IBM Education Assistance for z/OS V2R2

Items: OCSP (Online Certificate Status Protocol)
PKCS#12 Certificate Keystore

Element/Component: System SSL

Material current as of May 2015

Agenda

- Trademarks
- Presentation Objectives
- Overview
- Usage & Invocation
- Presentation Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

Presentation Objectives

- At the end of this presentation, you should have an understanding of the System SSL enhancements for:
  - OCSP (Online Certificate Status Protocol)
  - PKCS#12 Certificate Keystore
- How to use these enhancements
- Understand how these enhancements affect installation and migration

Overview: OCSP (Online Certificate Status Protocol)

- Problem Statement / Need Addressed
  - Need easy and quick manner to determine certificate revocation status during the SSL/TLS handshake and when calling Certificate Management routine gsk_validate_certificate_mode()
  - System SSL supports the retrieval of Certificate Revocation Lists (CRLs) from an LDAP server to determine revocation status
    - CRLs can be very large which makes retrieval and storing them difficult
    - CRL must be parsed to determine if the certificate is revoked
    - CRL caching has some limitations:
      - Unable to set the cache size or the maximum size in bytes of a CRL allowed to be store in the cache
      - Global cache time out – All CRLs expire at the same time based upon when the first CRL was added to the cache

Overview: OCSP (Online Certificate Status Protocol)

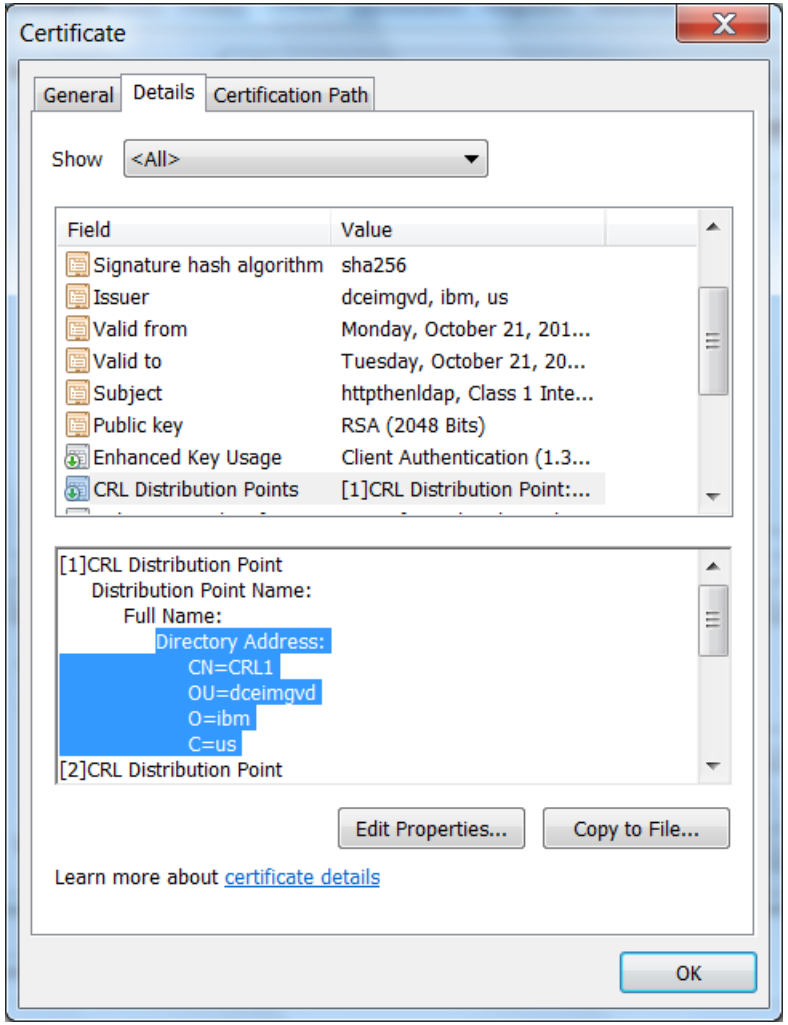
- Problem Statement / Need Addressed (continued)
  - CRL caching has some limitations (continued)
    - LDAP timeout – At the mercy of the LDAP server honoring the timeout value
  - Need ability to retrieve CRLs from HTTP servers
  - Support is needed for OCSP (Online Certificate Status Protocol) – RFC 2560

Overview: OCSP (Online Certificate Status Protocol)

- Solution
  - Add support for OCSP (Online Certificate Status Protocol)
  - Enhancements to LDAP CRL support:
    - Set cache size and cache entry max size
    - Allow CRLs to expire at different times based upon their individual expiration time
    - Allow LDAP timeout to be honored in System SSL in case LDAP server does not respond in a timely manner
  - Add support for HTTP CRLs retrieval
- Benefit / Value
  - Removes restriction that revocation information must be stored in an LDAP directory
  - Ability to utilize revocation information identified specifically to the certificate being validated
  - Timely retrieval of revocation information - OCSP

