Session 08

z/OS V1R9
System SSL Updates

Prepared by Patrick Kappeler
IBM Consulting IT Specialist
kappeler@fr.ibm.com

Redbooks
International Technical Support Organization

Trademarks

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

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.
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.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* 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.

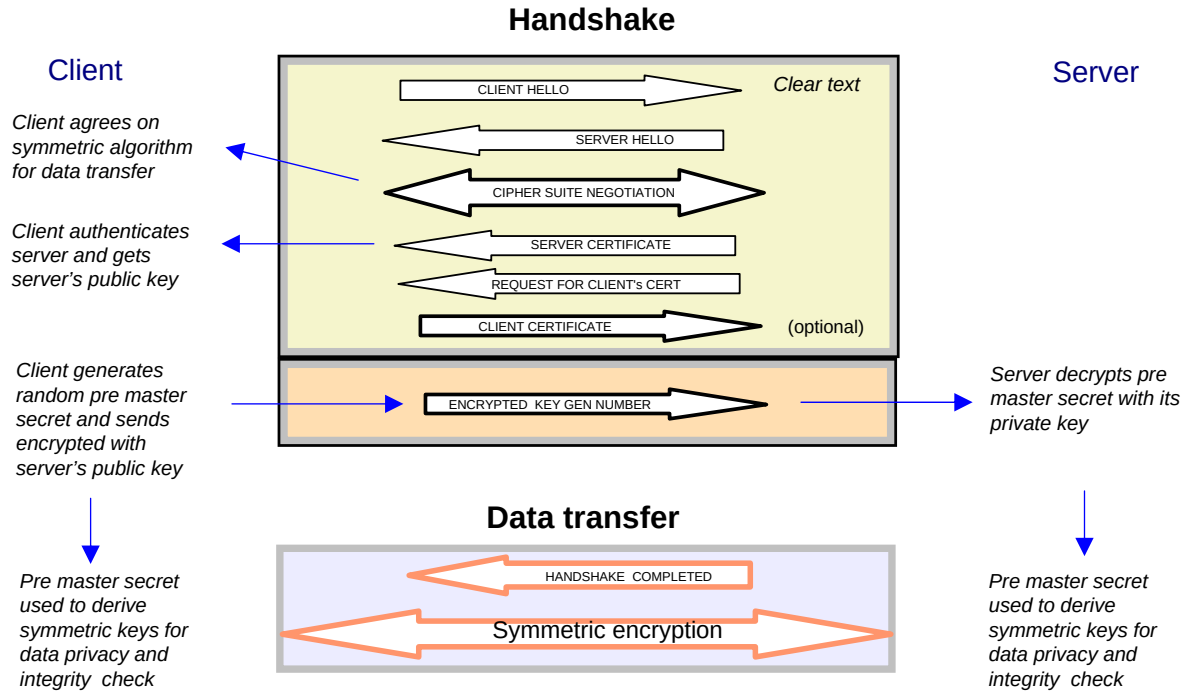
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- Certificate Revocation List Granularity
- Hostname Validation Granularity
- Hardware To Software Cryptography Notification
- Callback Re-handshake Notification

