IBM Education Assistant (IEA) for z/OS V2R3

Line Item Names: Detect and recover from hardware crypto outage
Standards Currency
FIPS key size enforcement
Tolerate new style GSKit CMS files

Element/Component: System SSL

Material was current as of March 2017

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Session Objectives

- At the end of this presentation, you should have an understanding of the System SSL enhancements for:
  - RAS
    - Detect and recover from hardware crypto outage
    - Tolerate new style GSKit CMS files
    - gskkyman usability enhancements
  - Standards Currency
  - FIPS key size enforcement
    - FIPS key enforcement for IBM TDS for z/OS (LDAP) (covered in the appendix of this presentation)
    - FIPS key enforcement for NAS (Kerberos) (covered in their presentation)
    - FIPS key enforcement for PKI Services (covered in their presentation)

Overview (RAS)

- Problem Statement / Need Addressed
  - Detect and recover from hardware crypto outage
    - When ICSF goes down, RSA clear key cryptographic operations revert to using software cryptography even if ICSF comes back up.
    - Hardware cryptography is not used again until the System SSL application is recycled.
  - Tolerate new style GSKit CMS files
    - System SSL routines are unable to use certificates that are contained in new style GSKit CMS files
  - gskkyman usability enhancements
    - Command line does not have the capability to display binary or DER encoded certificates (RFE 70659)
    - Unable to create kdb files without the default CA certificates included
    - Unable to display subject alternate names present in certificate requests via the gskkyman interactive menus

Overview (RAS)

- Solution
  - Detect and recover from hardware crypto outage
    - Attempt to use hardware crypto each time a RSA clear key cryptographic operation is required
  - Tolerate new style GSKit CMS files
    - Update System SSL routines so that new style GSKit CMS files can be read (no updates are allowed)
  - gskkyman usability enhancements
    - Add new command line option -der to allow display of DER encoded certificates
    - Add a new option 1b to the “Database” interactive menu in gskkyman to allow for creation of kdb files without known CAs
    - Update the display of the certificate requests to display the subject alternate names

Overview (RAS)

- Benefit / Value
  - Detect and recover from hardware crypto outage
    - No longer need to recycle the System SSL application when ICSF goes down
  - Tolerate new style GSKit CMS files
    - Will be able to directly using the certificates contained in the new style GSKit CMS files
  - gskkyman usability enhancements
    - Command options can be used to display certificates in kdb files (allows for easier shell scripting setup)
    - Default CA certificates no longer need to be included in newly created key database files
    - Subject alternate names can now be displayed in certificate requests in the gskkyman interactive menus

Usage & Invocation (RAS)

- Detect and recover from hardware crypto outage
  - No user intervention or configuration is required
    - Always attempt to use hardware crypto even when ICSF has gone down
- Tolerate new style GSKit CMS files
  - System SSL will transparently read certificates that exist in the new GSKit CMS files
- gskkyman usability enhancements
  - Command line option (-der) has been added to the -dc and -dcv options to allow display of DER encoded certificate files
    - **gskkyman -dc|-dcv [-k** *filename*|**-t** *tokenname*|**-p12** *filename***|*-der*** *filename***] [-l** *label***]**
  - The database menu in interactive mode has been updated for option 1b to create a key database file without the default CA certificates included (See appendix)
  - Certificate request display updated (See appendix)

Usage & Invocation – RAS updates

```
                         Database Menu


   1   - Create new database
   1b  - Create new empty database
   2   - Open 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


   0   - Exit program
```

Usage & Invocation – RAS updates

- gskkyman usability enhancements (continued)
  - Display of certificate requests from the Request or Token Certificate Request menu will now include subject alternate names

```
                    Key Information
                 Label: Cert Request
             Record ID: 13
      Issuer Record ID: 13
           Default key: No
 Private key algorithm: rsaEncryption
      Private key size: 2048
          Subject name: My Certificate Request
                          ID
                          IBM
                          Poughkeepsie
                          NY
                          US

Subject alternate name: DNS: mydns.com
                             EMAIL: myemail@us.ibm.com
                             IPV4: 9.9.9.9
```

Interactions & Dependencies (RAS)

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters:
  - Users of gskkyman
  - Any z/OS System SSL application

Overview – Standards Currency

- Problem Statement / Need Addressed
  - System SSL functionality is based upon industry standards. As TLS and x.509 Certificate standards change and functionality is changed or added System SSL must also change.
    - TLS handshake related updates
      - RFC 6460 – Suite B Profile for Transport Layer Security (TLS)
      - RFC 5759 – Suite B Certificate and Certificate Revocation List (CRL) Profile
      - RFC 7507 – TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks
    - OCSP (Online Certificate Status Protocol) Revocation updates:
      - RFC 6960 – x.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
      - RFC 6277 – Online Certificate Status Protocol Algorithm Agility
      - RFC 6066 – Transport Layer Security (TLS) Extensions Definitions
      - RFC 6961 - The Transport Layer Security (TLS) Multiple Certificate Status Request Extension