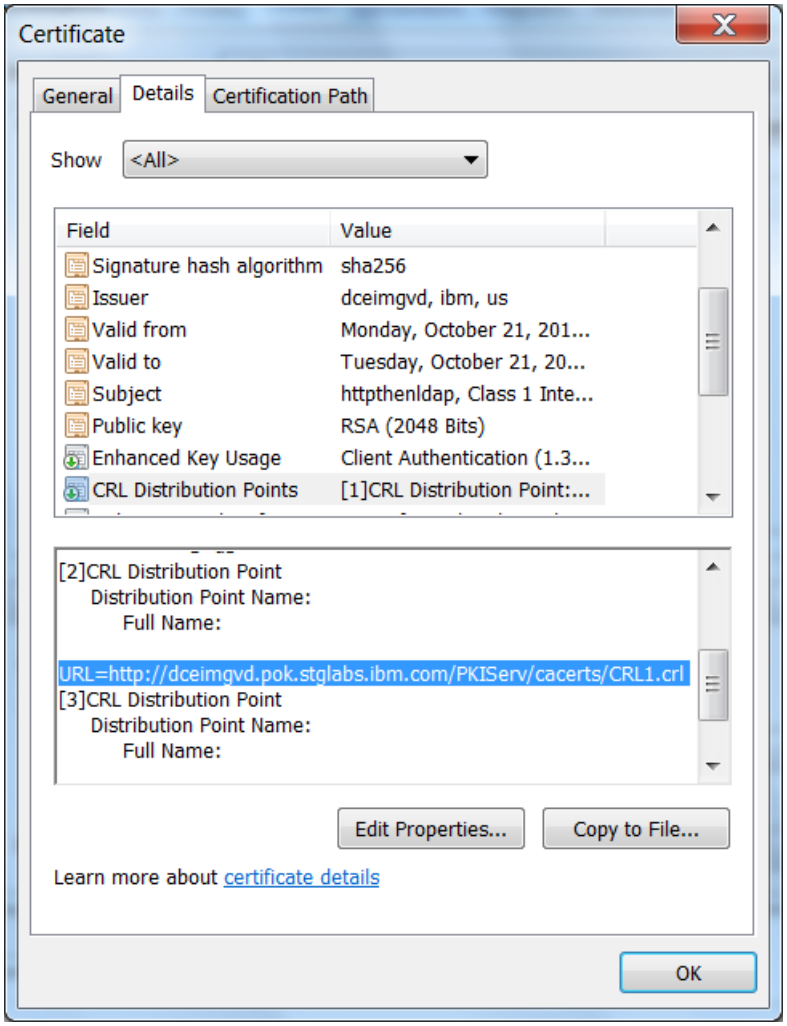
Overview: OCSP (Online Certificate Status Protocol)

- Prior to z/OS V2R2, System SSL supports certificate revocation through CRLs stored in a LDAP directory
  - LDAP Directory Server Name
  - Userid
  - Password
- CRLs are located through either a x.500 directory name specified in the certificates CRL Distribution Point Extension or the certificate's issuer name



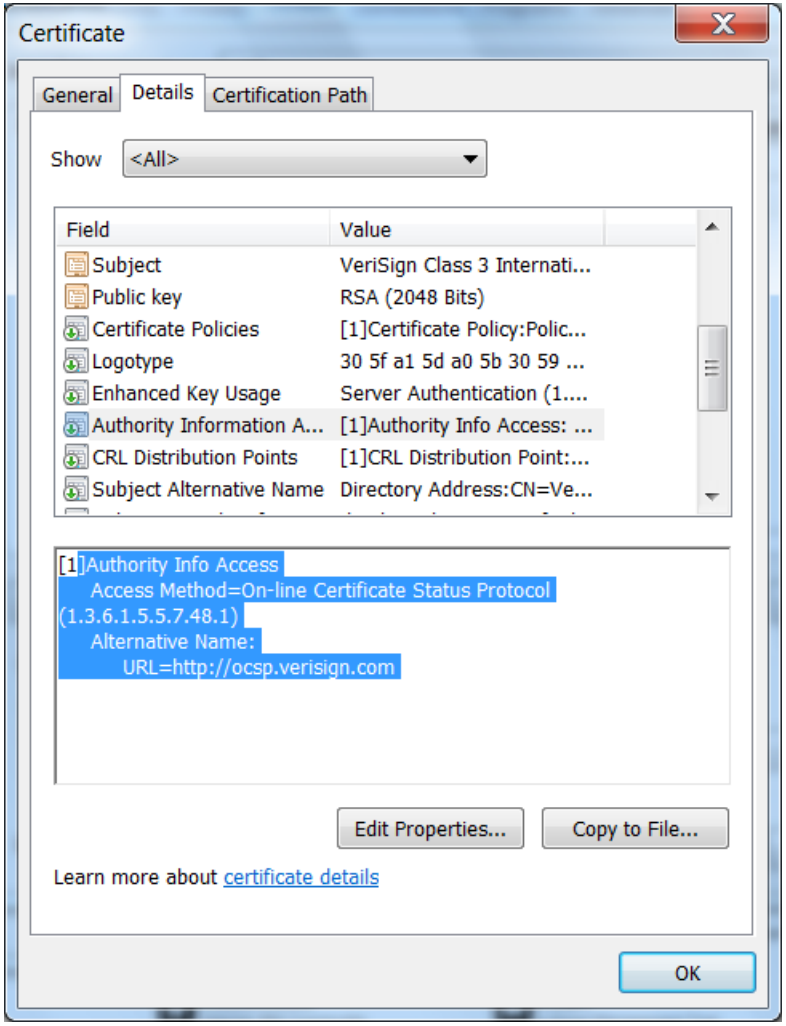
Overview: OCSP (Online Certificate Status Protocol)

