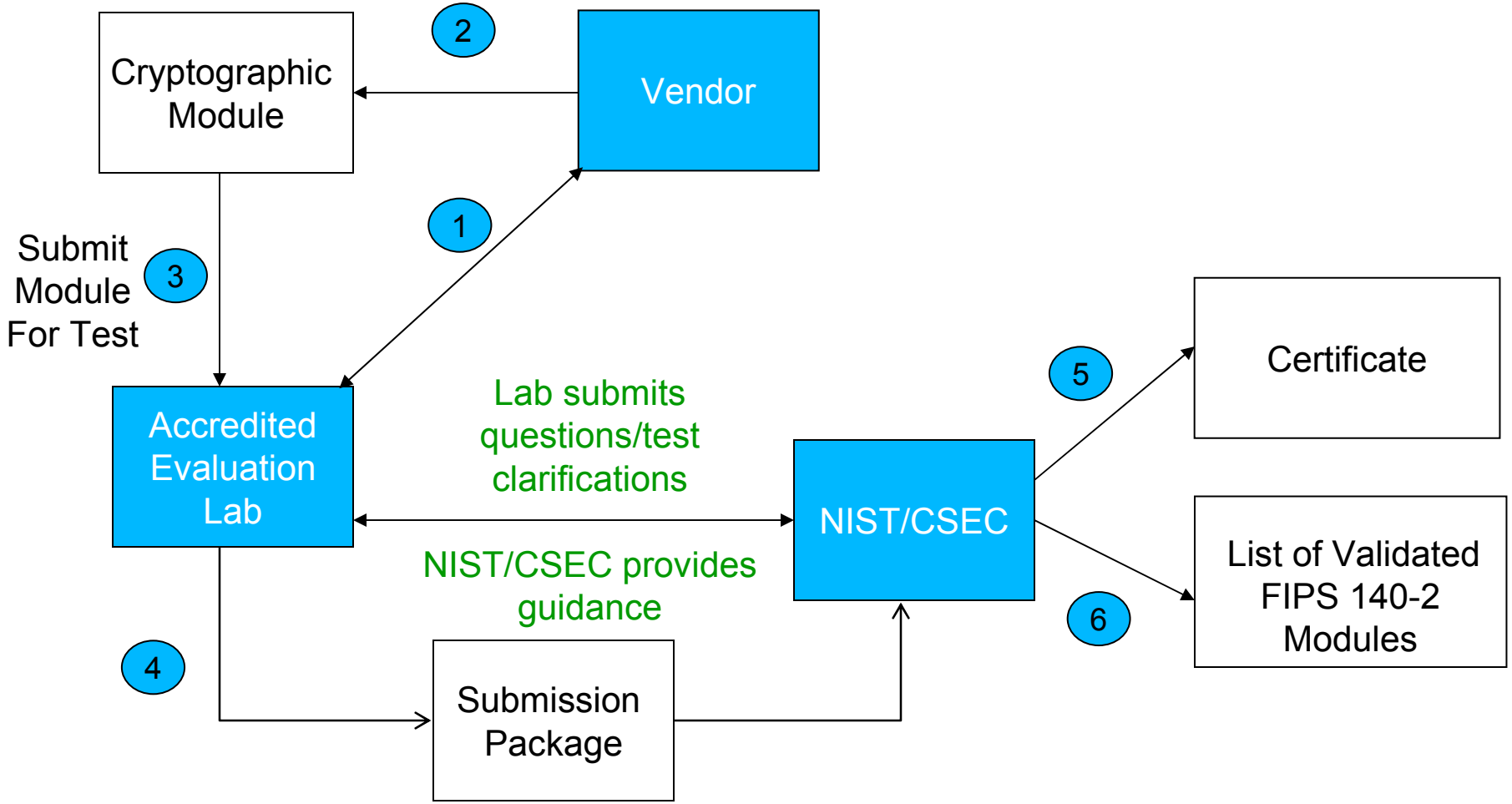
What is the Cryptographic Security Policy?

