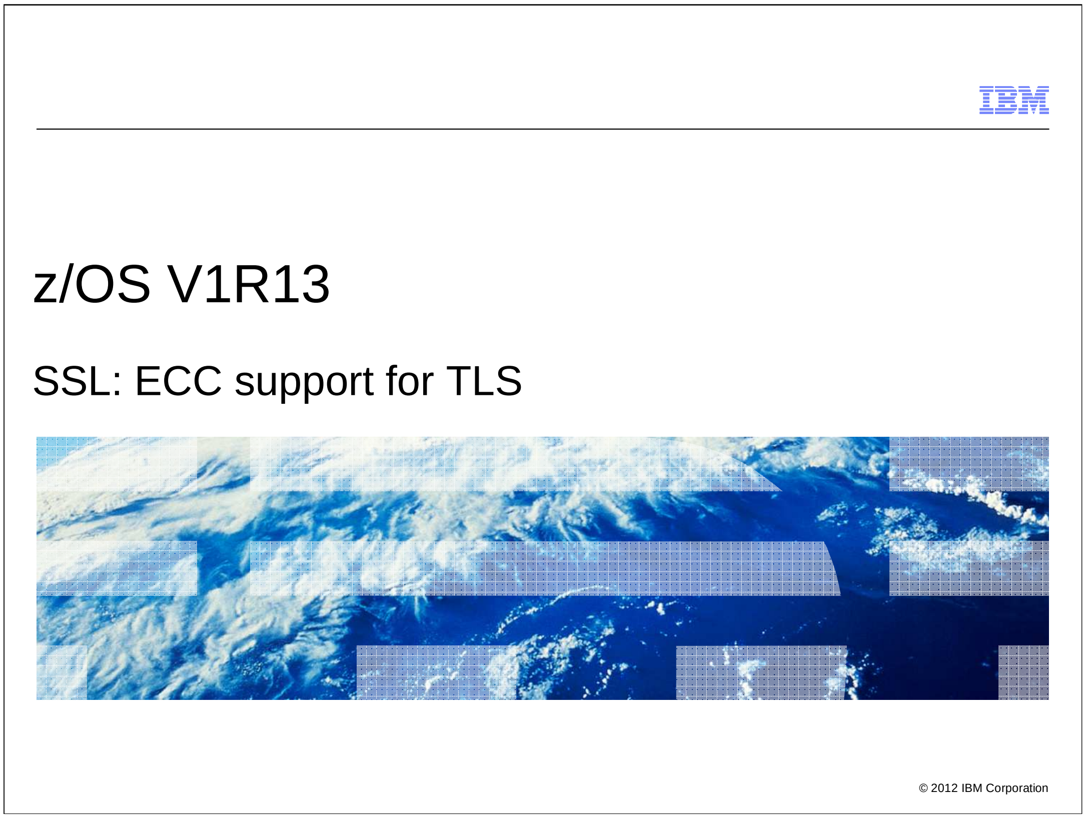
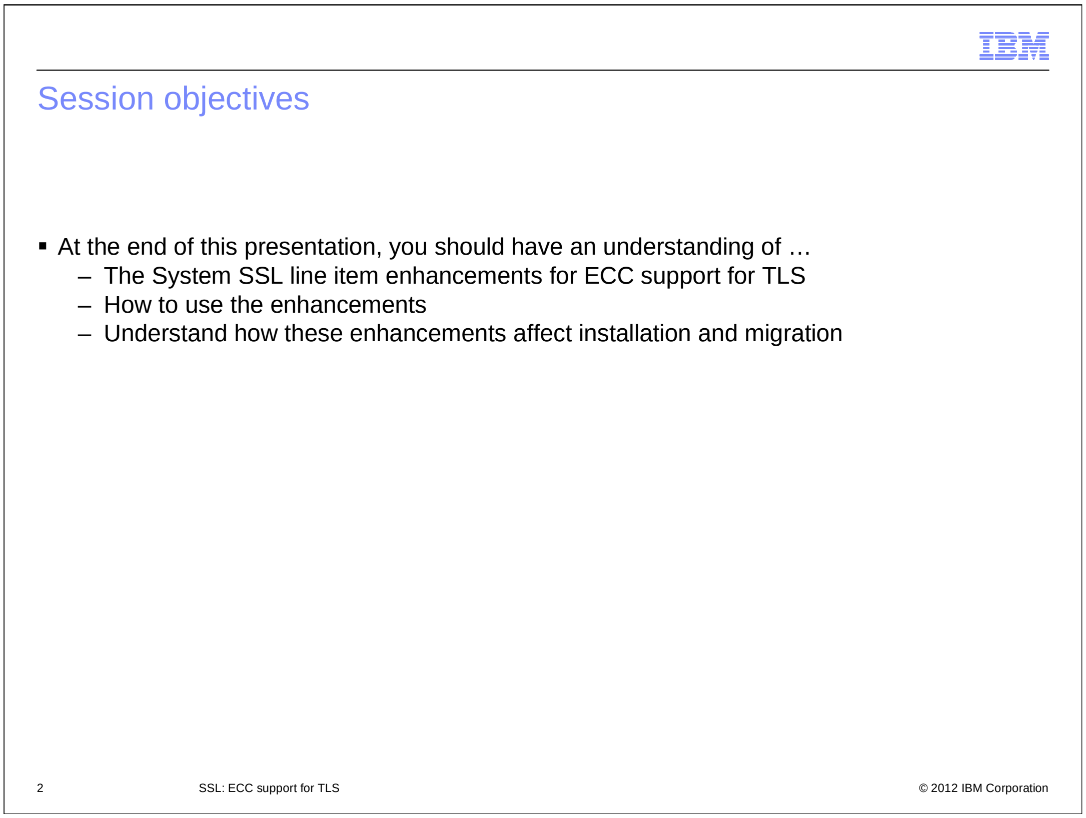