- CRLs obtained through an HTTP URI are identified by the CRL Distribution Point extension within the certificate being validated.



Overview: OCSP (Online Certificate Status Protocol)

- OCSP was created as an alternative to certificate revocation lists (CRLs)
- Provides a timely retrieval of revocation information
- OCSP Responders (Servers) are identified through either the:
  - Authority Information Access (AIA) extension within the certificate being validated
  - Locally specified OCSP Responder



Overview: OCSP (Online Certificate Status Protocol)

- By default no revocation checking is performed
- Each revocation method must be enabled to be used
- Default Revocation order when revocation methods are enabled
  - OCSP URL dedicated responder
  - Authority Information Access (AIA) extension
  - CRL Distribution Point (CDP) Extension (HTTP URI)
  - LDAP Server
- In storage caching is enabled by default for each enabled revocation method
- Revocation information will be allowed to stay in the cache for its defined validity period
  - For example, nextUpdate value in the OCSP Response

Overview: OCSP (Online Certificate Status Protocol)

- System SSL applications now have the capability to:
  - Enable all or a subset of the revocation methods
  - Override the default revocation order
  - Tailor the size of the internal caches and entries
  - Customize the communication timeout and data sizes when retrieving OCSP responses, HTTP CRLs or LDAP CRLs
- System SSL applications are able to tailor the revocation processing through either environment variables or API attribute values
- Applications using gsk_validate_certificate_mode() have the capability to specify OCSP, HTTP CDP and LDAP datasources.
  - New gsk_create_revocation_source() routine has been added to assist with the creation of the revocation data sources.
  - New gsk_free_revocation_source() routine frees the memory associated with the data sources when desired.

Overview: OCSP (Online Certificate Status Protocol)

- OCSP uses HTTP to communicate with an OCSP responder (server)
- System SSL in this case is an OCSP client
- OCSP request contains the serial number of the certificate being checked for revocation
- If OCSP request is well formed, OCSP responder returns the certificate revocation status:
  - Good (certificate is not revoked)
  - Revoked
  - Unknown (OCSP responder does not know about this particular certificate)

Usage & Invocation - OCSP

- New OCSP related environment variables and attribute types:
  - GSK_OCSP_ENABLE [ON | OFF]
  - GSK_OCSP_URL <*url*>
  - GSK_OCSP_URL_PRIORITY [ON | OFF]
  - GSK_OCSP_REQUEST_SIGKEYLABEL <*label*>
  - GSK_OCSP_REQUEST_SIGALG <*sigAlg*>
  - GSK_OCSP_RETRIEVE_VIA_GET [ON | OFF]
  - GSK_OCSP_PROXY_SERVER_NAME <*serverName*>
  - GSK_OCSP_PROXY_SERVER_PORT [1 – 65535]
  - GSK_OCSP_NONCE_GENERATION_ENABLE [ON | OFF]
  - GSK_OCSP_NONCE_CHECK_ENABLE [ON | OFF]
  - GSK_OCSP_NONCE_SIZE [8 – 256]
  - GSK_OCSP_CLIENT_CACHE_SIZE [0 – 32000]
  - GSK_OCSP_CLIENT_CACHE_ENTRY_MAXSIZE [0 – 32000]
  - GSK_OCSP_MAX_RESPONSE_SIZE [0 – 2147483647]
  - GSK_OCSP_RESPONSE_TIMEOUT [0 – 43200]

