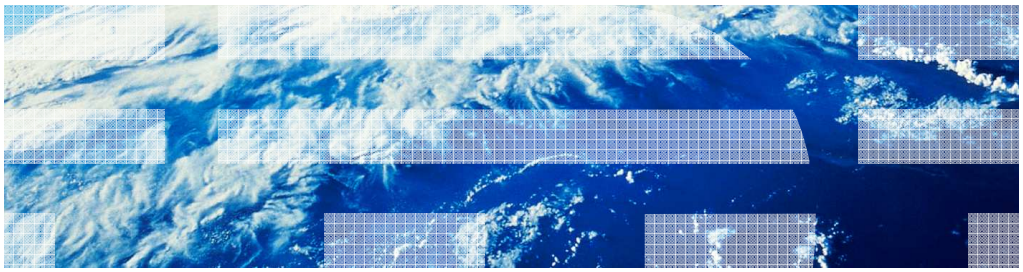
z/OS V1R13

SSL: ECC key reference by ICSF key label



Session objectives

- At the end of this presentation, you should have an understanding of …
  - The System SSL line item enhancements for
    - ECC Key Reference by ICSF Key Label
  - How to use the enhancements
  - Understand how these enhancements affect installation and migration

In V1R13, we are continuing to enhance our elliptic curve support. In V1R12 support was added for elliptic curve cryptography (ECC) certificates being imported into key database files and PKCS#11 tokens as well as the usage of the ECC certificates for digital signature sign and verification operations.

In V1R13 we are adding support for the generation of ECC certificates, ECC processing during the TLS handshake and usage of RACF certificates with their ECC private keys stored in ICSF's PKDS.

Overview - ECC key reference by ICSF key label

- **Problem Statement / Need Addressed**
  - With RACDCERT being enhanced (LI2423) to create and add certificates with their elliptic curve (ECC) keys stored in ICSF's PKDS, System SSL needs support for using these certificates.
- **Solution**
  - System SSL has been updated to handle ECC private keys being stored in ICSF's PKDS.
- **Benefit / Value**
  - Added security for protecting the ECC private key
  - ECC private key does not need to be in the clear to use.

Usage and invocation (1 of 2)

- No special invocation or application changes needed
- Just like other certificates, the ECC certificates must be connected to a SAF key ring and the application needs appropriate access to the key ring and certificate.
- Due to the nature of keys being stored in the PKDS, System SSL will call ICSF to perform required digital signature generation.

Usage and invocation (2 of 2)

- The SSL Started Task, “Display Crypto” command will show the status of ECC processing support available in hardware and software.
  f gsksrvr,d crypto

GSK1009I Cryptographic status

Algorithm	Hardware	Software
DES	56	56
3DES	168	168
AES	128	256
RC2	--	128
RC4	--	128
RSA Encrypt	4096	4096
RSA Sign	4096	4096
DSS	--	1024
SHA-1	160	160
SHA-2	512	512
ECC	521	521

The SSL Started Task, “Display Crypto” command shows the status of software and hardware support that can be used by System SSL during its cryptographic processing.

System SSL uses ICSF’s PKCS#11 support for ECC. This support is clear key based and performed through a software implementation within ICSF.

For secure ECC digital signature support, System SSL uses ICSF's callable service CSNDDSG.

This slide illustrates an example of the output from the “display crypto” command. ECC support shows it supports key sizes up to 521 for ECC. The “—” in the Hardware column indicates hardware is not available on the processor or through ICSF.

Interactions and dependencies

- Software Dependencies
  - ICSF Web Deliverable #10 (HCR7780) to be installed and operating on the system.
  - RACF (HRF7780) to be installed and operating on the system (or equivalent ESM that supports elliptic curves in ICSF's PKDS).
- Hardware Dependencies
  - zEnterprise Server with Crypto Express3 Coprocessor cards
- Exploiters
  - Any customers or users that may require ECC based certificates or want to perform TLS handshakes using ECC based key exchanges.

Before z/OS V1R12, System SSL contained software implementations for all utilized algorithms. Either through direct calls to CPACF or ICSF, System SSL is able to exploit cryptographic support provided through either the CPACF or Crypto Express cards. With the introduction of Elliptic Curve Cryptography in R12, System SSL no longer has its own software implementation. It will be relying on ICSF's PKCS#11 support for ECC.

ICSF HCR7780 is shipped in the base of z/OS V1R13 and provides ECC support. The usage of the ICSF callable services can be control through access to the CSFSERV resource class. System SSL ECC support requires read access to the CSF1DVK, CSF1GAV, CSF1GKP, CSF1PKS, CSF1PKV, CSF1TRC and CSF1TRD resources depending on the function being performed by SSL. If utilizing ECC private keys stored in the PKDS, READ may also be needed to the CSFKEYS resource class.

Migration and coexistence considerations

- None.

Installation

- None

Session summary

- You should now be able to:
  - Understand the recent changes in System SSL
  - Understand the migration changes
  - Identify how to install System SSL
  - Be able to find any of the above information in the relevant publications

Appendix - References

- **Publication**
  - System Secure Sockets Layer Programming SC24-5901-10
- **Specifications**
  - RFC4492, Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) – http://tools.ietf.org/html/rfc4492
  - Standards for Efficient Cryptography Group (SECG), "SEC 1: Elliptic Curve Cryptography", http://www.secg.org/download/aid-780/sec1-v2.pdf
  - Standards for Efficient Cryptography Group (SECG), "SEC 2: Recommended Elliptic Curve Domain Parameters", http://www.secg.org/download/aid-386/sec2_final.pdf
  - RFC3279, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – http://www.rfc-editor.org/rfc/rfc3279.txt
  - RFC5480, Elliptic Curve Cryptography Subject Public Key Information – http://www.rfc-editor.org/rfc/rfc5480.txt
  - RFC5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation – http://www.rfc-editor.org/rfc/rfc5639.txt
  - FIPS 186-2, Digital Signature Standard (DSS) – http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.pdf

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, Express, RACF, z/OS, and zEnterprise are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.