z/OS V1R13

SSL: ECC support for TLS



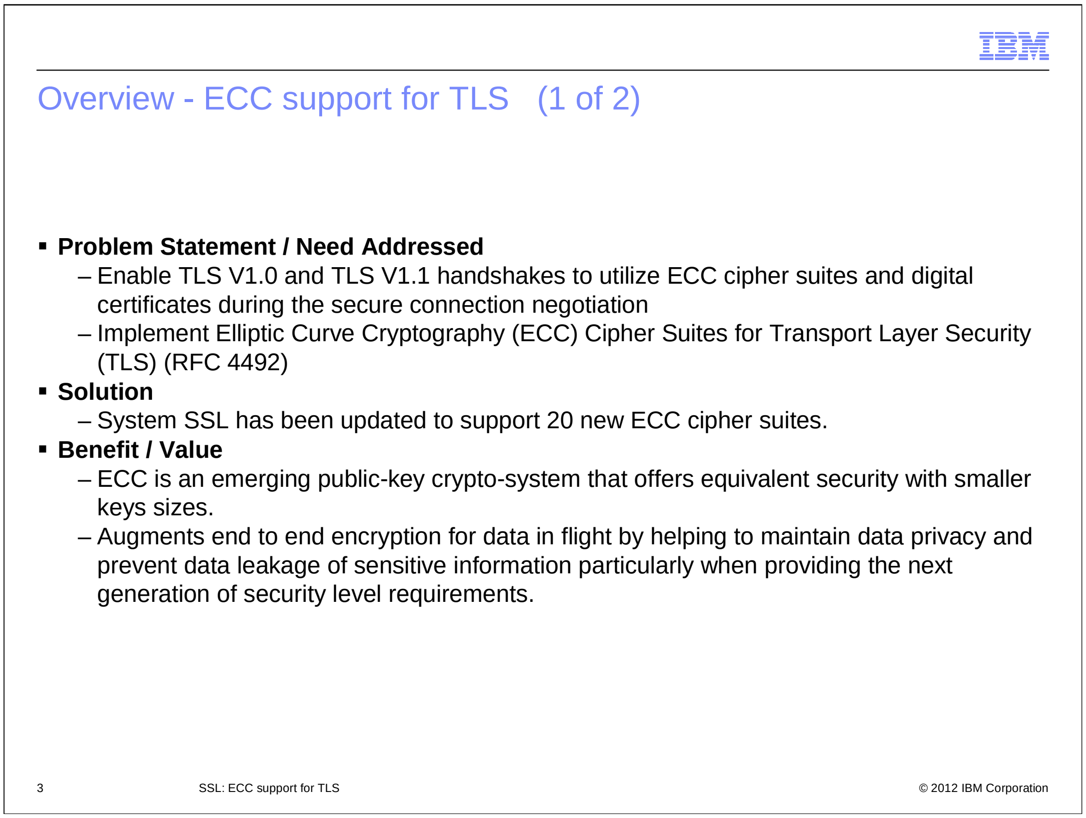
Session objectives

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

2 SSL: ECC support for TLS © 2012 IBM Corporation

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.

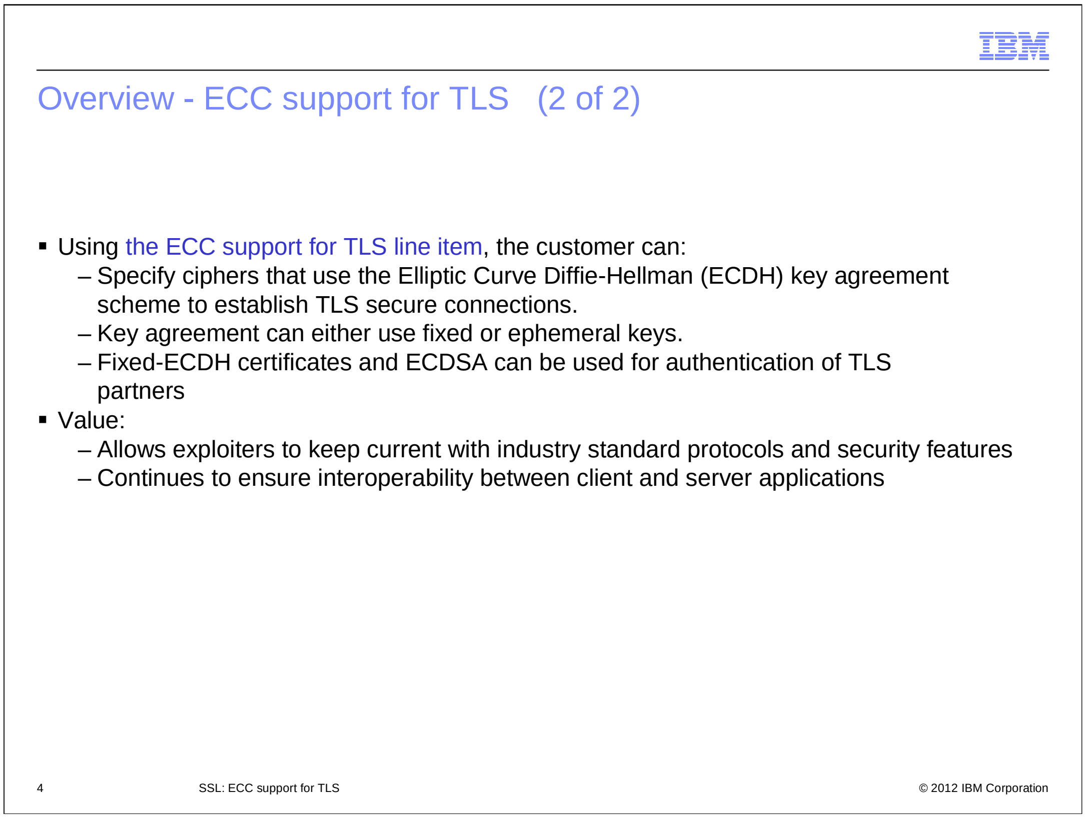


Overview - ECC support for TLS (1 of 2)

- **Problem Statement / Need Addressed**
  - Enable TLS V1.0 and TLS V1.1 handshakes to utilize ECC cipher suites and digital certificates during the secure connection negotiation
  - Implement Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) (RFC 4492)
- **Solution**
  - System SSL has been updated to support 20 new ECC cipher suites.
- **Benefit / Value**
  - ECC is an emerging public-key crypto-system that offers equivalent security with smaller keys sizes.
  - Augments end to end encryption for data in flight by helping to maintain data privacy and prevent data leakage of sensitive information particularly when providing the next generation of security level requirements.