Usage & Invocation - OCSP

- GSK_OCSP_ENABLE [ON | OFF] – Specifies whether the AIA extensions in certificates are to be used for revocation checking
  - gsk_attribute_[sg]et_enum()
    - GSK_OCSP_ENABLE_OFF: Default
    - GSK_OCSP_ENABLE_ON
- GSK_OCSP_URL <*url*> – Specifies the HTTP URL of an OCSP responder
  - Certificates do not need an AIA extension to check an OCSP responder for revocation information
  - gsk_attribute_[sg]et_buffer()
- GSK_OCSP_URL_PRIORITY [ON | OFF] – Indicates if the GSK_OCSP_URL defined responder is checked before the responders in the AIA extension
  - gsk_attribute_[sg]et_enum()
    - GSK_OCSP_URL_PRIORITY_OFF
    - GSK_OCSP_URL_PRIORITY_ON: Default

Usage & Invocation - OCSP

- GSK_OCSP_REQUEST_SIGKEYLABEL <*label*> – Specifies the label of the key used to sign OCSP requests to the GSK_OCSP_URL defined responder
  - gsk_attribute_[sg]et_buffer() - Default: NULL
- GSK_OCSP_REQUEST_SIGALG <*sigAlg*> – Specifies the hash and signature algorithm pair used to sign OCSP requests to the GSK_OCSP_URL defined responder
  - gsk_attribute_[sg]et_buffer() - Default: 0401 (RSA with SHA256)
- GSK_OCSP_RETRIEVE_VIA_GET [ON | OFF] - Specifies if the HTTP GET method should be used when sending an OCSP request
  - gsk_attribute_[sg]et_enum()
    - GSK_OCSP_RETRIEVE_VIA_GET_OFF: Default – Use POST
    - GSK_OCSP_RETRIEVE_VIA_GET_ON

Usage & Invocation - OCSP

- GSK_OCSP_PROXY_SERVER_NAME <*serverName*> – Specifies the DNS name or IP address of the OCSP proxy server
  - gsk_attribute_[sg]et_buffer() - Default: NULL

- GSK_OCSP_PROXY_SERVER_PORT [1 – 65535] – Specifies the OCSP proxy server port
  - gsk_attribute_[sg]et_numeric_value() - Default: 80

Usage & Invocation - OCSP

- GSK_OCSP_NONCE_GENERATION_ENABLE [ON | OFF] – Specifies if OCSP requests include a generated nonce
  - gsk_attribute_[sg]et_enum()
    - GSK_OCSP_NONCE_GENERATION_ENABLE_ON
    - GSK_OCSP_NONCE_GENERATION_ENABLE_OFF: Default
- GSK_OCSP_NONCE_CHECK_ENABLE [ON | OFF] – Specifies if OCSP response nonce checking is enabled. (Setting this to ON sets *GENERATION_ENABLE to ON)
  - gsk_attribute_[sg]et_enum()
    - GSK_OCSP_NONCE_CHECK_ENABLE_ON
    - GSK_OCSP_NONCE_CHECK_ENABLE_OFF: Default
- GSK_OCSP_NONCE_SIZE [8 – 256] – Specifies the size in bytes for the value of the nonce to be sent in OCSP requests
  - gsk_attribute_[sg]et_numeric_value() - Default: 8

Usage & Invocation - OCSP

- GSK_OCSP_CLIENT_CACHE_SIZE [0 – 32000] – Specifies the maximum number of OCSP responses or cached certificate statuses to be kept in the OCSP response cache
  - gsk_attribute_[sg]et_numeric_value() - Default: 256
- GSK_OCSP_CLIENT_CACHE_ENTRY_MAXSIZE [0 – 32000] - Specifies the maximum number of OCSP responses or cached certificate statuses that are allowed to be kept in the OCSP response cache for an issuing CA certificate
  - gsk_attribute_[sg]et_numeric_value() - Default: 0
- GSK_OCSP_MAX_RESPONSE_SIZE [0 – 2147483647] – Specifies the maximum size in bytes that is accepted as a response from an OCSP responder.
  - gsk_attribute_[sg]et_numeric_value() - Default: 20480 (20K)
- GSK_OCSP_RESPONSE_TIMEOUT [0 – 43200] – Specifies the time in seconds to wait for a response from the OCSP responder
  - gsk_attribute_[sg]et_numeric_value() - Default: 15

Usage & Invocation – HTTP CRL

- New HTTP CRL related environment variables and attribute types:
  - GSK_HTTP_CDP_ENABLE [ON | OFF]
  - GSK_HTTP_CDP_CACHE_SIZE [0 – 32000]
  - GSK_HTTP_CDP_CACHE_ENTRY_MAXSIZE [0 – 2147483647]
  - GSK_HTTP_CDP_PROXY_SERVER_NAME <*serverName*>
  - GSK_HTTP_CDP_PROXY_SERVER_PORT [1 – 65535]
  - GSK_HTTP_CDP_MAX_RESPONSE_SIZE [0 – 2147483647]
  - GSK_HTTP_CDP_RESPONSE_TIMEOUT [0 – 43200]

