IBM Software Group

IBM WebSphere Technical Conference

Featuring WebSphere, WebSphere Portal, WebSphere BI, WebSphere MQ and CICS – Nov 29th – December 3rd 2004 - Munich

C103TS Taking CICS Web Security to the next level

Peter Havercan
peter_havercan@uk.ibm.com

WebSphere software

e business on demand software

Taking CICS Web Security to the next level - Notes

This presentation will describe the capabilities provided by the security enhancements in CICS Transaction Server 3.1, with particular emphasis on the facilities that are used by CICS Web Support.

Acknowledgements

Notes

This page intentionally left blank.

Session Agenda

- **Support for Transport Layer Security (TLS)**
- **Cipher suites**
  - Support for AES cipher suites
  - Specification of minimum and maximum encryption level
- **Performance enhancements**
  - SSL caching support
  - Support for increased number of secure connections
- **Changes to revocation processing**
  - Certificate revocation lists
  - EXEC CICS VERIFY processing
- **Support for mixed case passwords**

Session Agenda - Notes

CICS TS 3.1 is implementing support for the Transport Layer Security (TLS) 1.0. This new protocol, based on Secure Sockets Layer (SSL) 3.0 is provided by the System SSL component of z/OS.

CICS TS 3.1 will now support the 128-bit and 256-bit Advanced Encryption Standard cipher suites. CICS will also allow you to specify a range of cipher suites on the TCPIPSERVICE, CORBASERVER and URIMAP resource definitions. CICS will only negotiate a session with a partner that supports the selected cipher suites.

CICS TS 3.1 has made a number of changes to provide for an increased number of SSL connections and to reduced the performance cost of re-using an SSL connection. CICS will now allow SSL session IDs to be shared across a sysplex. CICS has also restructured SSL processing to exploit the Open Transaction Environment (OTE) with its S8 TCBs.

CICS has a new utility transaction, CCRL, which can be invoked from a terminal or started, which will download a certificate authority's revocation lists into a local LDAP server for use by PKI processing.

CICS TS 3.1 has made changes to the security verification process. In prior releases, CICS did not check the revoked status for a user when issuing an EXEC CICS VERIFY or with ATTACHSEC(VERIFY). In this release, CICS will check the revoked status of the user and not allow the request to proceed if the user is in revoked status. CICS will also check to see if the users connection to a group is revoked.

CICS TS 3.1 will support passwords with mixed case.

CICS support for Transport Layer Security

- **TLS is the latest version of the Secure Sockets Layer protocol**
  - Specification documented in RFC 2246
- **z/OS 1.4 System SSL incorporates:**
  - SSL 2.0
  - SSL 3.0
  - TLS 1.0

CICS support for Transport Layer Security - Notes

CICS TS 3.1 provides support for the Transport Layer Security (TLS) 1.0. This new protocol, based on Secure Sockets Layer (SSL) 3.0 is provided on the z/OS platform by the System SSL component.

Cipher Suites

- **Support for AES cipher suites**
  - 128-bit and 256-bit encryption
- **Specification of cipher suites to be used for encryption**
  - Allows for a minimum and maximum level of encryption
    - If partner doesn't support the selected choices no connection will be established
    - Specified on:
      - TCPIPSERVICE for inbound HTTP and IIOP requests
      - CORBASERVER for outbound IIOP requests
      - URIMAP for outbound HTTP requests

Cipher Suites - Notes

CICS TS 3.1 will now support the 128-bit and 256- bit Advanced Encryption Standard cipher suites.

CICS will also allow you to specify a range of cipher suites on the TCPIPSERVICE (for inbound requests), CORBASERVER (for outbound IIOP) and URIMAP (for outbound HTTP) resource definitions. CIPHERS can also be specified on the new EXEC WEB OPEN command for outbound HTTP connections.

CICS will only negotiate a session with a partner that supports at least one of the selected cipher suites.

Cipher Suites…

- **Range of available cipher suites for CICS to use is specified in the SIT**
  - ENCRYPTION={STRONG | MEDIUM | WEAK}
    - For compatibility
      - ENCRYPTION=NORMAL will be treated as ENCRYPTION=MEDIUM (but is no longer the default)
- **Selection of cipher suites and order of preference**
  - Specified in CIPHERS attribute
    - Two-digit hexadecimal codes indicate cipher suites
    - Order determines preference
      - e.g. CIPHERS(352F0A0504)
    - Replaces PRIVACY parameter

Cipher Suites - Notes

The default range of cipher suites available to CICS to use when negotiating a session is specified in the Systems Initialization Table (SIT) by the ENCRYPTION parameter.