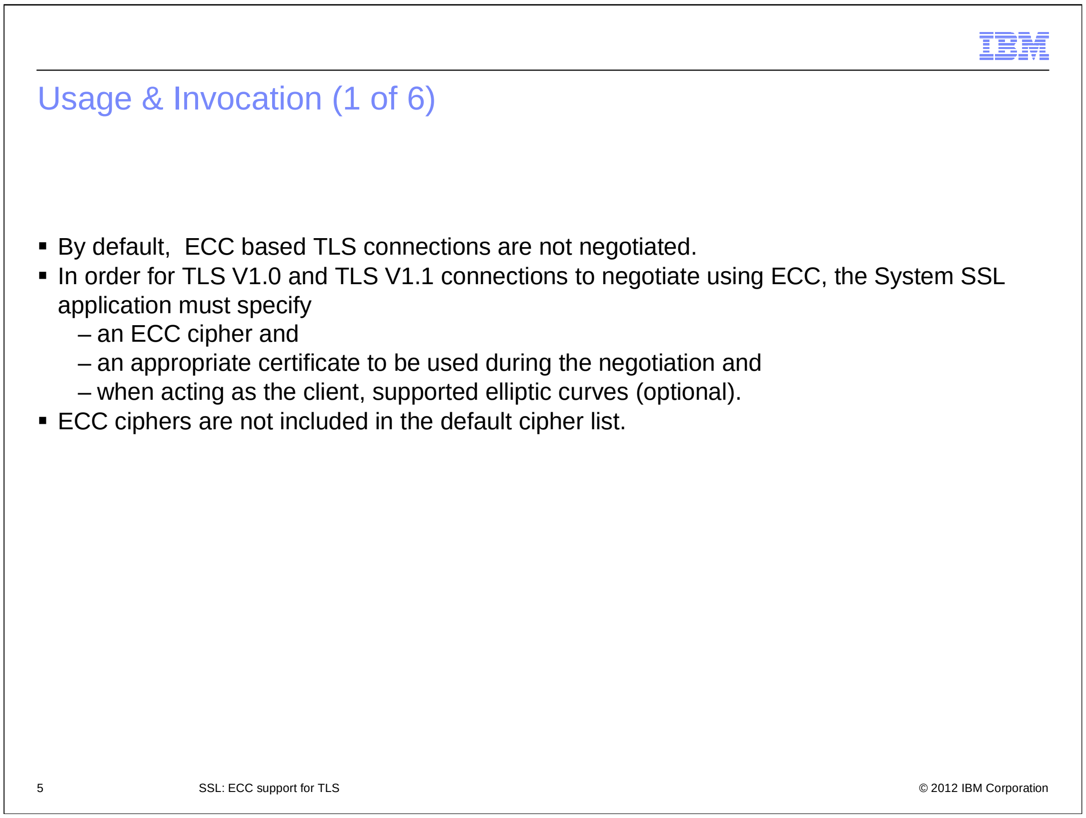
Prior to R13, System SSL supported TLS handshakes which either utilized RSA or Diffie-hellman for its key exchange method. With the introduction of RFC 4492, TLS handshakes using Elliptic Curve Diffie-Hellman key exchange was introduced.

The existing ciphers supported by System SSL identified the use of RSA and DH key exchange. In order to support Elliptic Curve Diffie-Helllman key exchange, RFC 4492 introduced a series of new ciphers specifically used for ECC specific ciphers.



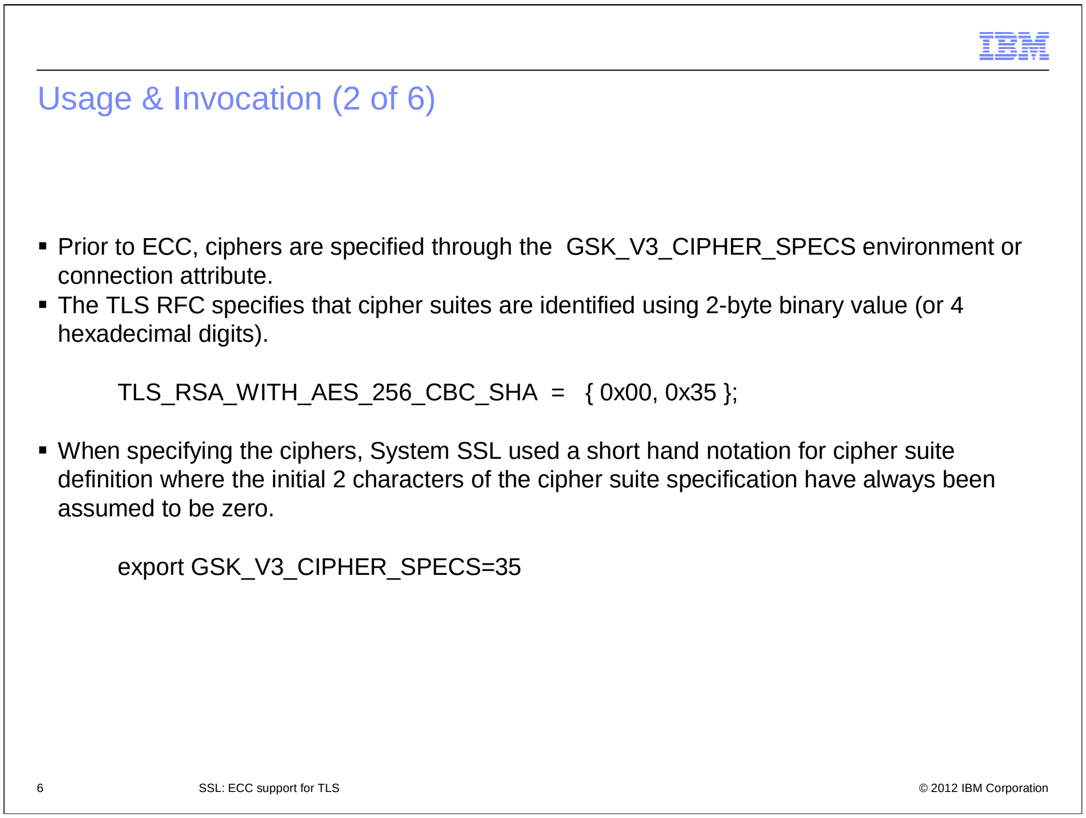
Overview - ECC support for TLS (2 of 2)

- Using the ECC support for TLS line item, the customer can:
  - Specify ciphers that use the Elliptic Curve Diffie-Hellman (ECDH) key agreement scheme to establish TLS secure connections.
  - Key agreement can either use fixed or ephemeral keys.
  - Fixed-ECDH certificates and ECDSA can be used for authentication of TLS partners
- Value:
  - Allows exploiters to keep current with industry standard protocols and security features
  - Continues to ensure interoperability between client and server applications



Usage & Invocation (1 of 6)

- By default, ECC based TLS connections are not negotiated.
- In order for TLS V1.0 and TLS V1.1 connections to negotiate using ECC, the System SSL application must specify
  - an ECC cipher and
  - an appropriate certificate to be used during the negotiation and
  - when acting as the client, supported elliptic curves (optional).
- ECC ciphers are not included in the default cipher list.