- The Cryptographic Security Policy is a formal document that describes how the product meets the 11 security requirements of the FIPS 140-2 standard and how to operate the cryptographic module in FIPS 140-2 manner.

- Submitted to NIST with evaluation package and posted to NIST website once validation has been completed.

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

FIPS 140-2 Validation Process



What is System SSL

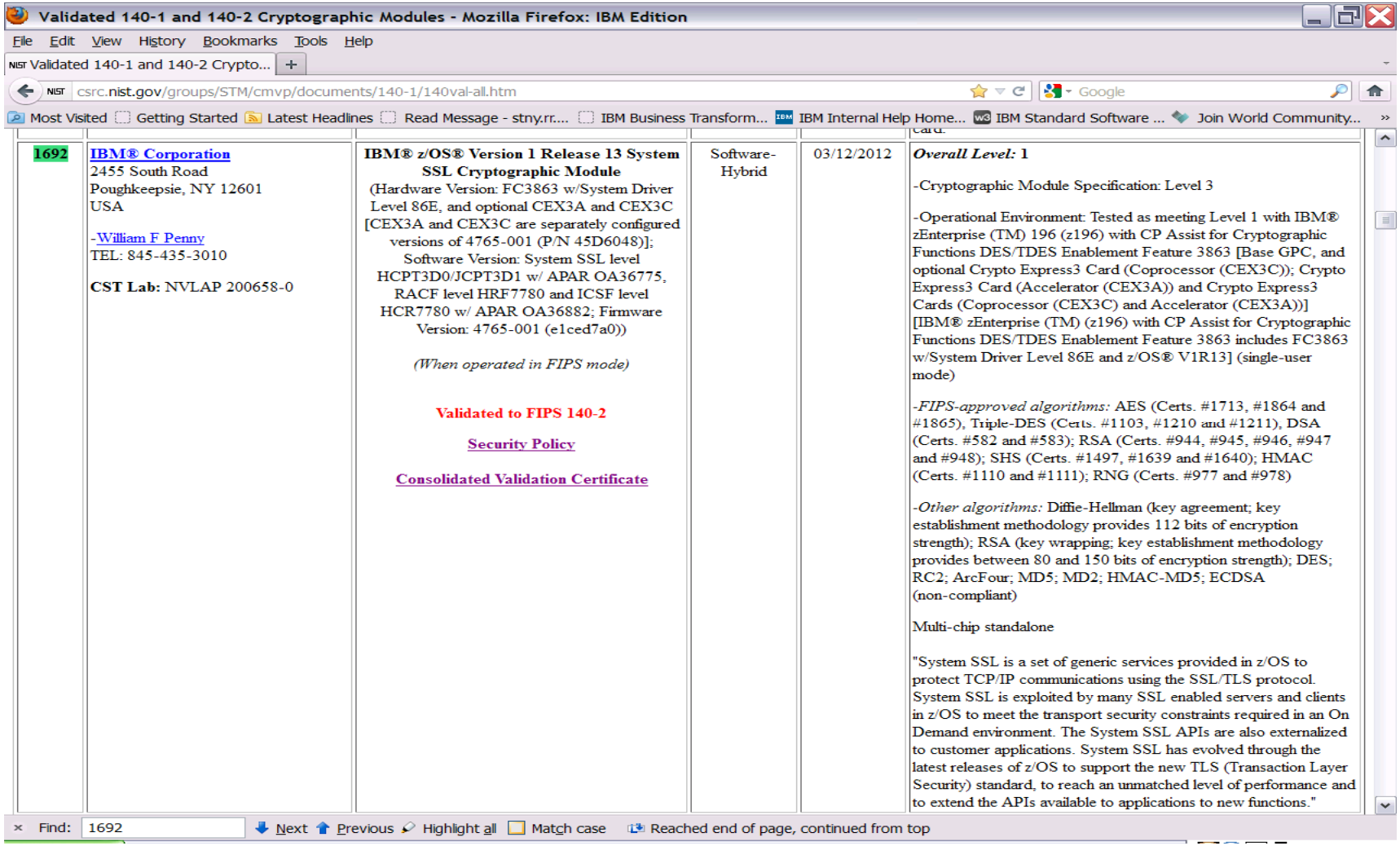
- An element of the z/OS base Cryptographic Services element that provides:
  - A certificate management utility, gskkyman, for managing certificates within a key database file as well as a suite of APIs to allow application writers the ability to write their own certificate management programs.
  - Applications a mechanism (suite of C/C++ POSIX callable application programming interfaces (APIS)) for applications to securely communicate over an open communications network using SSL/TLS protocol
  - Although not part of the SSL protocol support, System SSL also contains a suite of APIs that allows for applications to build/read PKCS#7 messages.