The default has changed in CICS TS 3.1 from ENCRYPTION=NORMAL to ENCRYPTION=STRONG.

ENCRYPTION=MEDIUM has replaced ENCRYPTION=NORMAL. To maintain compatibility with prior releases a specification of ENCRYPTION=NORMAL will be treated as ENCRYPTION=MEDIUM. The actual ranges of cipher suites belonging to each level are listed on the following pages.

The actual selection of the cipher suites to be used is specified on the resource definitions: TCPIPSERVICE, CORBASERVER and URIMAP. The CIPHERS parameter is a set of two-digit hexadecimal codes identifying the specific cipher suites. The codes are the same as those specified in the TLS specification. The order in which the codes are listed in the CIPHERS parameter indicates your preference.

The CIPHERS parameter will replace the PRIVACY parameter. The PRIVACY parameter will still be shown on the RDO panels, but it will not be possible to modify it except by changing the CIPHERS list. INQURE TCPIPSERVICE PRIVACY will still function.

Cipher Suites…

STRONG
Specifies that CICS should use only the following cipher suites:

Cipher suite	Encryption algorithm	Key length	MAC algorithm
01	No encryption		MD5
02	No encryption		SHA
03	RC4	40 bits	MD5
04	RC4	128 bits	MD5
05	RC4	128 bits	SHA
06	RC2	40 bits	MD5
09	DES	56 bits	SHA
0A	Triple DES	168 bits	SHA
2F	AES	128 bits	SHA
35	AES	256 bits	SHA

The terms used in this table are:

MD5 Message Digest algorithm

SHA Secure Hash algorithm

RC2, RC4
Rivest encryption

DES Data Encryption Standard

Triple DES
DES applied three times

AES Advanced Encryption Standard

Cipher Suites - Notes

These are the available cipher suites for use by CICS when ENCRYPTION=STRONG is specified in the SIT.

Cipher suite 00 is available for ENCRYPTION STRONG, MEDIUM and WEAK. This cipher suite indicates no encryption and no MAC algorithm. This is supported by the protocol, but is **not recommended**.

Cipher Suites…

MEDIUM
Specifies that CICS should use only the following cipher suites:

Cipher suite	Encryption algorithm	Key length	MAC algorithm
01	No encryption		MD5
02	No encryption		SHA
03	RC4	40 bits	MD5
06	RC2	40 bits	MD5
09	DES	56 bits	SHA

The terms used in this table are:

MD5 Message Digest algorithm

SHA Secure Hash algorithm

RC2, RC4
Rivest encryption

DES Data Encryption Standard

Cipher Suites - Notes

These are the available cipher suites for use by CICS when ENCRYPTION=MEDIUM or NORMAL is specified in the SIT.

Cipher Suites…

WEAK
Specifies that CICS should use only the following cipher suites:

Cipher suite	Encryption algorithm	Key length	MAC algorithm
01	No encryption		MD5
02	No encryption		SHA
03	RC4	40 bits	MD5
06	RC2	40 bits	MD5

The terms used in this table are:

MD5 Message Digest algorithm

SHA Secure Hash algorithm

RC2, RC4
Rivest encryption

Cipher Suites - Notes

These are the available cipher suites for use by CICS when ENCRYPTION=WEAK is specified in the SIT.

Performance Enhancements

- **CICS support for SSL caching**
  - Allows session ID information to be shared across the sysplex
- **OTE exploitation by CICS SSL connection management**
  - New SP mode TCB
    - Reduces system storage requirements
  - Existing S8 TCBs
    - Now only allocated for the duration of the SSL requests
    - Provides for increased number of simultaneous SSL sessions