Overview – Standards Currency

- Solution
  - Suite B (RFCs 6460 and 5759)
    - The GSK_SUITE_B_PROFILE environment / attribute support has been updated to allow specification of 128 minimum and 192 minimum profiles.
    - When the minimum profile settings are specified, the certificate validation performed adheres to RFC 5759 which elevates many of the “may” and “should” level options specified in RFC 5280.
  - Protocol Fallback (RFC 7507)
    - Add support for the Signaling Cipher Suite Value (SCSV). The SCSV indicates to the server that the client is attempting to fallback to an earlier TLS or SSL protocol version after a previous handshake attempt failed. The server fails if it supports a higher protocol.

Overview – Standards Currency

- Solution
  - OCSP Revocation Support was added to System SSL in V2R2 and was based on RFC 2560. In V2R3, System SSL added the following functional enhancement for RFCs 6277 and 6960
    - Allow for the specification of a preference ordered list of hash and signature algorithm pair that will be provided on the OCSP request to indicate to the OCSP responder which algorithms should be used by the responder to signed the OCSP response.
  - Support for the “Certificate Status Request” (RFC 6066) and the “Multiple Certificate Status Request” (RFC 6961) extensions being specified in the “CLIENT-HELLO” message. These extensions indicate that the client wants the server to obtain the OCSP responses for the server's certificate(s) on its behalf.
    - Commonly referred to as OCSP stapling as the OCSP responses are sent in a SSL/TLS handshake message

Overview – Standards Currency

- Benefit / Value
  - OCSP related updates
    - Allows for more secure hashing algorithms to be used for the OCSP response – if the OCSP responder supports it
    - Constrained clients (such as mobile devices and web browsers) the ability to request the OCSP responses for the server's certificates without directly needing to contact the OCSP responder
  - TLS handshake related updates
    - Allows for additional certificate checking to be done while in a Suite B 128-bit minimum or 192-bit minimum environment
    - Ensures that clients are using the latest TLS protocol level supported by the server

Usage & Invocation – Suite B

- **GSK_SUITE_B_PROFILE** environment variable and attribute (gsk_attribute_[gs]et_enum()) is updated for 128MIN and 192MIN
  - 128MIN
    - Ciphers enabled: C02BC02C
    - Hash and Signature algorithms: 04030503
      - 0403: ECDSA with SHA-256, 0503: ECDSA with SHA-384
    - Supported ecurves: 00230024
      - 0023: secp256r1, 0024: secp384r1
  - 192MIN
    - Ciphers enabled: C02C
    - Hash and Signature algorithms: 0503
    - Supported ecurves: 0024
  - 128 (Existing support)
    - Ciphers enabled: C02BC023
    - Hash and Signature algorithms: 0403
    - Supported ecurves: 0023

Usage & Invocation – Suite B

- 192 (Existing support)
  - Ciphers enabled: C02CC024
  - Hash and Signature algorithms: 0503
  - Supported ecurves: 0024
- All (Existing support)
  - Ciphers enabled: C02CC024C02BC023
  - Hash and Signature algorithms: 05030403
  - Supported ecurves: 00230024

- When Suite B is set to 128MIN or 192MIN, the certificates must adhere to the specifications documented in RFC 5759
- Enhances the certificate validation specifications outlined in RFC 5280

Usage & Invocation – Protocol Fallback

- Indicates what the server ought to do if the SCSV (Signaling Cipher Specification Value) is included in the client's cipher list during the CLIENT-HELLO message in a SSL/TLS handshake
- Clients, such as web browsers, include the SCSV (x'5600') on subsequent handshake attempts if a previous handshake attempt has failed.
- New **GSK_SERVER_FALLBACK_SCSV** environment variable and attribute type (gsk_attribute_[sg]et_enum())
  - **ON** (GSK_SERVER_FALLBACK_SCSV_ON): Indicates that the server supports the TLS fallback Signaling Cipher Suite Value (SCSV). If the SCSV is present in the client's supported list and the TLS or SSL protocol level that is specified by the client during the handshake is less than the highest TLS or SSL protocol level that is supported by the server, the SSL or TLS handshake attempt fails.
  - **OFF** (GSK_SERVER_FALLBACK_SCSV_OFF): Indicates that the server ignores the SCSV when included in the client's supported cipher list during an SSL or TLS handshake. Default setting

Usage & Invocation – OCSP: RFC 6960

- Allow System SSL applications enabled for OCSP to specify a preference ordered list hash and signature algorithms for signing the OCSP response