System SSL Evaluated Releases

- z/OS V1R10 FIPS 140-2 – Certificate #1389 (8/12/2010)
- z/OS V1R11 FIPS 140-2 – Certificate #1492 (2/4/2011)
- z/OS V1R12 FIPS 140-2 – Certificate #1600 (9/8/2011)
- z/OS V1R13 FIPS 140-2 – Certificate #1692 (3/12/2012)

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

z/OS V1R13 System SSL Evaluation



z/OS V1R13 System SSL Evaluation

FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0015

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: _____

Dated: 13 April 2012

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 3 April 2012

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

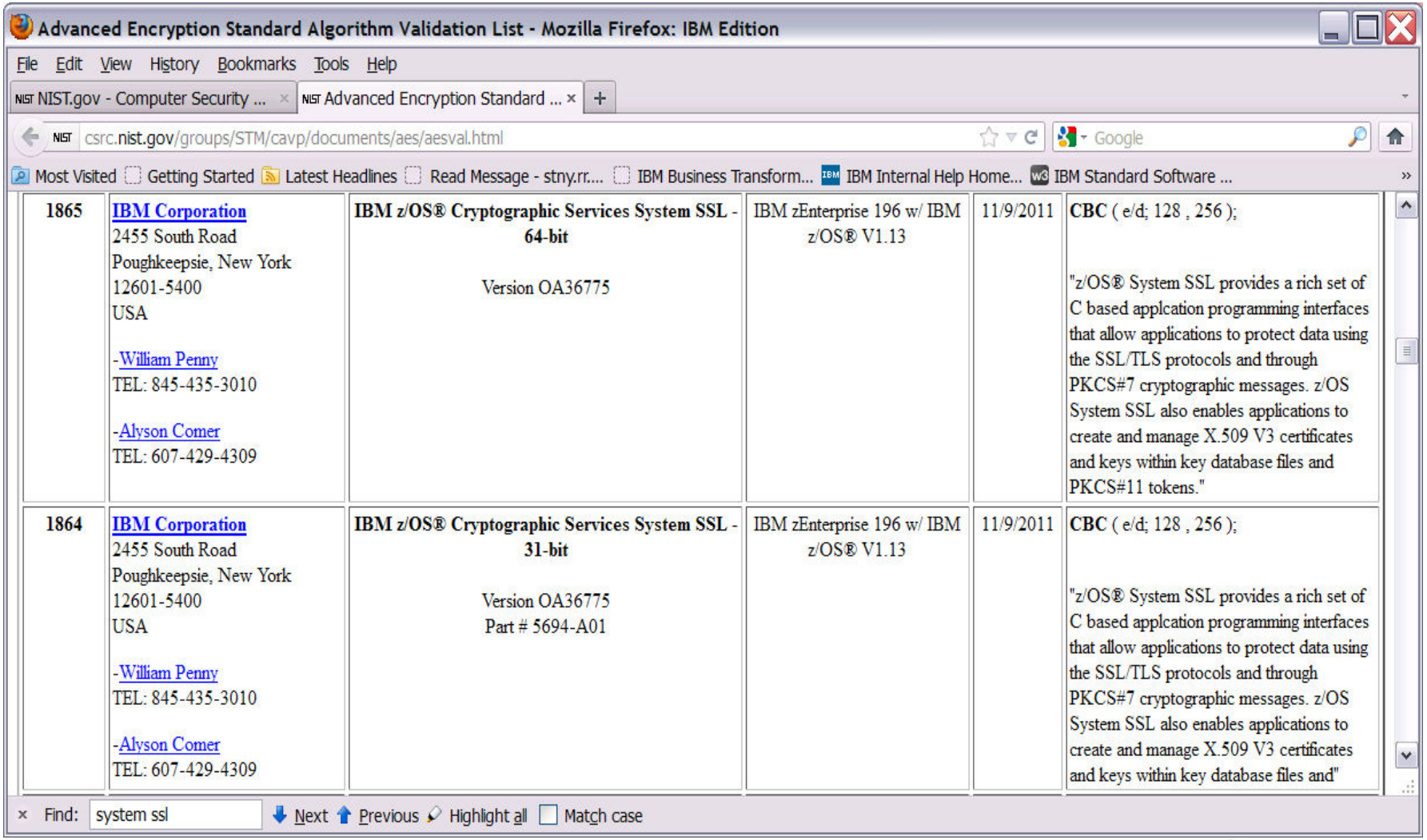
TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Page 1 of 3