Performance Enhancements - Notes

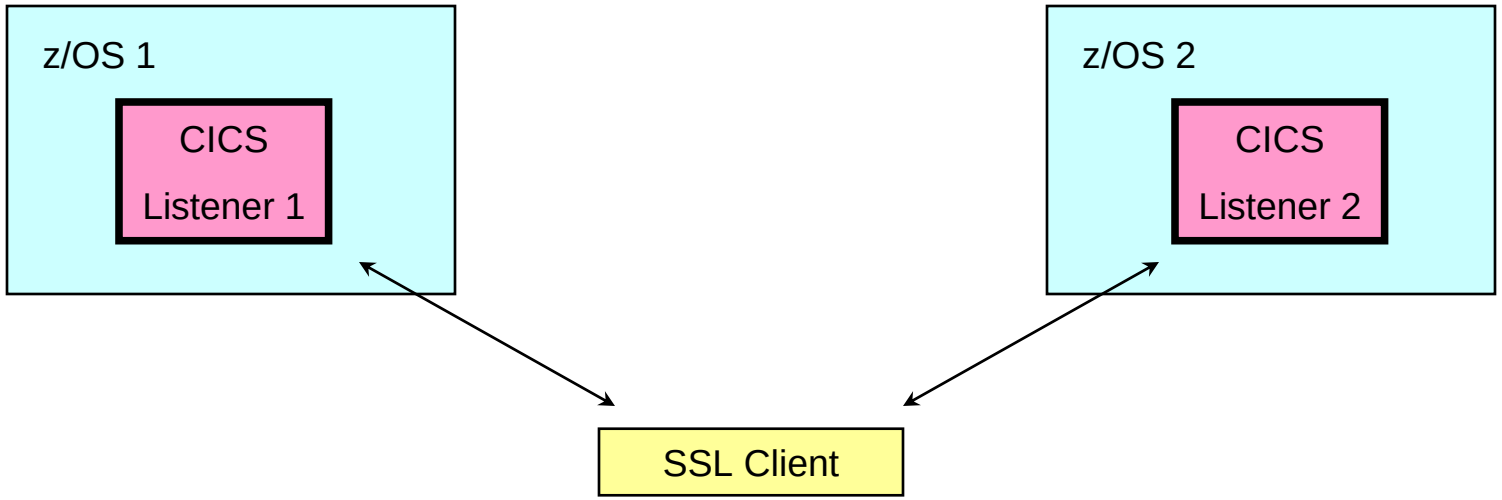
CICS has made a number of performance enhancements to its SSL processing to improve the performance of establishing a connection and to support greater numbers of SSL connections.

You can specify whether you want to share session IDs across a sysplex by using the SSL cache. CICS will perform a partial SSL handshake if the client has negotiated with CICS previously. If the cache is shared across a number of CICS regions, this will improve the performance of SSL negotiation and connection throughput.

CICS uses the open transaction environment (OTE) to manage SSL connections. There is a new open TCB mode called SP, that is used for socket pthread owning tasks. Each SSL connection uses an S8 TCB, which is allocated from the SSL pool. The S8 TCBs run as UNIX pthreads. This allows many more simultaneous SSL connections in CICS than the limit of 256 in previous releases.

Performance Enhancements

- **SSL Sysplex Caching**
  - Today the SSL session id is cached local to every CICS region
    - If the same client connects to a different CICS region a full SSL handshake is required
      - Impacts cloned CICS listener regions



Performance Enhancements - Notes

In today's CICS SSL implementation, a client who successfully connects to one CICS regions and then connects to another CICS region will be required to go through a full SSL handshake in both cases. This is because the SSL cache is local to a CICS address space.

Performance Enhancements

- **SSL Sysplex Caching…**
  - Makes server session information across a sysplex
    - Requires all systems in the sysplex to use the same ESM
    - Requires SSL Started Task (GSKSRVR) to be implemented
      - Supports TLS 1.0 and SSL 3.0 protocols
      - GSKSRVR Environment Variables
        - > GSK_LOCAL_THREADS: number of threads
        - > GSK_SIDCACHE_SIZE: sysplex session cache size in megabytes
        - > GSK_SIDCACHE_TIMEOUT: session cache entry timeout in minutes
    - Enable CICS to use sysplex caching
      - SIT parameter
        - > SSLCACHE={CICS | SYSPLEX }

Performance Enhancements - Notes

The sysplex session cache support makes SSL server session information available across the sysplex. An SSL session established with a server on one system in the sysplex can be resumed using a server on another system in the sysplex as long as the SSL client presents the session identifier obtained for the first session when initiating the second session. SSL V3 and TLS V1 server session information can be stored in the sysplex session cache while SSL V2 server session information and all client session information is stored only in the SSL cache for the application process.

