Building FIPS 140-2 Compliant Configuration for SAS9.3 BI Web Applications

Heesun Park, PhD
SAS Institute, Inc

ACSAC 2011
December 2011, Orlando, USA

Table of Contents

- Overview of FIPS 140-2: “Security requirements for Cryptographic Modules”
- FIPS 140-2 Approved Encryption Algorithms
- Protection of Critical Security Parameters (CSP)
- Configuration for SAS 9.3 EBI Web Applications
- Securing Transport
- Securing Application Server
- Protection of CSPs for SAS 9.3 Server Configuration
- Conclusion

FIPS 140-2 Overview

- Security Levels (1 through 4)
- Evaluation Assurance Level (EAL1 through EAL7)
- Security Requirements
- Functional Security Objectives
- Cryptographic Module Validation Program (CMVP)
- Critical Security Parameters (CSP)

FIPS 140-2 Functional Security Objectives

- To implement “Approved” security functions
- To protect cryptographic module from unauthorized use or operation
- To prevent the unauthorized and undetected modification of CSPs
- To detect errors in the operation of the cryptographic module and to prevent the compromise of sensitive data and CSPs resulting from these errors

FIPS 140-2 Approved Cryptographic Algorithms and Modules

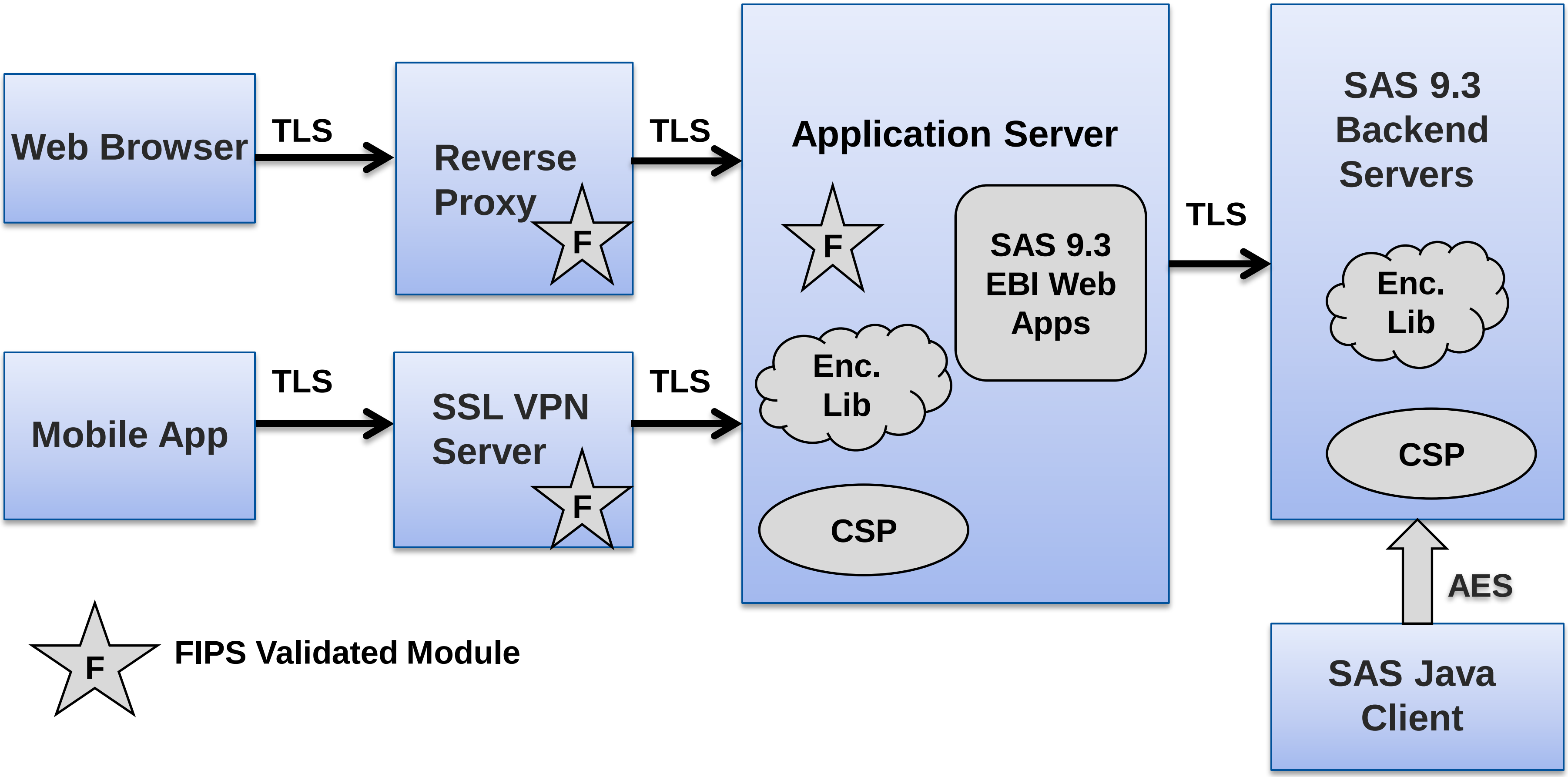
- SSL Handshake Protocol: TLS 1.0
- Key Exchange Algorithms: DSA, RSA, Diffe-Helman
- Symmetric Encryption Algorithms: AES, 3DES
- Hash Algorithm: SHA-1
- CMVP: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