- **GSK_OCSP_RESPONSE_SIGALG_PAIRS** environment variable / attribute type (gsk_attribute_[gs]et_buffer())
  - Allowed hash and signature algorithms

    0101 – MD5 with RSA
    0201 – SHA-1 with RSA
    0202 – SHA-1 with DSA
    0203 – SHA-1 with ECDSA
    0301 – SHA-224 with RSA
    0302 – SHA-224 with DSA
    0303 – SHA-224 with ECDSA
    0401 – SHA-256 with RSA
    0402 – SHA-256 with DSA
    0403 – SHA-256 with ECDSA
    0501 – SHA-384 with RSA
    0503 – SHA-348 with ECDSA
    0601 – SHA-512 with RSA
    0603 – SHA-512 with ECDSA

  - Example: 060105010401

  - Default: None – Indicates that the OCSP response will be signed based upon the OCSP responder configuration which in most cases is the algorithm used to sign the OCSP request

Usage & Invocation – OCSP Stapling

- Support the "Certificate Status" and "Multiple Certificate Status" request extensions if specified by the client on a "CLIENT-HELLO" message. These extensions indicate to the server to retrieve the OCSP responses for server certificates and send them to the client
  - OCSP support must be enabled in the server: GSK_OCSP_URL and/or GSK_OCSP_ENABLE
- **GSK_SERVER_OCSP_STAPLING** new environment variable / attribute type (gsk_attribute_[sg]et_enum())
  - **OFF**: Server does not support the extensions and the OCSP responder(s) are not queried for revocation status of server's certificates
  - **ENDCERT**: Server supports the extensions but the OCSP responder is only contacted for the revocation status of the server's end entity certificate
  - **ANY**: Server supports the extensions and if the "Multiple Certificate Status" request extension is specified the OCSP responder(s) are contacted to retrieve the revocation status of each of the server's certificates – other than the server's root CA certificate

Usage & Invocation – OCSP Stapling

- Server applications can query to determine if the “Certificate Status” or “Multiple Certificate Status” request extension been negotiated between the client and server on a connection handle
  - GSK_TLSEXT_SERVER_OCSP_STAPLING - gsk_attribute_get_enum()
    - GSK_TLSEXT_SERVER_OCSP_STAPLING_ON – Indicates that the server has negotiated either of the extensions
    - GSK_TLSEXT_SERVER_OCSP_STAPLING_OFF – Indicates that the server has NOT negotiated either of the extensions

Usage & Invocation – OCSP Stapling

- Server applications can check to see if an OCSP response has been sent to the client during the SSL/TLS handshake process on a connection handle
  - GSK_SERVER_OCSP_STAPLING_CERTSTATUS – gsk_attribute_get_enum()
    - GSK_SERVER_OCSP_STAPLING_CERTSTATUS_ENDENTITY – Server is able to successfully retrieve the OCSP response for the server's end entity certificate and send it back to the client.
    - GSK_SERVER_OCSP_STAPLING_CERTSTATUS_ANY – Server is able to successfully retrieve the OCSP responses for more than one of the server's certificates in its chain and sends them back to the client.
    - GSK_SERVER_OCSP_STAPLING_CERTSTATUS_OFF – Server is not configured for OCSP stapling or is unable to successfully retrieve the OCSP responses for the server's end entity certificate or any certificates in the server's chain.

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - IBM HTTP Server powered by Apache and a web browser, such as Firefox (OCSP stapling)
  - AT-TLS
  - Any System SSL application

Overview – FIPS enforcement

- Problem Statement / Need Addressed
  - System SSL applications running in FIPS mode need to enforce the algorithm and key length restrictions cited in:
    - NIST Special Publication 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.*
  - US Federal Government applications that exploit the TLS protocol follow specifications cited in:
    - NIST Special Publication 800-52 Revision1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.*

Overview – FIPS enforcement

- Solution
  - New System SSL FIPS levels: LEVEL1, LEVEL2, and LEVEL3
  - Allow server applications the ability to use multiple key labels
  - Minimum peer certificate version and minimum peer certificate key sizes for RSA, DSA, DH, and ECDSA are now supported
  - Minimum Diffie-Hellman group size can be specified for server and client applications
- Benefit / Value
  - System SSL applications will now adhere to the latest FIPS 140-2 Level 1 specifications
  - Server applications are able to handle secure connections from additional client applications
  - Applications are able to ensure that peer certificates meet minimum requirements