Usage & Invocation (2 of 6)

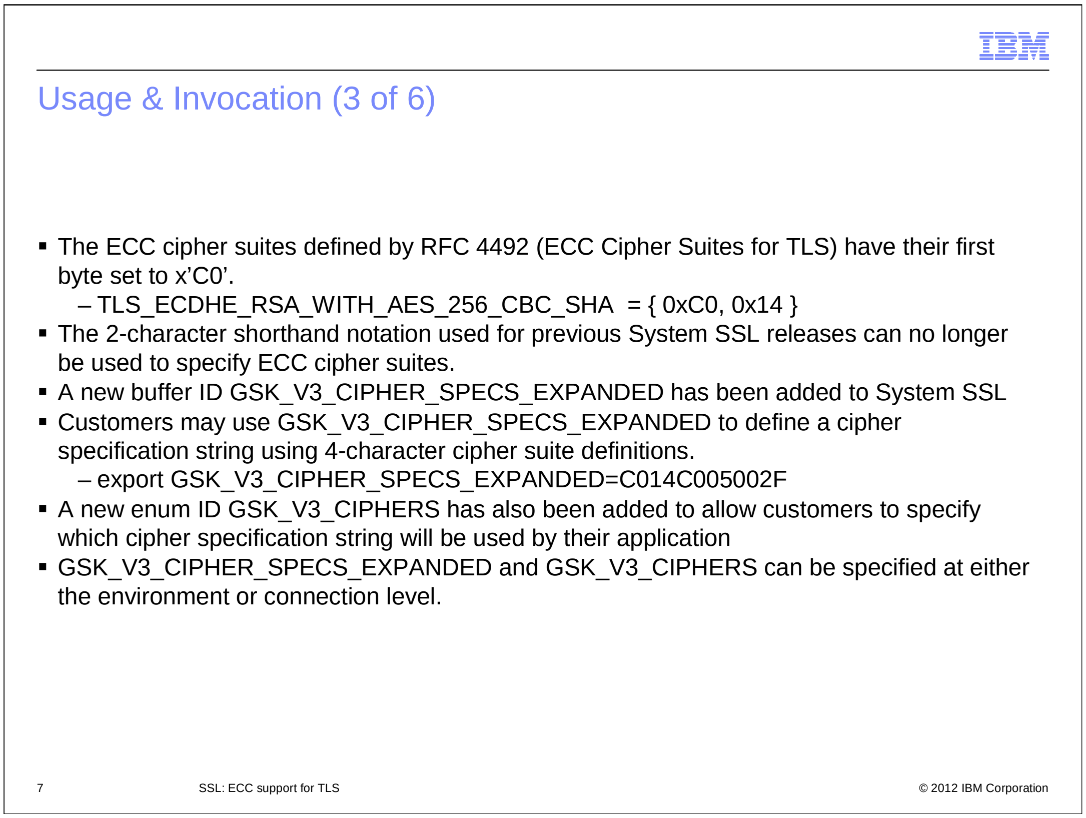
- Prior to ECC, ciphers are specified through the GSK_V3_CIPHER_SPECS environment or connection attribute.
- The TLS RFC specifies that cipher suites are identified using 2-byte binary value (or 4 hexadecimal digits).

```
TLS_RSA_WITH_AES_256_CBC_SHA  =   { 0x00, 0x35 };
```

- When specifying the ciphers, System SSL used a short hand notation for cipher suite definition where the initial 2 characters of the cipher suite specification have always been assumed to be zero.

```
export GSK_V3_CIPHER_SPECS=35
```

With the introduction of ECC ciphers, System SSL's strategy for cipher specification was modified. Prior to ECC ciphers, System SSL supported 2 character cipher identifiers. These values mapped to the latter portion of the cipher in the TLS RFCs 2246 and 4346. Since all ciphers started with 2 characters zeros, System SSL assumed the values were 00 and the values were never specified.

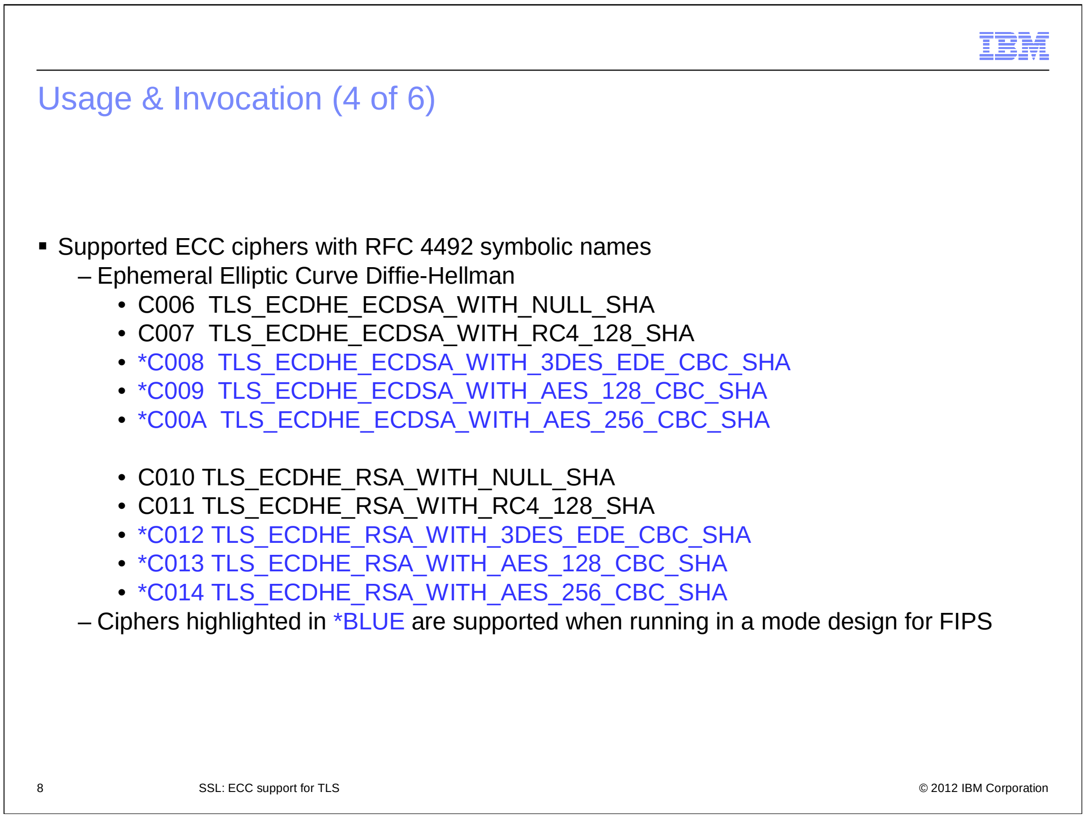


Usage & Invocation (3 of 6)