4/3/2012

× Find: 1692 Next Previous Highlight all Match case Reached end of page, continued from top

z/OS V1R13 System SSL AES Validation



1865	**IBM Corporation** 2455 South Road Poughkeepsie, New York 12601-5400 USA -William Penny TEL: 845-435-3010 -Alyson Comer TEL: 607-429-4309	**IBM z/OS® Cryptographic Services System SSL - 64-bit** Version OA36775	IBM zEnterprise 196 w/ IBM z/OS® V1.13	11/9/2011	**CBC** (e/d; 128 , 256); "z/OS® System SSL provides a rich set of C based applcation programming interfaces that allow applications to protect data using the SSL/TLS protocols and through PKCS#7 cryptographic messages. z/OS System SSL also enables applications to create and manage X.509 V3 certificates and keys within key database files and PKCS#11 tokens."
1864	**IBM Corporation** 2455 South Road Poughkeepsie, New York 12601-5400 USA -William Penny TEL: 845-435-3010 -Alyson Comer TEL: 607-429-4309	**IBM z/OS® Cryptographic Services System SSL - 31-bit** Version OA36775 Part # 5694-A01	IBM zEnterprise 196 w/ IBM z/OS® V1.13	11/9/2011	**CBC** (e/d; 128 , 256); "z/OS® System SSL provides a rich set of C based applcation programming interfaces that allow applications to protect data using the SSL/TLS protocols and through PKCS#7 cryptographic messages. z/OS System SSL also enables applications to create and manage X.509 V3 certificates and keys within key database files and"

Using System SSL z/OS V1R13 in FIPS mode

- System SSL was certified at Level 1
- System SSL was certified as **Hybrid**. Hybrid allows System SSL to utilize the symmetric/hashing algorithms available through the CPACF crypto instructions within the processor, RSA encryption within the CryptoExpress 3 cards and its own software algorithms
- Cryptographic Boundary
  - Platforms
    - CSTL Lab evaluated
      - *IBM zEnterprise™ 196 (z196) with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 (Base GPC)*
        - *Crypto Express3 card (coprocessor, accelerator)*
    - Vendor Affirmed
      - IBM System z10® Enterprise Class (z10 EC) with CP Assist for Cryptographic Functions DES/TDES Enablement Feature 3863 (Base GPC)
        - *Crypto Express3 card (coprocessor, accelerator)*
  - Operating System
    - z/OS Version 1 Release 13

Using System SSL z/OS V1R13 in FIPS mode

- Cryptographic Module
  - gskkyman, System SSL DLLs, System SSL Started task
  - CP Assist for Cryptographic Functions (CPACF)
  - ICSF – “pipe“ to cryptographic card
  - Crypto Express3 card
  - RACF Program Signature Verification Module (IRRPVERS)