z/OS V1R9 System SSL Enhancements

The SSL/TLS Protocol



System SSL At z/OS V1R9

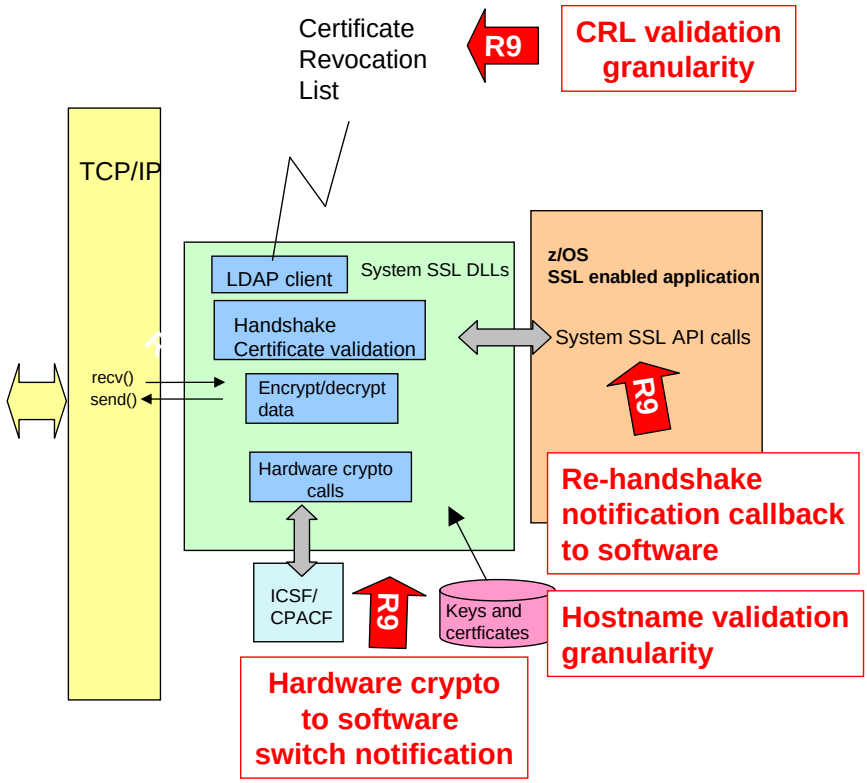
* SSL= Secure Socket layer
TLS= Transport Layer Security

- A set of C/C++ functions for establishing and using SSL/TLS * socket connections as an SSL/TLS server or client
- A set of C/C++ functions for applications to
  - manipulate keys and certificates databases, build and process PKCS#7 messages
- A key and certificates management facility (GSKKYMAN)

R9

Support of z/OS PKCS11 tokens

Already seen in session 06



Certificate Revocation List Granularity

A new environment variable:

GSK_CRL_SECURITY_LEVEL_LOW - Certificate validation will not fail if the LDAP server cannot be contacted .

GSK_CRL_SECURITY_LEVEL_MEDIUM - Certificate validation requires the LDAP server to be contactable, but does not require a CRL to be defined (default setting)

GSK_CRL_SECURITY_LEVEL_HIGH - Certificate validation requires the LDAP server to be contactable, and a CRL to be defined

Hostname Validation Granularity

An option to verify the partner's host name as it should appear in its certificate :

GSKCMS_VALIDATE_HOSTNAME_CN validate the host name against 1) - the common name (CN), 2)- the subject alternate name extension (DNS format) in the certificate

GSKCMS_VALIDATE_HOSTNAME_CN_ONLY validate the host name against the common name (CN) of the certificate only.

GSKCMS_VALIDATE_HOSTNAME_DNS validate the host name against 1)- the subject alternate name extension, 2)- the common name.

GSKCMS_VALIDATE_HOSTNAME_DNS_ONLY validate the host name against the subject alternate name extension only.

z/OS System SSL At z/OS V1R9

Hardware to software cryptography switch notification

Transparent to applications

•New messages - Require the SSL started task (GSKSRVR) to be configured and up and running prior to the SSL applications

Console message

GSK01051E jobname/ASID - Hardware encryption error. ICSF hardware encryption processing is unavailable

GSKSRVR system log message

GSK01052W jobname/ASID - Hardware encryption error. algorithm encryption processing switched to software

Callback Rehandshake Notification

Application provides callback routines names:

•One routine to be called back when the rehandshake starts
•One routine to be called back when the rehandshake completes

Support of z/OS PKCS#11 tokens by gskkyman

The System SSL gskkyman utility has been updated to handle PKCS#11 tokens as well as digital certificates and keys

See session 06

Thank You

Any Questions ?

Appendix

- System SSL Programming Guide SC24-5901-06
- RFC 2818 – HTTP over TLS - www.ietf.org/rfc/rfc2818.txt
- RFC 2246 – The TLS Protocol Version 1.0 – www.ieft.org/rfc/rfc2246.txt
- RFC 2459 – Internet X.509 PKI Certificate and CRL profile – www.ieft.org/rfc/rfc2459.txt