- The ECC cipher suites defined by RFC 4492 (ECC Cipher Suites for TLS) have their first byte set to x’C0’.
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA = { 0xC0, 0x14 }
- The 2-character shorthand notation used for previous System SSL releases can no longer be used to specify ECC cipher suites.
- A new buffer ID GSK_V3_CIPHER_SPECS_EXPANDED has been added to System SSL
- Customers may use GSK_V3_CIPHER_SPECS_EXPANDED to define a cipher specification string using 4-character cipher suite definitions.
  - export GSK_V3_CIPHER_SPECS_EXPANDED=C014C005002F
- A new enum ID GSK_V3_CIPHERS has also been added to allow customers to specify which cipher specification string will be used by their application
- GSK_V3_CIPHER_SPECS_EXPANDED and GSK_V3_CIPHERS can be specified at either the environment or connection level.

7 SSL: ECC support for TLS © 2012 IBM Corporation

When ECC ciphers were introduced, the RFC identified ECC ciphers by changing the leading character zeros to “C0”. In order for System SSL to accommodate the new cipher identifiers, applications supporting ECC ciphers will be required to used the GSK_V3_CIPHER_EXPANDED attribute in addition to specifying the GSK_V3_CIPHER attribute to indicate that the SSL environment or connection will be utilizing 4 byte cipher values instead of 2 byte cipher values.



Usage & Invocation (4 of 6)

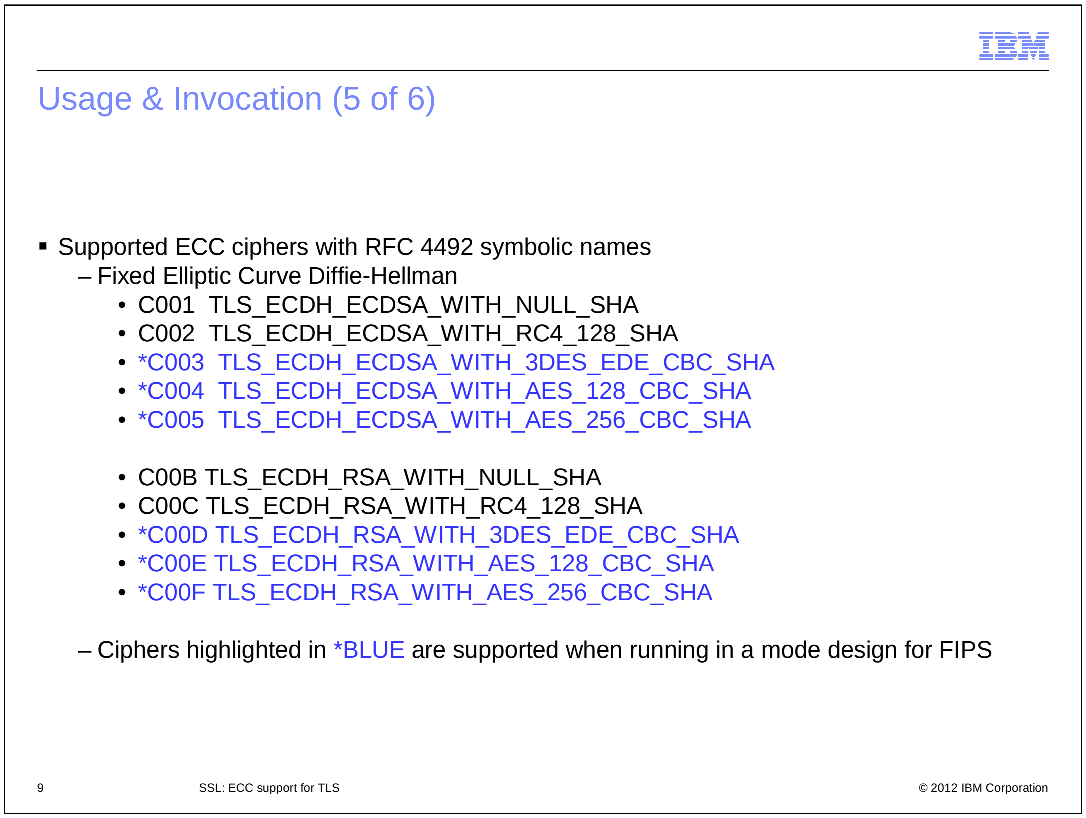
- Supported ECC ciphers with RFC 4492 symbolic names
  - Ephemeral Elliptic Curve Diffie-Hellman
    - C006 TLS_ECDHE_ECDSA_WITH_NULL_SHA
    - C007 TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
    - *C008 TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
    - *C009 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
    - *C00A TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
    - C010 TLS_ECDHE_RSA_WITH_NULL_SHA
    - C011 TLS_ECDHE_RSA_WITH_RC4_128_SHA
    - *C012 TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
    - *C013 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    - *C014 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  - Ciphers highlighted in *BLUE are supported when running in a mode design for FIPS

RFC 4492 defines ciphers for

- Ephemeral Elliptic Curve Diffie-Hellman
- Fixed Elliptic Curve Diffie-Hellman

- This slide lists the supported Ephemeral Elliptic Curve Diffie-Hellman ciphers with the cipher symbolic names from the RFC. Note that the ciphers allow the usage of both ECDSA and RSA based certificates and strong crypto. The ciphers allowing RSA based certificates allows implementations currently using RSA based certificates to continue using the them with an ephemeral key exchange.

- Anonymous Ephemeral Elliptic Curve Diffie-Hellman is not supported.