Algorithms and Key Sizes

	Non-FIPS		FIPS	
Algorithm	**Key Size**	**Hardware**	**Key Size**	**Hardware***
RC2	40 and 128			
RC4	40 and 128			
DES	56	X		
Triple DES	168	X	168	X
AES-CBC	128 and 256	X	128 and 256	X
AES-GCM	128 and 256	X	128 and 256	X
RSA	512-4096	X	1024-4096	X
DSA	512-1024		1024	
DH	512-2048		2048	
ECDSA – non-compliant	160-521	X	192-521	X
MD2, MD5				
SHA-1		X		X
SHA-2 (224/256/384/512)		X		X

* FIPS mode supports only Clear Keys

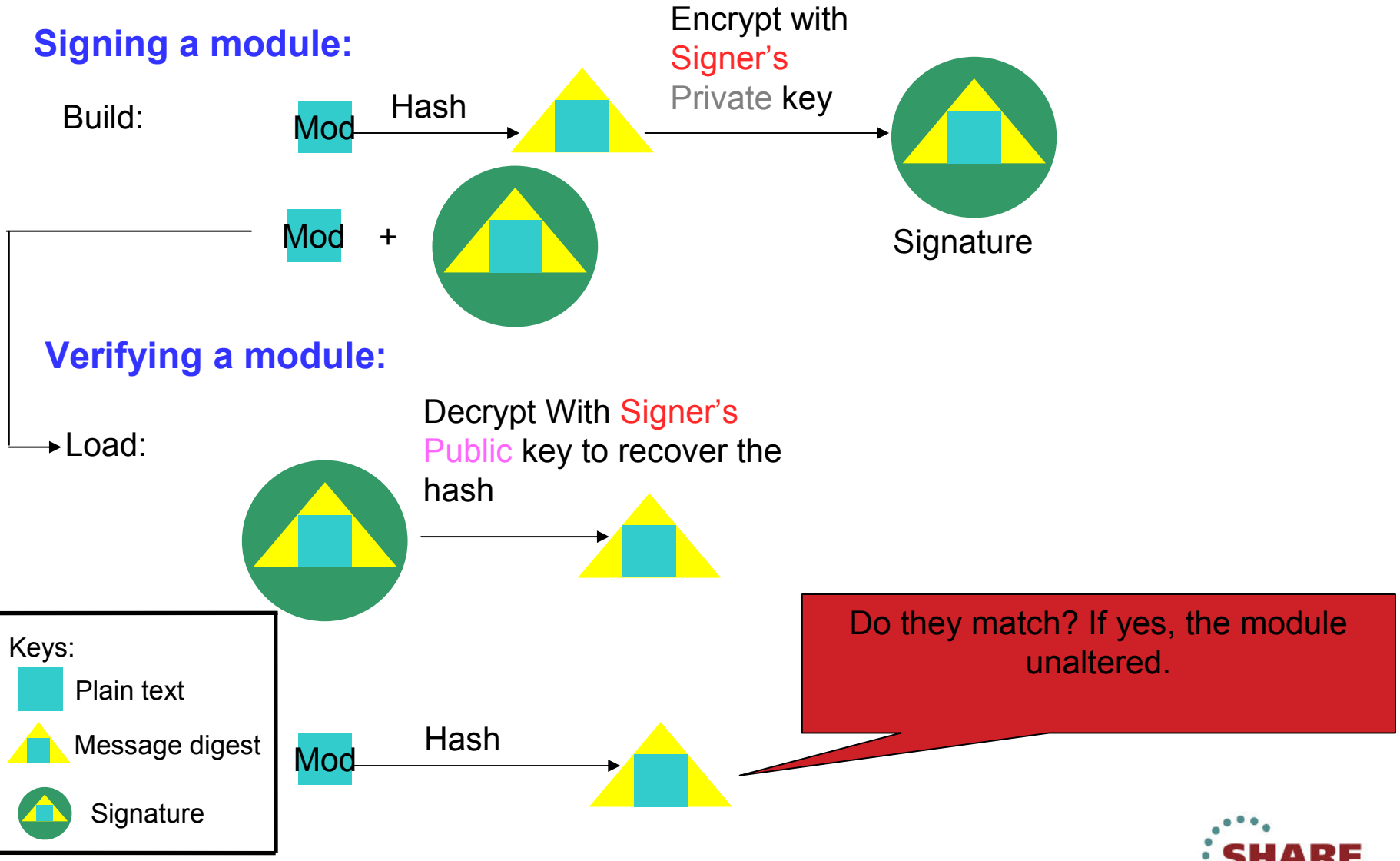
SSL/TLS Protocols

- TLS V1.0, TLS V1.1 and TLS V1.2 (V1R13 only) protocols are supported in FIPS mode.
- SSL V2 and SSL V3 are not supported and are ignored if specified.
- Ciphers limited to algorithms supported in FIPS mode.
  - Triple DES
  - AES