The SSL started task (GSKSRVR) provides sysplex session cache support.

In order to use the sysplex session cache, each system in the sysplex must be using the same external security manager (for example, z/OS Security Server RACF) and a userid on one system in the sysplex must represent the same user on all other systems in the sysplex (that is, userid ZED on System A has the same access rights as userid ZED on System B). The external security manager must support the RACROUTE REQUEST=EXTRACT,TYPE=ENVRXTR and RACROUTE REQUEST=FASTAUTH functions.

SSLCACHE={CICS| SYSPLEX} Specifies whether SSL is to use the local or sysplex caching of session ids. Sysplex caching is only allowed if multiple CICS socket-owning regions accept SSL connections at the same IP address.

SSL Open Transaction Environment Exploitation

- **Current SSL implementation**
  - Uses a separate S8 TCB for each SSL requests
    - Fixed pool size
      - Specified by SSLTCBS
    - Each TCB has its own LE enclave
    - S8 TCB is assigned for the duration of the requesting task

SSL Open Transaction Environment Exploitation - Notes

The current CICS implementation for SSL uses a fixed pool of S8 TCBs to hand requests. The pool size is specified by the SIT parameter SSLTCBs. The maximum number of SSL TCBs is 255 per CICS address space.

Each S8 TCB has its own LE enclave and the TCB is assigned for the duration of the requesting task.

SSL Open Transaction Environnent Exploitation…

- **OTE implementation**
  - SP TCB
    - Created when KEYRING is specified in the SIT
    - Owns the LE enclave and SSL cache
  - S8 TCBs
    - Variable pool size
      - Controlled by MAXSSLTCBS parameter
    - Runs as a UNIX pthread
    - Assigned for the duration of the request

SSL Open Transaction Environment Exploitation - Notes

CICS 3.1 uses the open transaction environment (OTE) to manage SSL connections.

There is a new open TCB mode called SP, that is used for socket pthread owning tasks. The SSL pool is managed by the one SP TCB that runs in the CICS region. The SP TCB and subsequent SSL pool will only be created if the KEYRING parameter is present in the SIT.

Each SSL connection uses an S8 TCB, which is allocated from the SSL pool. The S8 TCBs run as UNIX pthreads. This allows many more simultaneous SSL connections in CICS than the limit of 256 in previous releases. MAXSSLTCBS has a limit of 1024 TCBs. All of the S8 TCBs run within a single enclave, which also contains the SP TCB and the SSL cache.

S8 TCBs are now only locked to a transaction for the period that it needs to perform SSL functions. After the SSL negotiation is complete, the TCB is released back into the SSL pool to be reused.

Certificate Revocation Lists

- **Digital Certificates**
  - Are used in the process of validating signed data or securely transmitting encryption keys
  - Have a limited lifetime
    - Specified in the certificate's contents
    - Can be explicitly revoked

Certificate Revocation Lists - Notes

To make an environment secure, you must be sure that any communication is with "trusted" sites whose identity you can be sure of. SSL uses certificates for authentication -- these are digitally signed documents which bind the public key to the identity of the private key owner. Authentication happens at connection time, and is independent of the application or the application protocol. Authentication involves making sure that sites with which you communicate are who they claim to be. With SSL, authentication is performed by an exchange of certificates, which are blocks of data in a format described in ITU-T standard X.509. The X.509 certificates are issued, and digitally signed by an external authority known as a certificate authority.

Certificates have a limited lifetime when issued. A certificate can also be revoked by the issuing authority.

Certificate Revocation Lists

- **Digital Certificates…**
  - General certificate validation flow is as follows:
    - The recipient of signed data verifies that the claimed identity of the user is in accordance with the identity contained in the certificate
    - The recipient validates that no certificate in the path is revoked and that all certificates are within their validity periods
    - The recipient verifies that the data has not been altered since signing, by using the public key in the certificate

Certificate Revocation Lists - Notes

There is a need to validate the certificate received from a partner. This is part of the connection process in the SSL handshake.

The SSL handshake is an exchange of information that takes place between the client and the server when a connection is established. It is during the handshake that client and server negotiate the encryption algorithms that they will use, and authenticate one another. The main features of the SSL handshake are:

The client and server exchange information about the SSL version number and the cipher suites that they both support.

The server sends its certificate and other information to the client. Some of the information is encrypted with the server's private key. If the client can successfully decrypt the information with the server's public key, it is assured of the server's identity.