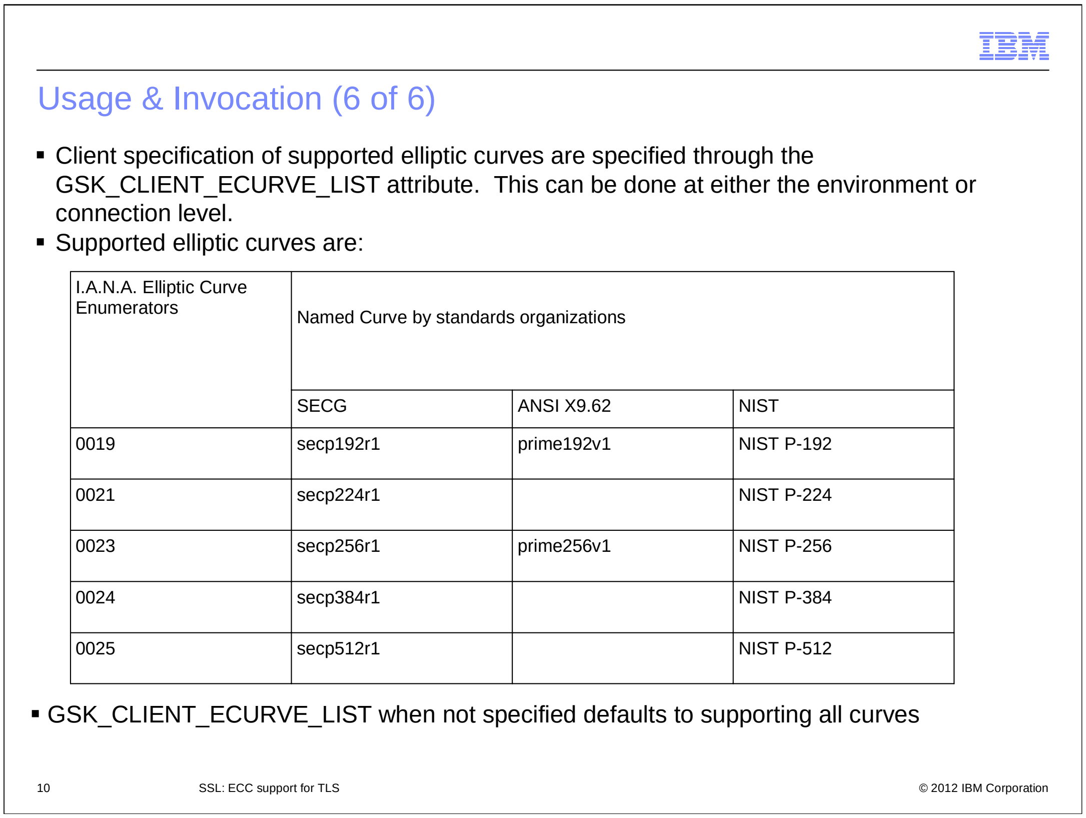
Usage & Invocation (5 of 6)

- Supported ECC ciphers with RFC 4492 symbolic names
  - – Fixed Elliptic Curve Diffie-Hellman
    - C001 TLS_ECDH_ECDSA_WITH_NULL_SHA
    - C002 TLS_ECDH_ECDSA_WITH_RC4_128_SHA
    - *C003 TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
    - *C004 TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
    - *C005 TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA

    - C00B TLS_ECDH_RSA_WITH_NULL_SHA
    - C00C TLS_ECDH_RSA_WITH_RC4_128_SHA
    - *C00D TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
    - *C00E TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
    - *C00F TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
  - – Ciphers highlighted in *BLUE are supported when running in a mode design for FIPS

- This slide lists the supported Fixed Elliptic Curve Diffie-Hellman ciphers with the cipher symbolic names from the RFC. Note that the ciphers allow the usage of ECC certificates keys signed with either ECDSA or RSA certificates.

- Anonymous Fixed Elliptic Curve Diffie-Hellman is not supported.



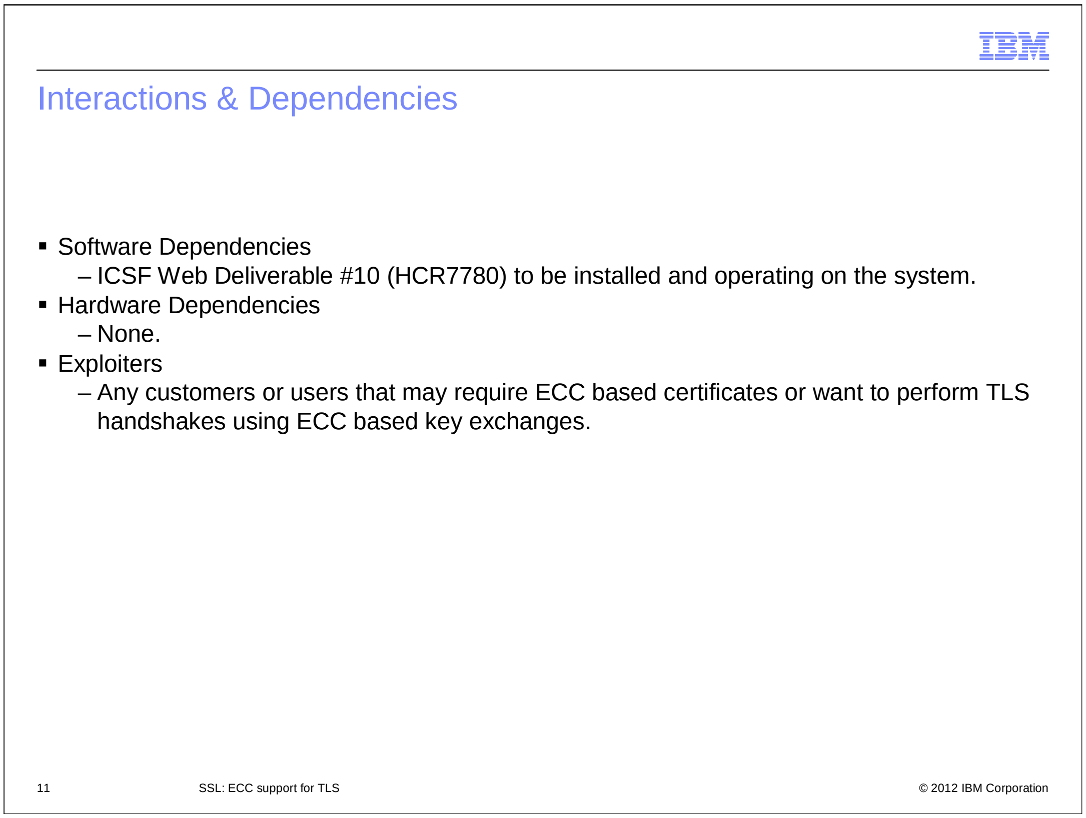
Usage & Invocation (6 of 6)

- Client specification of supported elliptic curves are specified through the GSK_CLIENT_ECURVE_LIST attribute. This can be done at either the environment or connection level.
- Supported elliptic curves are:

I.A.N.A. Elliptic Curve Enumerators	Named Curve by standards organizations		
	SECG	ANSI X9.62	NIST
0019	secp192r1	prime192v1	NIST P-192
0021	secp224r1		NIST P-224
0023	secp256r1	prime256v1	NIST P-256
0024	secp384r1		NIST P-384
0025	secp512r1		NIST P-512

- GSK_CLIENT_ECURVE_LIST when not specified defaults to supporting all curves

The GSK_CLIENT_ECURVE_LIST attribute allows the client application to limit what elliptic curves can be used during the handshake process.