System SSL Module Integrity Test

- FIPS validation requires cryptographic module to perform an integrity test to ensure software modules within the cryptographic boundary have not been modified since they were built.
- System SSL uses RACF's program (code) signing support which entails the use of digital signatures.
- Signature verification provides a method to ensure the System SSL modules remain unchanged from the time they were built, installed onto the system, and loaded into storage to be used by a FIPS enabled System SSL application.

Program (Code) Signing for integrity



System SSL Cryptographic Module Configuration - Module Verification

Modules that form the System SSL FIPS 140-2 cryptographic module are digitally signed using an IBM key during the build process

GSKCMS31	GSKSSL	GSKKYMAN	IRRPVERS
GSKCMS64	GSKSSL64	GSKSRVR	
GSKC31F	GSKS31F	GSKSRBWT	
GSKC64F	GSKS64F	GSKSRBRD	

- Encryption key used to sign the System SSL modules is an RSA private key that belongs to an x.509 certificate signed by the STG Code Signing CA certificate. The STG Code Signing CA certificate is shipped as a default CERTAUTH certificate in the RACF database under the label 'STG Code Signing CA'.

- RACF profiles must be defined to enable the validation of the module signature (added during the IBM module build process) when loaded by the system.

System SSL Module Verification

- Detailed steps to enable module signature validation are documented in the publication “Cryptographic Services System Secure Sockets Layer Programming”, in the chapter “System SSL and FIPS 140-2”.

- Configuration Step highlights:

1. A signature verification SAF key ring needs to exist containing the root CA used to sign the System SSL signing certificate used during the SSL build process.
   - Userid/CODE.SIGNATURE.VERIFICATION.KEYRING The userid can be any valid RACF userid
   - Root CA is shipped NOTRUSTed and needs to be made TRUSTed

2. Facility class profile IRR.PROGRAM.SIGNATURE.VERIFICATION profile needs to exist and the APPLDATA field needs to contain the name of the signature verification key ring.

System SSL Module Verification

3. Activate PROGRAM control
4. Create the PROGRAM class profile that protects the program verification module IRRPVERS and specify its signature verification options.
5. Activate program signature verification by running the IRRVERLD program which loads and verifies the program verification module IRRPVERS.
6. Create the PROGRAM class profiles to indicate the System SSL modules must be signed.
7. Refresh PROGRAM control

System SSL Module Verification

- Create code signing key ring and connect STG code signing CA certificate
  - RACDCERT CERTAUTH LIST(LABEL('STG Code Signing CA'))
  - RACDCERT CERTAUTH ALTER (LABEL('STG Code Signing CA')) TRUST
  - RACDCERT ID(RACFADM) ADDRING(CODE.SIGNATURE.VERIFICATION.KEYRING)
  - RACDCERT ID(RACFADM) CONNECT(RING(CODE.SIGNATURE.VERIFICATION.KEYRING) CERTAUTH LABEL('STG Code Signing CA') USAGE(CERTAUTH))
- Create facility profile to active code signing capabilities
  - RDEFINE FACILITY IRR.PROGRAM.SIGNATURE.VERIFICATION APPLDATA('RACFADM/CODE.SIGNATURE.VERIFICATION.KEYRING')
- Activate changes and enable PROGRAM control
  - SETROPTS RACLIST(FACILITY) REFRESH
  - SETROPTS RACLIST(DIGTCERT, DIGTRING) REFRESH
  - SETROPTS WHEN(PROGRAM)
- Activate signature verification support
  - RDEFINE PROGRAM IRRPVERS ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
  - SETROPTS WHEN(PROGRAM) REFRESH
  - Execute IRRVERLD job