If client authentication is required, the client sends its certificate and other information to the server. Some of the information is encrypted with the client's private key. If the server can successfully decrypt the information with the client's public key, it is assured of the client's identity.

The client and server exchange random information which each generates and which is used to establish session keys: these are symmetric keys which are used to encrypt and decrypt information during the SSL session. The keys are also used to verify the integrity of the data.

Certificate Revocation Lists

- **A Certificate Revocation List (CRL) is a file that lists all invalid and revoked certificates for a specific Certificate Authority (CA)**
- **CAs periodically update their CRLs and make them available for others to publish in local Lightweight Directory Access Protocol (LDAP) directories**
  - Available for download
  - Retrieved information stored in an LDAP server
    - Refer to z/OS 1.5 Cryptographic Services PKI Guide and Reference

Certificate Revocation Lists - Notes

In order that one system can be assured that a certificate received from another system is genuine, a trusted third party that can vouch for the certificate is needed.

Certificate authorities are independent bodies who act as the trusted third parties, by issuing certificates for use by others. Before issuing a certificate, a certificate authority will examine the credentials of the person or organization that has requested the certificate. When the certificate has been issued, information about it is held on a publicly accessible repository. Users can consult the repository to check the status and validity of any certificates received.

Certificate authorities will periodically create and publish Certificate Revocation Lists (CRLs). The CRLs can be downloaded and used as part of the certificate validation process. The downloaded information can be stored locally in an LDAP server and is used by z/OS Public Key Infrastructure services.

Certificate Revocation Lists

- **CICS provides a utility transaction to download CRLs**
  - CCRL transaction
    - Can be invoked from a terminal: CCRL *url-list*
      - e.g. **CCRL**
        http://crl.verisign.com/ATTClass1Individual.crl
        http://crl.geotrust.com/crls/secureca.crl
    - Can be invoked as a started task:
      - **EXEC CICS START TRANSID(CCRL)**
        FROM('http://crl.verisign.com/ATTClass1Individual.crl
        http://crl.geotrust.com/crls/secureca.crl')
        LENGTH(89) INTERVAL(960000)
  - New SIT parameter
    - CRLSERVER
      - Specifies name of the LDAP server where the certificate revocation list should be stored

Certificate Revocation Lists - Notes

Certificate revocation lists are available from certificate authorities such as Verisign, Geotrust, and Equifax. They are kept in CRL repositories that are available on the world wide web and can be downloaded and stored in the LDAP server.

To populate the LDAP server and update certificate revocation lists, use the CICS-supplied transaction CCRL. You can run the CCRL transaction from a terminal or using a START command. Use the START command to schedule regular updates.

From a terminal, enter CCRL *url-list* where *url-list* is a space-delimited list of URLS that specify the locations of the certificate revocation lists that you want to download.

To use a START command, enter EXEC CICS START TRANSID(CCRL) FROM (*url-list*) LENGTH (*url-list-length*) [INTERVAL(*hhmmss*)|TIME(*hhmmss*)] where *url-list* is a space-delimited list of URLs from where certificate revocation lists can be downloaded, *url-list-length* is the length of the URL list, and *hhmmss* is the interval or expiration time at which the CCRL transaction is to be scheduled.

There is a new SIT parameter, CRLSERVER, which specifies the TCP/IP address and port number of the LDAP server into which the CRL is to be loaded. This is used by the CCRL transaction and is also used by System SSL when validating certificates.

Changes to Revocation Processing

- **Current releases of CICS**
  - Do not check the revoked status of a USERID for:
    - EXEC CICS VERIFY
    - ATTACHSEC(VERIFY)
    - START with USERID
  - Do not check if a connection to a GROUP was revoked
- **Revoked status of a user ID or a user's group connection now honored by CICS 3.1**

Changes to Revocation Processing - Notes

The current implementations of ATTACHSEC(VERIFY), EXEC CICS VERIFY PASSWORD and EXEC CICS START TRANSID() USERID() do not check the revoked status of the USERID being verified. After the USERID and password have been verified by either of these techniques, CICS allows the user to reuse a security environment that had been built earlier and represented by a previously created ACEE. If the USERID has been revoked since that security environment had been built, the pre-built security environment still persists and CICS is therefore allowing users to continue to reuse it even though they are revoked.