Usage & Invocation - HTTP CRL

- GSK_HTTP_CDP_ENABLE [ON | OFF] – Specifies if certificate revocation checking with the HTTP URI values in the CDP extension is enabled.
  - gsk_attribute_[sg]et_enum()
    - GSK_HTTP_CDP_ENABLE_ON
    - GSK_HTTP_CDP_ENABLE_OFF: Default
- GSK_HTTP_CDP_CACHE_SIZE [0 – 32000] - Specifies the maximum number of CRLs that are allowed to be stored in the HTTP CDP CRL cache.
  - gsk_attribute_[sg]et_numeric_value() - Default: 32
- GSK_HTTP_CDP_CACHE_ENTRY_MAXSIZE [0 – 2147483647] – Specifies the maximum size in bytes of a CRL that is allowed to be stored in the HTTP CDP CRL cache.
  - gsk_attribute_[sg]et_numeric_value() - Default: 0

Usage & Invocation - HTTP CRL

- GSK_HTTP_CDP_PROXY_SERVER_NAME <*serverName*> - Specifies the DNS name or IP address of the HTTP proxy server for HTTP CDP CRL retrieval
  - gsk_attribute_[sg]et_buffer() - Default: NULL
- GSK_HTTP_CDP_PROXY_SERVER_PORT [1 – 65535] – Specifies the HTTP proxy server port for HTTP CDP CRL retrieval
  - gsk_attribute_[sg]et_numeric_value() - Default: 80
- GSK_HTTP_CDP_MAX_RESPONSE_SIZE [0 – 2147483647] – Specifies the maximum size in bytes accepted as a response from an HTTP server when retrieving a CRL
  - gsk_attribute_[sg]et_numeric_value() - Default: 20480 (20K)
- GSK_HTTP_CDP_RESPONSE_TIMEOUT [0 – 43200] – Specifies the time in seconds to wait for a response from an HTTP server
  - gsk_attribute_[sg]et_numeric_value() - Default: 15

Usage & Invocation – LDAP CRL

- System SSL supports LDAP basic and extended CRL caching support
- GSK_CRL_CACHE_EXTENDED [ON | OFF] – Specifies if LDAP basic or extended CRL cache support is enabled
  - gsk_attribute_[sg]et_enum()
    - GSK_CRL_CACHE_EXTENDED_ON
    - GSK_CRL_CACHE_EXTENDED_OFF: Default - Basic
- LDAP basic CRL caching support (Existing support)
  - CRLs are only cached when GSK_CRL_CACHE_TIMEOUT is greater than 0 and GSK_CRL_CACHE_SIZE is set to a non-zero number
  - Cache size defaults to -1 (unlimited)
  - Temporary CRLs are added to cache if not found on LDAP server
  - LDAP server response time out defaults to 15 seconds

Usage & Invocation - LDAP CRL

- LDAP extended CRL caching support
  - CRLs are only cached when they contain an expiration time greater than the current time
  - Cache size defaults to 32
  - Temporary CRLs are not added to the cache by default if not found on the LDAP server
  - LDAP server response time out defaults to 15 seconds
    - Difference: Time out is honored in System SSL in case LDAP server does not honor the timeout value.
- GSK_CRL_CACHE_SIZE [-1 – 32000]: Specifies the maximum number of CRLs that are allowed to be stored in the LDAP CRL cache
  - gsk_attribute_[sg]et_numeric_value()
    - Basic: Default: -1 (unlimited)
    - Extended: Default: 32

Usage & Invocation - LDAP CRL

- GSK_CRL_CACHE_TEMP_CRL [ON | OFF]: Specifies if a temporary LDAP CRL cache entry is added to the cache if the CRL does not reside on the LDAP server
  - gsk_attribute_[sg]et_enum()
    - GSK_CRL_CACHE_TEMP_CRL_ON: Basic default
    - GSK_CRL_CACHE_TEMP_CRL_OFF: Extended default
- GSK_CRL_CACHE_TEMP_CRL_TIMEOUT [1 – 720]: Specifies the time in hours that a temporary LDAP CRL cache entry resides in the LDAP extended CRL cache
  - gsk_attribute_[sg]et_numeric_value() - Default: 24
- GSK_CRL_CACHE_ENTRY_MAXSIZE [0 – 2147483647]: Specifies the maximum size in bytes of a CRL to be kept in the LDAP CRL cache
  - gsk_attribute_[sg]et_numeric_value() - Default: 0 (unlimited size)

Usage & Invocation - LDAP CRL

- GSK_LDAP_RESPONSE_TIMEOUT [0 – 43200]: Specifies the timeout in seconds to wait for a response from the LDAP server
  - gsk_attribute_[sg]et_numeric_value(): Default 15