Usage & Invocation – FIPS enforcement

- **GSK_FIPS_STATE** levels now supported in gsk_fips_state_set() and gsk_fips_state_query().
  - GSK_FIPS_STATE_OFF (existing and default)
  - GSK_FIPS_STATE_ON (existing) and GSK_FIPS_STATE_LEVEL1 (new)
    - FIPS-140-2 using 80 bit security strength
  - GSK_FIPS_STATE_LEVEL2 (new)
    - Supports using 112 bit security strength along with some LEGACY behavior as defined by NIST SP800-131A
  - GSK_FIPS_STATE_LEVEL3 (new)
    - Supports using 112 bit security strength as defined by NIST SP800-131A
- Multiple key labels can be specified in server applications using the **GSK_SERVER_KEYRING_LABEL_LIST** attribute type or the **GSK_SERVER_KEY_LABEL_LIST** environment variable
  - Supports diverse clients using different ciphers
  - Handles expiring certificates

Usage & Invocation – FIPS enforcement

- Specification of minimum peer certificate key sizes (attribute types / environment variables)
  - Default minimum key sizes
    - Non-FIPS, FIPS ON, or Level 1 – RSA/DSA/DH 512-1024, ECC 160-192
    - FIPS Level 2 or 3 – RSA/DSA/DH 2048, ECC 192
  - To allow smaller key sizes (non-FIPS) to be used or to require a larger key size
    - **GSK_PEER_ECC_MIN_KEY_SIZE**
    - **GSK_PEER_DH_MIN_KEY_SIZE**
    - **GSK_PEER_DSA_MIN_KEY_SIZE**
    - **GSK_PEER_RSA_MIN_KEY_SIZE**
- **GSK_PEER_CERT_MIN_VERSION** attribute type / environment variable specifies the minimum peer certificate version allowed
  - 3 (GSK_PEER_CERT_MIN_VERSION_3) – Current certificate standard
  - ANY (GSK_PEER_CERT_MIN_VERSION_ANY) - Default

Usage & Invocation – FIPS enforcement

- **GSK_CLIENT_EPHEMERAL_DH_GROUP_SIZE** attribute type / environment variable specifies the minimum accepted server DH group size allowed on ephemeral Diffie-Hellman key exchange message
  - **LEGACY**: Group size 1024 for non-FIPS, 2048 for FIPS
  - **2048**: Group size 2048
- **GSK_SERVER_EPHEMERAL_DH_GROUP_SIZE** attribute type / environment variable specifies the minimum accepted server DH group size allowed on ephemeral Diffie-Hellman key exchange message between the client and server
  - **LEGACY**: Group size 1024 for non-FIPS, 2048 for FIPS
  - **2048**: Minimum group size of 2048
  - **MATCH**: Match the ephemeral Diffie-Hellman group to the server certificate's key strength.
    - If the key size is <= 1024, group size of 1024 is used
    - If the key size is > 1024, group size of 2048 is used

Usage & Invocation – FIPS enforcement

- Cipher default (GSK_V2_CIPHER_SPECS, GSK_V3_CIPHER_SPECS, and GSK_V3_CIPHER_SPECS_EXPANDED) lists no longer contain DES or Triple DES ciphers

Interactions & Dependencies – FIPS enforcement

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - AT-TLS
  - IBM Tivoli Directory Server for z/OS
  - PKI Services
  - Network Authentication Services (Kerberos)

Migration & Coexistence Considerations – FIPS enforcement

- Migration
  - Default peer minimum key sizes are changing
  - DES and Triple DES ciphers are being removed from the default cipher lists

Session Summary

- You should now be able to:
  - Understand the recent changes in System SSL (RAS, Standards Currency, and FIPS key size enforcement)
  - Be able to find any of the above information in the relevant publication(s)

Appendix

- Publications
  - z/OS Cryptographic Services System Secure Sockets Layer Programming
- Specifications
  - NIST Special Publication 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.*
  - NIST Special Publication 800-52 Revision1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.*
  - RFC 6460 – Suite B Profile for Transport Layer Security (TLS)
  - RFC 5759 – Suite B Certificate and Certificate Revocation List (CRL) Profile
  - RFC 7507 – TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks
  - RFC 6960 – x.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
  - RFC 6277 – Online Certificate Status Protocol Algorithm Agility
  - RFC 6066 – Transport Layer Security (TLS) Extensions Definitions
  - RFC 6961 - The Transport Layer Security (TLS) Multiple Certificate Status Request Extension

Usage & Invocation

- IBM Tivoli Directory Server updates
- Server updates:
  - New sslFipsState configuration option to set the FIPS mode. Supported values are: OFF, LEVEL1, LEVEL2, and LEVEL3
- LDAP client and utility (db2pwden and ldapexop) updates:
  - New -x command line option added
  - ldapsearch -h 127.0.0.1 -p 3022 -Z **-x level3** -K keydatabasefile -P passwd -D cn=admin -w secret -s sub -b "o=IBM" "objectclass=*
- An application developer can invoke the ldap_ssl_set_fips_state() routine before invoking the ldap_ssl_client_init() routine to enable FIPS enforcement in the SSL/TLS connection.