CICS TS 3.1 will honor the revoked status of a USERID including the case where a user's connection to a GROUP is revoked.

CICS support for Mixed Case Passwords

- **Requires z/OS 1.7**
  - Mixed case support is mentioned in z/OS 1.7 preview
- **CESN enhancements**
  - Will not translate password field to upper case
    - Similar to CEDA mixed-case support
  - Will issue an appropriate caution message:
    - **DFHCE3540 Ensure that passwords are entered in the correct case.**

CICS support for Mixed Case Passwords - Notes

CICS TS 3.1 provides support for mixed case passwords.

Mixed case password support will require z/OS 1.7 which will provide Security Server support for mixed case passwords. (This support is mentioned on the z/OS 1.7 preview section of the z/OS 1.6 announcement letter.) CICS TS 3.1 will take advantage of this operating system enhancement if it is available. If the support is not available, CICS will always uppercase the password before presenting it to the External Security Manager.

CESN, the sign-on transaction, will be enhanced so as NOT to translate password fields into uppercase even if UCTRAN(YES) is specified for the terminal. This is similar to what CEDA currently does for mixed-case fields in CICS TS 2.3.

CESN will also be enhanced to issue a cautionary message if mixed case password support is available. The message "Ensure that passwords are entered in the correct case" will be issued.

Systems Programming Interface

- **INQUIRE TCPIPSERVICE, CORBASERVER and URIMAP**
  - CIPHERS
  - NUMCIPHERS
- **INQUIRE TCPIP**
  - CRLSERVER
  - SSLCACHE
- **INQUIRE and SET DISPATCHER**
  - MAXSSLTCBS
  - ACTSSLTCBS

Systems Programming Interface - Notes

The EXEC CICS commands INQUIRE TCPIPSERVICE, INQUIRE CORBASERVER and the new command INQUIRE URIMAP now include two security options.

CIPHERS(char56): returns the list of ciphers suites that are specified in the attribute CIPHERS for the resource definitions TCPIPSERVICE, CORBASERVER and URIMAP. This list of cipher suites are used to negotiate SSL connections. For example, if you were using weak encryption, the default value would be 03060102.

NUMCIPHERS=(hword): returns the number of cipher suites that are used to negotiate encryption levels as part of the SSL handshake.

The EXEC CICS INQUIRE TCPIP command also has two security options.

CRLSERVER(char256): returns the name of the LDAP server that is specified in the CRLSERVER system initialization parameter, that is used to store the certificate revocation lists.

SSLCACHE(cvda): returns a CVDA value indicating which cache is being used by SSL to store session ids. CVDA values are:
CICS The local SSL cache for the CICS region is being used
SSLSYSPLEX The SSL cache in the coupling facility is being used by SSL.

There are changes to the INQUIRE DISPATCHER and SET DISPATCHER commands to handle the SSL TCB pool. The following two options have been added:

MAXSSLTCBS(fword): returns the current maximum number of TCBs in the SSL OTE pool, as specified in the MAXSSLTCBS system initialization parameter.

ACTSSLTCBS(fword): returns the actual number of TCBs in the SSL OTE pool.

Summary

- **Support for TLS 1.0**
- **Support for cipher suites**
  - New AES 128 and 256 encodings
  - Specification of minimum and maximum encryption level
- **Performance enhancements**
  - SSL session id caching
  - OTE exploitation
- **New Certificate Revocation Lists utility transaction**
- **Mixed case password support**

Summary - Notes

There are a range of benefits that come from the improvements to security.

CICS now supports the Transport Layer Security (TLS) 1.0 protocol as well as SSL 3.0, allowing you to use the new AES cipher suites that offer 128-bit and 256-bit encryption.

There is more flexibility in controlling the encryption negotiation between client and server. You can specify a minimum as well as a maximum encryption level in CICS for negotiating with particular users.

CICS can now check all certificates against a certificate revocation list (CRL) when negotiating with clients. Any connections using revoked certificates are closed immediately.

You can specify whether you want to share session IDs across a sysplex by using the SSL cache. CICS will perform a partial SSL handshake if the client has negotiated with CICS previously. If the cache is shared across a number of CICS regions, this will improve the performance of SSL negotiation and connection

There are improvements to the performance of SSL to support new functions such as Web Services. The number of simultaneous SSL connections that can be used in the system at one time has increased to achieve better throughput.