System SSL Module Verification

- RDEFINE PROGRAM GSKSSL ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
- RDEFINE PROGRAM GSKSSL64 ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
- RDEFINE PROGRAM GSKS31F ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
- RDEFINE PROGRAM GSKS64F ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
- RDEFINE PROGRAM GSKCMS31 ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
- RDEFINE PROGRAM GSKCMS64 ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
- RDEFINE PROGRAM GSKC31F ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
- RDEFINE PROGRAM GSKC64F ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
- RDEFINE PROGRAM GSKSRVR ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
- RDEFINE PROGRAM GSKKYMAN ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
- RDEFINE PROGRAM GSKSRBRD ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))
- RDEFINE PROGRAM GSKSRBWT ADDMEM('SYS1.SIEALNKE'//NOPADCHK) UACC(READ) SIGVER(SIGREQUIRED(YES) FAILLOAD(ANYBAD) SIGAUDIT(ANYBAD))

- SETROPTS WHEN(PROGRAM) REFRESH

Using System SSL z/OS V1R13 in FIPS mode

- System SSL has the capability to execute securely in a mode that has been designed to meet the NIST FIPS 140-2 criteria.
- Executes in either 'FIPS mode' or 'non-FIPS mode‘.
- By default runs in 'non-FIPS' mode.

Certificates and Certificate Stores

- **Supported Certificate Stores**
  - SAF Key Rings
  - PKCS #11 Tokens
  - Key Database Files created through gskkyman
- **Key database files**
  - must be recreated through gskkyman specifying FIPS mode
  - Will only contain certificates valid for FIPS mode (FIPS databases can also be used in non-FIPS mode but not vice versa)
- **SAF Key rings and PKCS #11 tokens**
  - contain certificates with keys sizes or algorithms that are not supported in FIPS mode as long as those certificates are never used while executing in FIPS mode.
  - if an attempt to use a certificate with unsupported key size or algorithms is made, then the process will fail.
  - corrective action is to either add/replace certificates with key sizes and algorithms that are valid in FIPS mode

Create FIPS key database file

Database Menu

1 - Create new key database
2 - Open key database
3 – Change database password
4 – Change database record length
5 – Delete database
6 – Create key parameter file
7 – Display certificate file (Binary or Base64 ASN.1 DER)

11 – Create new token
12 – Delete token
13 – Manage token
14 – Manage token from list of tokens

Enter option number: 1
Enter key database name (press ENTER to return to menu): /home/server/key.kdb
Enter database password (press ENTER to return to menu): password
Re-enter database password: password
Enter password expiration in days (press ENTER for no expiration): enter
Enter database record length (press ENTER to use 5000): enter

Enter 1 for FIPS mode database or 0 to continue: 1

Key database /home/server/key.kdb created.

Application Changes

- To enable your application to execute in the mode designed to meet FIPS 140-2, API gsk_fips_state_set needs to be called.
  - gsk_status **gsk_fips_state_set** (GSK_FIPS_STATE_ENUM_VALUE enumValue)
  - **GSK_FIPS_STATE_ON –** Sets state to FIPS mode
  - **GSK_FIPS_STATE_OFF –** Sets state to non-FIPS mode.
- In order to set GSK_FIPS_STATE_ON, this function must be executed **prior** to all other SSL API functions with the exception of gsk_get_cms_vector, gsk_get_ssl_vector and gsk_fips_state_query.
- Notes:
  - Applications cannot switch from non-FIPS to FIPS mode.
  - Applications can switch from FIPS to non-FIPS mode.

Application Changes cont'd

- To determine the active FIPS mode,
  - gsk_status **gsk_fips_state_query** (GSK_FIPS_STATE_ENUM_VALUE enumValue)
  - **GSK_FIPS_STATE_NOSET –** mode not set
  - **GSK_FIPS_STATE_ON –** FIPS mode enabled
  - **GSK_FIPS_STATE_OFF –** Non-FIPS mode enabled
- To execute self-tests on-demand
  - gsk_status **gsk_perform_kat**()

Application Changes cont'd

Handling severe cryptographic failures

- When executing in FIPS mode and a severe cryptographic problem is encountered, the application should be terminated and restarted.