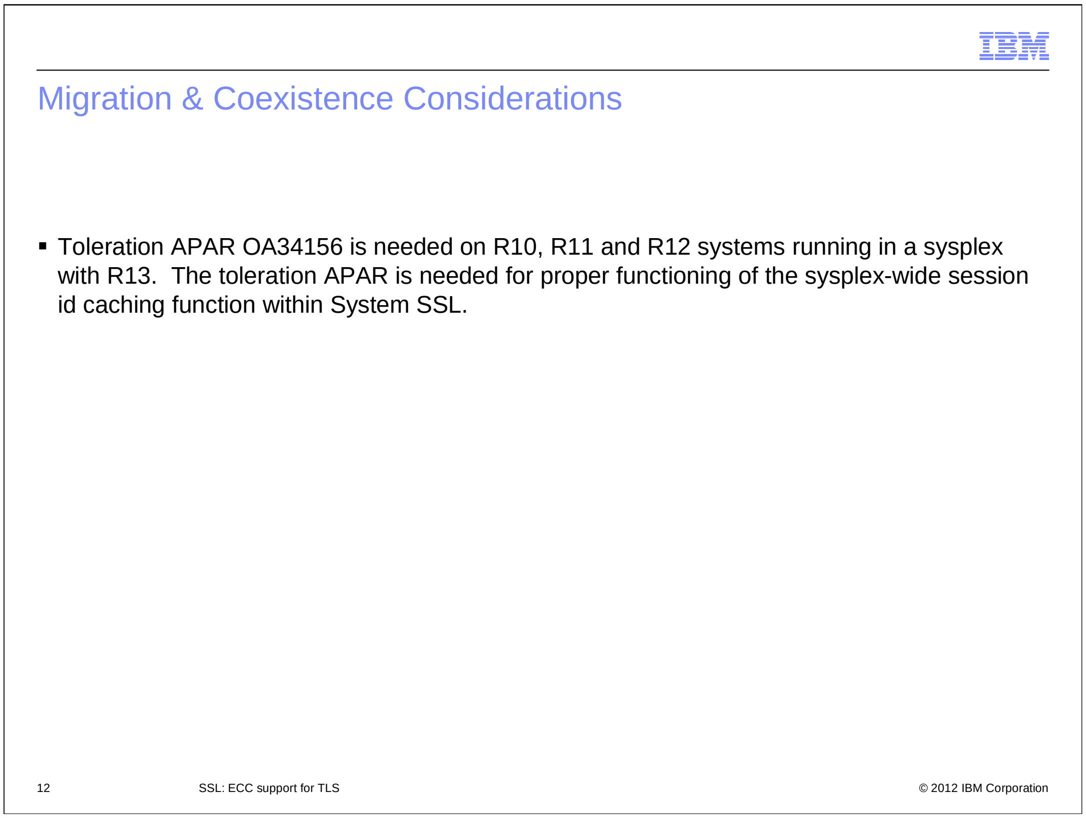


Interactions & Dependencies

- Software Dependencies
  - ICSF Web Deliverable #10 (HCR7780) to be installed and operating on the system.
- Hardware Dependencies
  - None.
- Exploiters
  - Any customers or users that may require ECC based certificates or want to perform TLS handshakes using ECC based key exchanges.

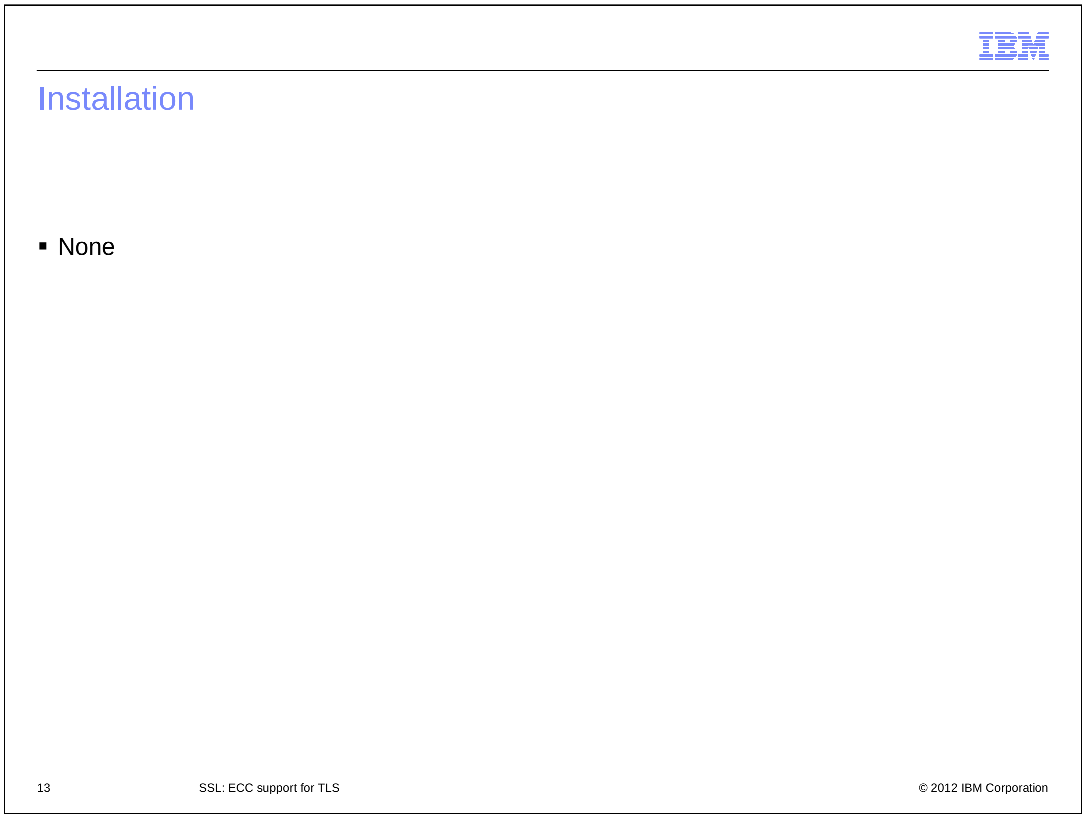
Prior to z/OS V1R12, System SSL contained software implementations for all utilized algorithms. Either through direct calls to CPACF or ICSF, System SSL is able to exploit cryptographic support provided through either the CPACF or Crypto Express cards. With the introduction of Elliptic Curve Cryptography 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.