Usage & Invocation - Revocation checking order

- System SSL can be configured to adjust the order configured revocation sources (OCSP, HTTP CRLs, and LDAP CRLs) are checked when validating the SSL/TLS partner certificate
- GSK_OCSP_URL_PRIORITY [ON | OFF]: Specifies the priority order for contacting OCSP responder locations if both GSK_OCSP_URL and GSK_OCSP_ENABLE are active
  - gsk_attribute_[sg]et_enum()
    - GSK_OCSP_URL_PRIORITY_ON: Default
    - GSK_OCSP_URL_PRIORITY_OFF
- GSK_AIA_CDP_PRIORITY [ON | OFF]: Specifies the priority order that the AIA and the CDP extensions are checked for certificate revocation information (Used to order OCSP and HTTP CRL checking)
  - gsk_attribute_[sg]et_enum()
    - GSK_AIA_CDP_PRIORITY_ON: Default
    - GSK_AIA_CDP_PRIORITY_OFF

Usage & Invocation - Revocation security enforcement

- GSK_REVOCATION_SECURITY_LEVEL [LOW | MEDIUM | HIGH]: Specifies the level of security when contacting an OCSP responder or an HTTP server in the CDP extension
  - gsk_attribute_[sg]et_enum_value()
    - GSKCMS_REVOCATION_SECURITY_LEVEL_LOW: Certificate validation does not fail if the OCSP responder or HTTP server in the CDP extension cannot be reached.
    - GSKCMS_REVOCATION_SECURITY_LEVEL_MEDIUM: Certificate validation requires the OCSP responder or HTTP server in the CDP extension to be contactable. Default setting.
    - GSKCMS_REVOCATION_SECURITY_LEVEL_HIGH: Certificate validation requires the OCSP responder or HTTP server in the CDP extension to be contactable and provide valid revocation information. The AIA and CDP extensions must contain valid HTTP URI values that can be contacted.

Usage & Invocation – Limiting the number of OCSP and HTTP URLs contacted

- GSK_MAX_SOURCE_REV_EXT_LOC_VALUES [0 - 256]: Specifies the maximum number of location values that are contacted per revocation source when attempting validation of a certificate.
  - Revocation source = An AIA or CDP extension in a certificate
  - Default: 10 locations
    - Contact up to 10 URI values in a specific data source in a certificate
- GSK_MAX_VALIDATION_REV_EXT_LOC_VALUES [0 - 1024]: Specifies the maximum number of location values that are contacted when performing validation of a certificate.
  - Default: 100 locations
    - Contact up to 100 URI values in all AIA and CDP extensions in a certificate

Usage & Invocation – Updated Certificate Management Services routines

- gsk_validate_certificate_mode()
  - gsk_status gsk_validate_certificate_mode (
    gskdb_data_sources * *data_sources*,
    x509_certificate * *subject_certificate*,
    gsk_boolean *accept_root*,
    gsk_int32 * *issuer_record_id*,
    GSKCMS_CERT_VALIDATION_MODE *validation_mode*,
    gsk_uint32 *arg_count*
    [,**GSKCMS_CERT_VALIDATE_KEYRING_ROOT** *validate_root*]
    [,**GSKCMS_REVOCATION_SECURITY_LEVEL** *security_level*]
    [,**gsk_int32** *max_source_rev_ext_loc_values*]
    [,**gsk_int32** *max_validation_rev_ext_loc_values*]…)
- data_sources – Can now specify OCSP, CDP, and LDAP extended revocation handles returned from gsk_create_revocation_source()
- arg_count – Can now be set to 0, 1, 2, 3, or 4 for the number of optional parameters
- security_level (new parameter)– revocation security level for CDP and OCSP data sources

Usage & Invocation – Updated Certificate Management Services routines

- max_source_rev_ext_loc_values (new parameter) – Specifies the maximum number of locations that will be contacted per data source when attempting validation of a certificate.
- max_validate_rev_ext_loc_values (new parameter) - Specifies the maximum number of HTTP URI values that will be contacted when performing validation of a certificate chain.