  - OpenSSL FIPS Object Module
  - IBM Java JCE FIPS 140-2 Cryptographic Module
  - (many more)

FIPS Validation Claims and Criteria

- "The proper claim is that the vendor product ***uses*** FISP 140-2 validated cryptography, not that the product (Apache httpd, application server, etc) itself is validated. This means that the claim can be from incontrovertible to dubious, with some large grey area in between."

Configuration for SAS 9.3 Enterprise BI Web Applications



Securing Transport – SSL Handshake (I)

- Handshake protocol should be TLS 1.0
- Server identity certificate should be signed by CA with SHA-1 hash algorithm.
- FIPS 140-2 approved symmetric encryption algorithm should be available on both sides.
- FIPS 140-2 validated cryptographic module could reside in reverse proxy server, SSL VPN server and application server.
- FIPS 140-2 validated cryptographic module will enforce the use of FIPS 140-2 approved symmetric encryption algorithm during SSL handshake process.

Source of Encryption Algorithms (Cipher Suites)

- IE8 depends on the Windows operating system SSL library (Schannel.dll). Newer Windows OS carries FIPS 140-2 approved encryption algorithms.
- FireFox7 carries its own encryption algorithms. Selection of encryption algorithms can be controlled through its configuration utility – about:config.
- JDK on which application server is based carries the cipher suites. Selection of FIPS approved encryption algorithm can be made through the application server's admin console (in case of WebSphere) or through <connector> definition for the server (in case of Jboss)

SSL Handshake Monitoring Tool – sec_con_FIPS

- It is a lightweight web application deployed in application server.
- It displays all SSL handshake and encryption library related information including handshake protocol selected, available encryption algorithms, FIPS 140-2 approved encryption algorithms, selected symmetric encryption algorithm, hash algorithm used, etc.
- It also displays JAAS authentication related information such as Subject, Principals and security role mapping information to facilitate authentication (Single Sign-On) debugging.
- It is available upon request.

Protection of CSPs from Application Server

- FIPS validated cryptographic module typically covers SSL based communication only.
- Symmetric encryption algorithms in cipher suites should include FIPS 140-2 approved ones.
- For protection of internal CSPs such as passwords and keys, they need to be encrypted with FIPS approved encryption algorithms.
- Some application servers offer “Use FIPS algorithms” SSL option (WebSphere).

FIPS mode in “Connector” level

- When an application server does not have FIPS validated cryptographic module, use of FIPS approved encryption algorithm can be forced in “connector” level.
- Jboss connector definition example:

```
<Connector port="8443" address="${jboss.bind.address}"
        protocol="HTTP/1.1" SSLEnabled="true"
        maxThreads="150" scheme="https" secure="true"
        emptySessionPath="true" clientAuth="false" sslProtocol="TLS"
        keystoreFile="/usr/local/certs/serverids.jks" keystorePass="mypassword"
        ciphers=
”TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA” />
```