- If execution continues, all APIs will fail except for:
  - gsk_get_cms_vector
  - gsk_get_ssl_vector
  - gsk_fips_state_query
  - gsk_query_crypto_level
  - gsk_strerror

- Severe cryptographic return codes are:
  - CMSERR_BAD_RNG_OUTPUT - Failure during random number generation
  - GSK_ERR_RNG, GSK_ERROR_RNG - Failure during random number generation
  - CMSERR_FIPS_KEY_PAIR_CONSISTENCY - Failure when generating either a RSA or DSA key pair
  - CMSERR_KATPW_FAILED - Failure was encountered by the gsk_perform_kat API when performing known answer tests against the System SSL cryptographic algorithms.

Enabling AT-TLS Security Policy for FIPS

- Application Transparent Transport Layer Security (AT-TLS) consolidates TLS implementation in one location, reducing or eliminating application development overhead, maintenance, and parameter specification. AT-TLS is based on z/OS System SSL, and transparently implements these protocols in the TCP layer of the stack

- Attributes of the TLS connections are defined by a security policy.

- To set FIPS mode within a security policy
  - **TTLSGroupAction Parameters:**
    - TTLSGroupAdvancedParms
      - *FIPS140 Off (default)*
      - *FIPS140 On*

How did System SSL meet FIPS 140-2 Level 1 Requirements

Cryptographic module specification	Security Policy states cryptographic boundary, platforms, approved security functions and modes
Cryptographic module ports and interfaces	System SSL external publication describes all interfaces to the cryptographic module; Security Policy lists APIs
Roles, services and authentication	Supports logical separation of roles, all supported approved security functions in Security Policy, authentication through z/OS operating system login process
Finite state model	Internal document provided to CST Lab
Physical security	Production grade components
Operational environment	Security Policy describes operational environment; APIs gsk_fips_state_set, gsk_fips_state_query, gsk_perform_kat etc.
Cryptographic Key Mgmt	Keys can flow into and out of cryptographic module in the clear, all CSPs zeroed out when no longer used, using approved RNG, key generation and key exchange security functions
EMI/EMC	FCC A and B ratings
Self-test	Power up, Continuous, Pair-wise consistency and Integrity tests
Design assurance	Appropriate Design documents to CST lab
Mitigation of other attacks	N/A

When is validation needed?

- My application or product contains 1 or more cryptographic algorithm implementations?
  1. Validation is required if any of the cryptographic algorithms are for a FIPS approved algorithm. Non-approved algorithms cannot be validated and must not be utilized when running in FIPS compliant mode
  2. All algorithm implementations are for FIPS non-approved algorithms. Validation is not possible

- My application or product utilizes crypto provided by an approved cryptographic module.
  1. No special validation needs to be done. Application is consider compliant as long as the application is using the cryptographic module according to the module's Security Policy

Review

- **Overview of FIPS 140-2**
  - What is FIPS 140-2
  - FIPS 140-2 Requirements
  - FIPS 140-2 Security Levels
  - FIPS 140-2 Validation Types
  - Security Policy
  - Validation Process Flow
- **Using z/OS System SSL in FIPS mode**
  - Requirements/Configuration
  - Application changes
  - Enabling AT-TLS for FIPS

References

- **FIPS 140-2 Security Requirements for Cryptographic Modules:**
  http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- **Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules:**
  http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm
- **Cryptographic Algorithm Validation Program**
  http://csrc.nist.gov/groups/STM/cavp/index.html
- **Validated Algorithms:**
  http://csrc.nist.gov/groups/STM/cavp/validation.html
- **Testing Laboratories:**
  http://csrc.nist.gov/groups/STM/testing_labs/index.html
- **Cryptographic Server Manual**
  Cryptographic Services System Secure Sockets Layer Programming

Questions?

Alyson Comer
Session 12536