Usage & Invocation – New Certificate Management Services routines

- gsk_status gsk_create_revocation_source (
  gskdb_source * source,
  gsk_handle * revocation_source)
  - source (input): Specifies the parameters needed for the revocation data source handle to be created
  - revocation_source (output): Returns the revocation data source handle

Usage & Invocation – New Certificate Management Services routines

- void gsk_free_revocation_source (
  gsk_handle * revocation_handle)
  - revocation_handle (input): Specifies a revocation source handle to be freed

Usage & Invocation – New Certificate Management Services routines

- gsk_status gsk_set_directory_numeric_value (
  gsk_handle directory_handle,
  GSKCMS_DIRECTORY_NUM_ID num_id,
  int num_value)
- gsk_status gsk_get_directory_numeric_value (
  gsk_handle directory_handle,
  GSKCMS_DIRECTORY_NUM_ID num_id,
  int * num_value)
- Routines set and get the following for LDAP basic CRL support:
  - GSKCMS_CRL_CACHE_SIZE
  - GSKCMS_CRL_CACHE_ENTRY_MAXSIZE
  - GSKCMS_LDAP_RESPONSE_TIMEOUT

Usage & Invocation – Example configurations

- Example 1: Configure System SSL to do certificate validation using revocation information provided through the AIA and CDP extensions within the certificate.
  - The AIA contains any OCSP responders to be used and the CDP contains any HTTP servers to be used.
  - The OCSP responders within the AIA extension are checked first. If the OCSP responders cannot be contacted, the HTTP servers within the CDP extension are used.
  - If the OCSP responders and HTTP servers cannot be contacted, the handshake fails.

```
GSK_OCSP_ENABLE=ON
GSK_HTTP_CDP_ENABLE=ON
GSK_AIA_CDP_PRIORITY=ON
GSK_REVOCATION_SECURITY_LEVEL=MEDIUM
```

Usage & Invocation – Example configurations

- Example 2: Certificate validation uses revocation information provided through the dedicated OCSP responder and the AIA and CDP extensions within the certificate. The revocation providers are checked in the following order:
  - HTTP servers within the CDP extensions.
  - OCSP responders in the AIA extensions.
  - Dedicated OCSP responder.

If none of the OCSP responders or HTTP servers can be contacted, certificate validation fails.

```
GSK_OCSP_URL=http://999.999.999.999
GSK_OCSP_ENABLE=ON
GSK_OCSP_URL_PRIORITY=OFF
GSK_HTTP_CDP_ENABLE=ON
GSK_AIA_CDP_PRIORITY=OFF
GSK_REVOCATION_SECURITY_LEVEL=MEDIUM
```

Overview: PKCS #12 – Certificate Store

- Problem Statement / Need Addressed
  - Need the ability to use a PKCS#12 V3 file for an SSL/TLS environment
- Solution
  - Provide the ability to use a PKCS#12 V3 file as the Certificate/key store for a SSL/TLS environment
  - Available in z/OS V1R13 and z/OS V2R1 in APAR OA45216
    - V1R13 PTFs: UA74152, UA74369, and UA74275
    - V2R1 PTFs: UA74370, UA74371, and UA74564
- Benefit / Value
  - Allows for broader certificate store capability to support user friendly conversion of applications to System SSL from other SSL implementations (ie. openSSL)
  - Allow direct usage of PKCS #12 file certificates/keys

Usage & Invocation: PKCS #12 Certificate Store

- What is PKCS #12?
  - This standard describes a transfer syntax for personal identity information, including private keys, certificates, miscellaneous secrets, and extensions.
- Where do PKCS #12 (p12) files come from?
  - System SSL and RACF can create a single certificate chain p12 file. For example, when gskkyman performs an export to binary Version 3 file, the result is a p12 file.
  - Other providers such as OpenSSL can create multiple certificate chains in a single p12 file.
- How are these p12 files protected?
  - They can be protected with a certificate or a password. System SSL only supports password protection. Integrity of the file is ensured through a SHA-1 message authentication (MAC).

Usage & Invocation: PKCS #12 Certificate Store

- What are the contents of a PKCS #12 file?
  - Each object within the file is known as a bag
  - System SSL recognizes bags containing x.509 certificates, PKCS#8 encrypted private keys and clear private keys.
  - All other bags are ignored.

- What PKCS #12 file formats are supported?
  - Although System SSL supports both BINARY and Base64 files, the file used for SSL/TLS environments must be BINARY

Usage & Invocation: PKCS #12 Certificate Store

- Certificate/key store support is specified through two existing environment attributes:
  - GSK_KEYRING_FILE – Now supports specifying the PKCS #12 file name
  - GSK_KEYRING_PW – Now supports specifying the PKCS #12 file's password
  - These attributes can be set via USS environment variables or directly in the System SSL application with gsk_attribute_set_buffer()
- System SSL code will handle reading in the certificates contained in the PKCS#12 file while initializing the SSL environment
  - Note: System SSL is not providing the ability to add or modify the certificates contained in a PKCS#12 file. Support is read-only.

Usage & Invocation: PKCS #12 Certificate Store

- gskkyman key database files and SAF key rings have the notion of a label. Each certificate represented has a unique label.
- PKCS #12 files have the notion of an optional friendly name.
- When processing the PKCS #12 file, the friendly name is used as the certificate label. If no friendly name, the certificate's subject DN is used as the label. Label is truncated at 127 characters.
- PKCS #12 files do not have the notion of a default certificate. SSL/TLS applications must specify the certificate label to be used for the secure connection.