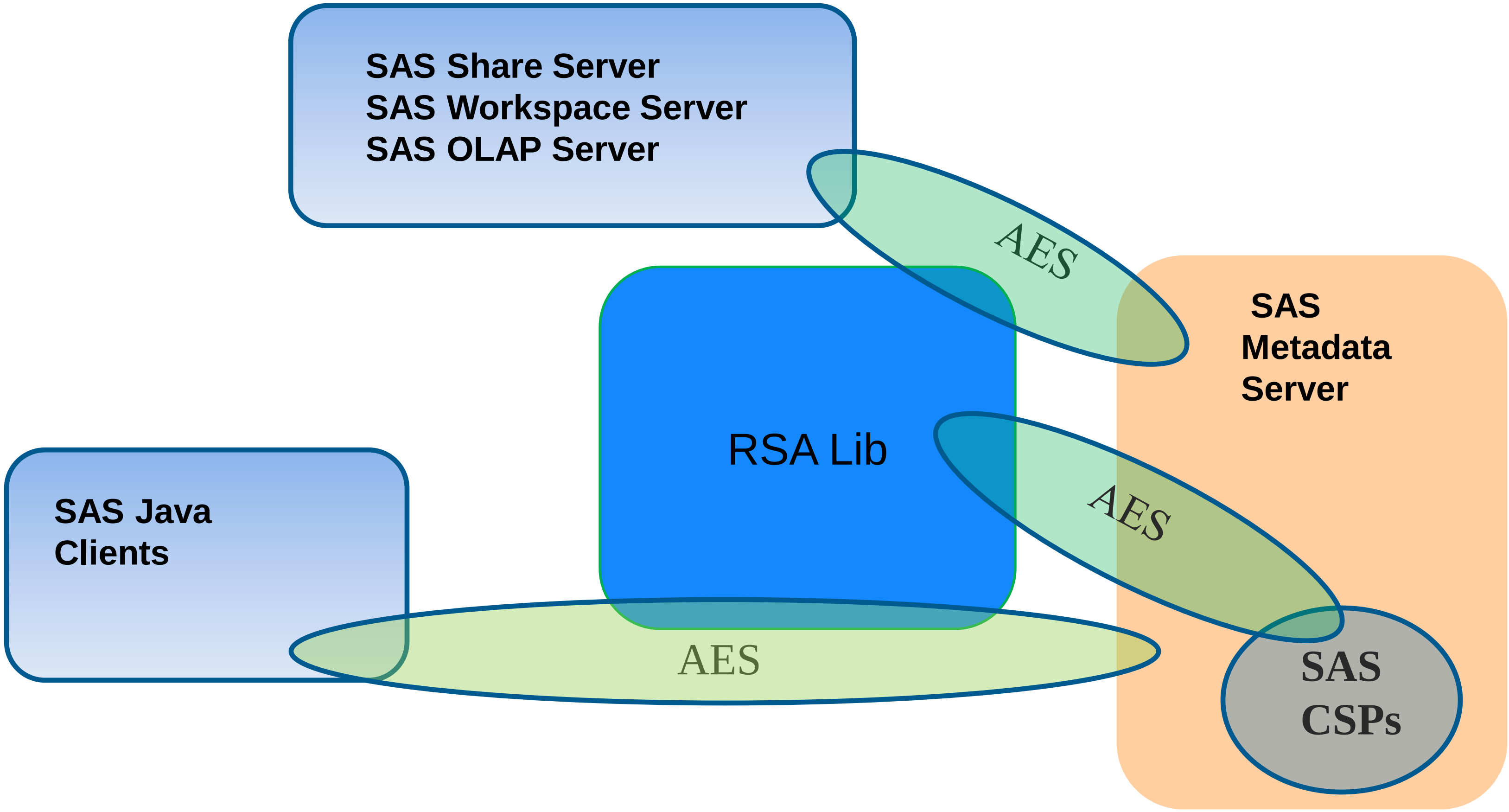
Protection of CSPs for SAS 9.3 Server Configuration

- SAS Global option “encryptFIPS” forces use of AES encryption for CSPs, communication between SAS Java Clients and SAS Metadata server and communication between SAS Metadata server and other servers.
- SAS Metadata server manages most of SAS CSP resources for SAS server configuration.
- FIPS 140-2 approved AES encryption comes from RSA library that SAS licensed.
- Encryption of application data should be handled separately.

List of SAS 9.3 Configuration CSPs

- Login password on disk in the metadata (AES)
- Internal account password on disk in the metadata (SHA-256)
- Password on disk in a configuration file (AES)
- SAS data sets on disk (optional) – it can be done better with hardware based encryption option.

FIPS mode operation in SAS 9.3 Server Configuration



Conclusion

- Strict FIPS 140-2 compliance for whole configuration is very difficult.
- The policy of the organization should prioritize the depth and the width of the FIPS mode of operation.
- Each configuration level, such as client applications, application server layer and compute server layer, should be evaluated based on the risk tolerance level of the organization.

References

- FIPS 140-2 : “SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES”
- http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- NIST Special Publication 800-52 : “Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations “
- http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf

Contact Information

- Name: Heesun Park
- Email: sashsp@sas.com
- Phone: (919) 531-7769