Usage & Invocation: PKCS #12 Certificate Store

- System SSL utility gskkyman utility has been modified:
  - To display the contents of a PKCS #12 file using the command line display certificate or display certificate verbose options (-dc or -dcv)
  - New option -p12 is used to pass in the PKCS #12 file name
  - Still prompted for the file password as before

Usage & Invocation: PKCS #12 Certificate Store

```
> gskkyman -?
gskkyman
gskkyman -dc|-dcv [-k filename|-t tokenname|-p12 filename] [-l label]
gskkyman -dk [-k filename]
...

Functions
  -dc Display certificate details
  -dcv Display certificate verbose details
  ...
Options
  ...
  -p Import/export file
  -p12 PKCS #12 file
  ...
```

Usage & Invocation: PKCS #12 Certificate Store

```
> gskkyman -dc -p12 twochains.p12

Enter database password (press ENTER to cancel):
Label:
        <server certificate>
Trusted:
        Yes
Version:
        3
…
Private key:
         Yes
Default key:
         No
Certificate extensions:
         4
```

Presentation Summary

- You should now be able to:
  - Understand the recent changes in System SSL (OCSP and PKCS #12)
  - Be able to find any of the above information in the relevant publication(s)

Appendix

- Publications
  - *z/OS Cryptographic Services System Secure Sockets Layer* (SC14-7495)
- Specifications
  - RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile
  - RFC 2560 – X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
  - RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
  - RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Appendix additional notes: Usage & Invocation – New structures to use with gsk_create_revocation_source()

- New gskdb_source structure defined in gskcms.h

```
typedef struct _gskdb_source {
 gskdb_source_type            type;
 gsk_octet                    rsvd_1[2];
 union {
     gskdb_ocsp_source            ocspSource;
     gskdb_cdp_source             cdpSource;
     gskdb_extended_directory_source directorySource;
     gsk_octet                    rsvd[16];
 } u;
} gskdb_source;
```

Appendix additional notes: Usage & Invocation – New structures to use with gsk_create_revocation_source()

- New gskdb_ocsp_source structure defined in gskcms.h:

```
typedef struct _gskdb_ocsp_source {
    gsk_boolean                 ocspEnable;
    gsk_boolean                 ocspURLPriority;
    char *                      ocspURL;
    char *                      ocspProxyServerName;
    int                         ocspProxyServerPort;
    int                         ocspResponseTimeout;
    int                         ocspMaxResponseSize;
    int                         ocspCacheSize;
    int                         ocspCacheEntryMaxSize;
    int                         ocspNonceSize;
    gsk_handle *                ocspDbHandle;
    char *                      ocspReqLabel;
    x509_algorithm_type         ocspReqSignatureAlgorithm;
    gsk_boolean                 ocspGenerateNonce;
    gsk_boolean                 ocspCheckNonce;
    gsk_boolean                 ocspUseGetMethod;
    gsk_octet                   rsvd[40];
} gskdb_ocsp_source;
```

Appendix additional notes: Usage & Invocation – New structures to use with gsk_create_revocation_source()

- New gsk_cdp_source structure and cdpEnableFlags settings in gskcms.h:

```
typedef struct _gskdb_cdp_source {
   gsk_uint32                  cdpEnableFlags;
   int                         httpCdpCacheEntryMaxSize;
   int                         httpCdpCacheSize;
   char *                      httpCdpProxyServerName;
   int                         httpCdpProxyServerPort;
   int                         httpCdpMaxResponseSize;
   int                         httpCdpResponseTimeout;
   gsk_octet                   rsvd[40];
} gskdb_cdp_source;

    /*
     *  cdpEnableFlags settings
     */
    #define GSKCMS_CDP_ENABLE_NONE  0x00000000u     /* No CDP support    */
    #define GSKCMS_CDP_ENABLE_HTTP  0x00000001u     /* HTTP CDP support  */
    #define GSKCMS_CDP_ENABLE_ANY   0xffffffffu     /* All CDP support   */
```

Appendix additional notes: Usage & Invocation – New structures to use with gsk_create_revocation_source()

- New gskdb_extended_directory_source structure defined in gskcms.h:

```
typedef struct _gskdb_extended_directory_source {
    int                          crlCacheEntryMaxSize;
    int                          crlCacheSize;
    gsk_boolean                  crlCacheTempCRL;
    int                          crlCacheTempCRLTimeout;
    GSKCMS_DIRECTORY_ENUM_VALUE crlSecurityLevel;
    char *                       ldapPassword;
    int                          ldapPort;
    int                          ldapResponseTimeout;
    char *                       ldapServerName;
    char *                       ldapUser;
    gsk_octet                    rsvd[40];
} gskdb_extended_directory_source;
```