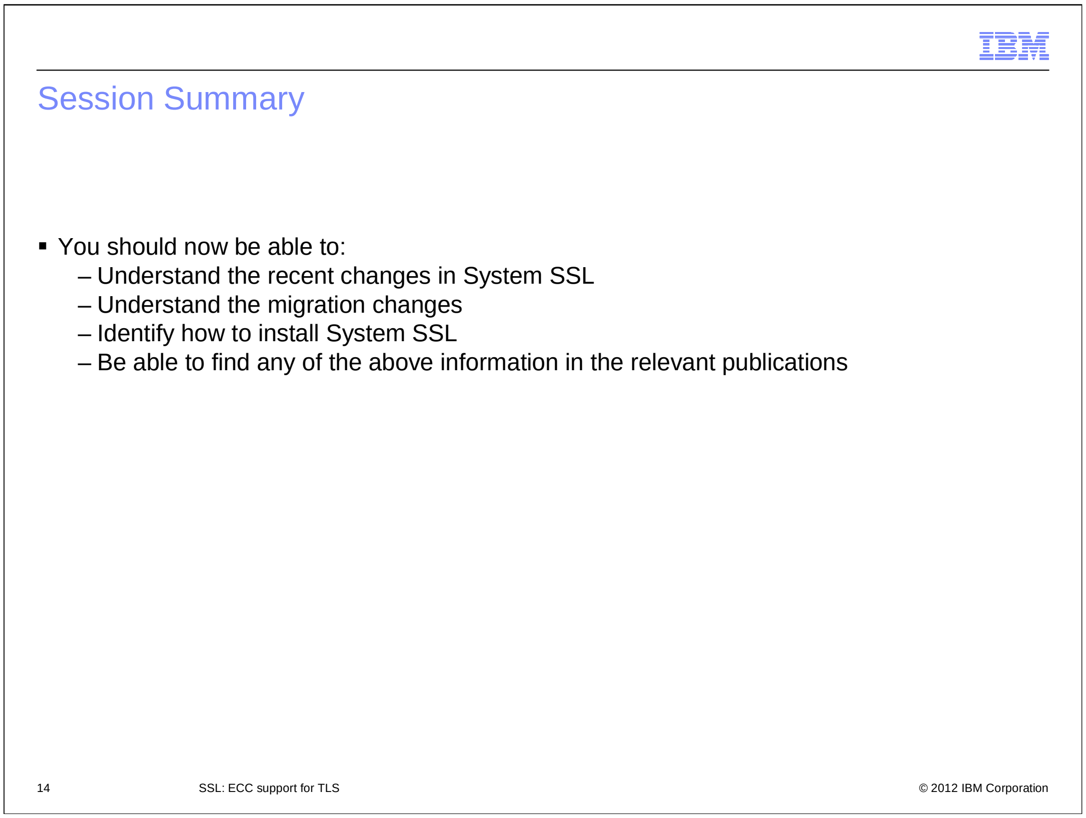
Migration & Coexistence Considerations

- Toleration APAR OA34156 is needed on R10, R11 and R12 systems running in a sysplex with R13. The toleration APAR is needed for proper functioning of the sysplex-wide session id caching function within System SSL.



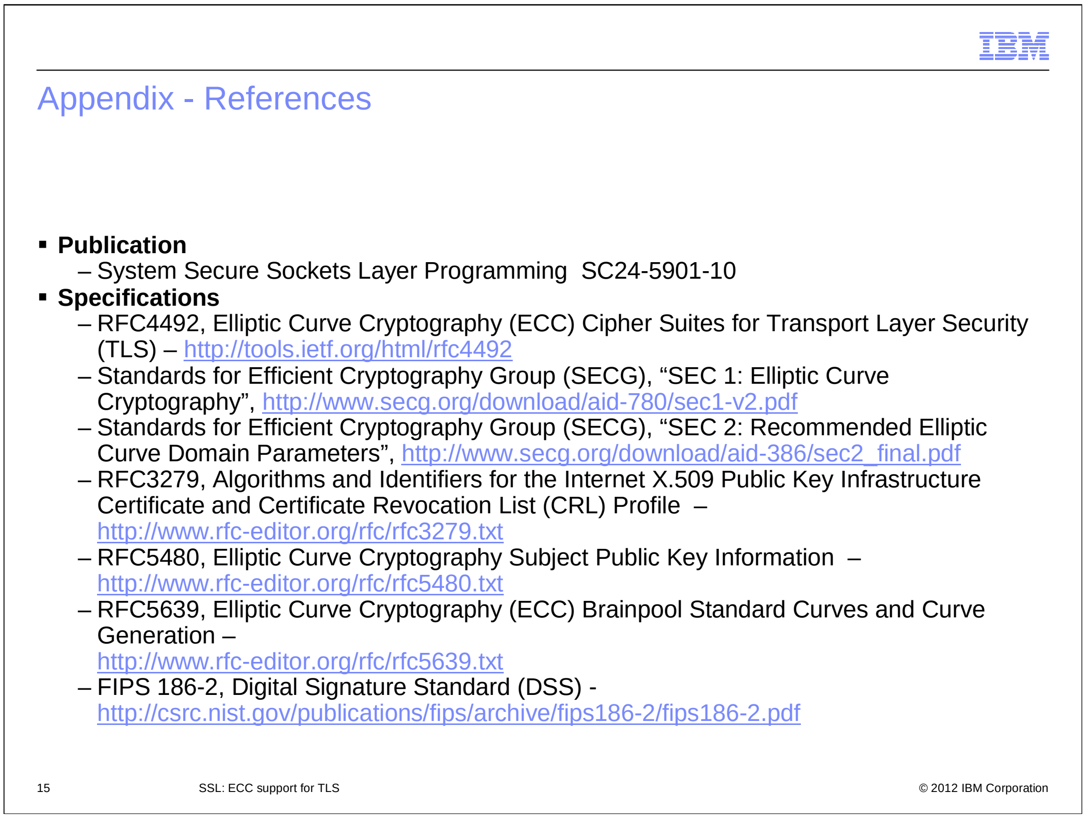
Installation

- None



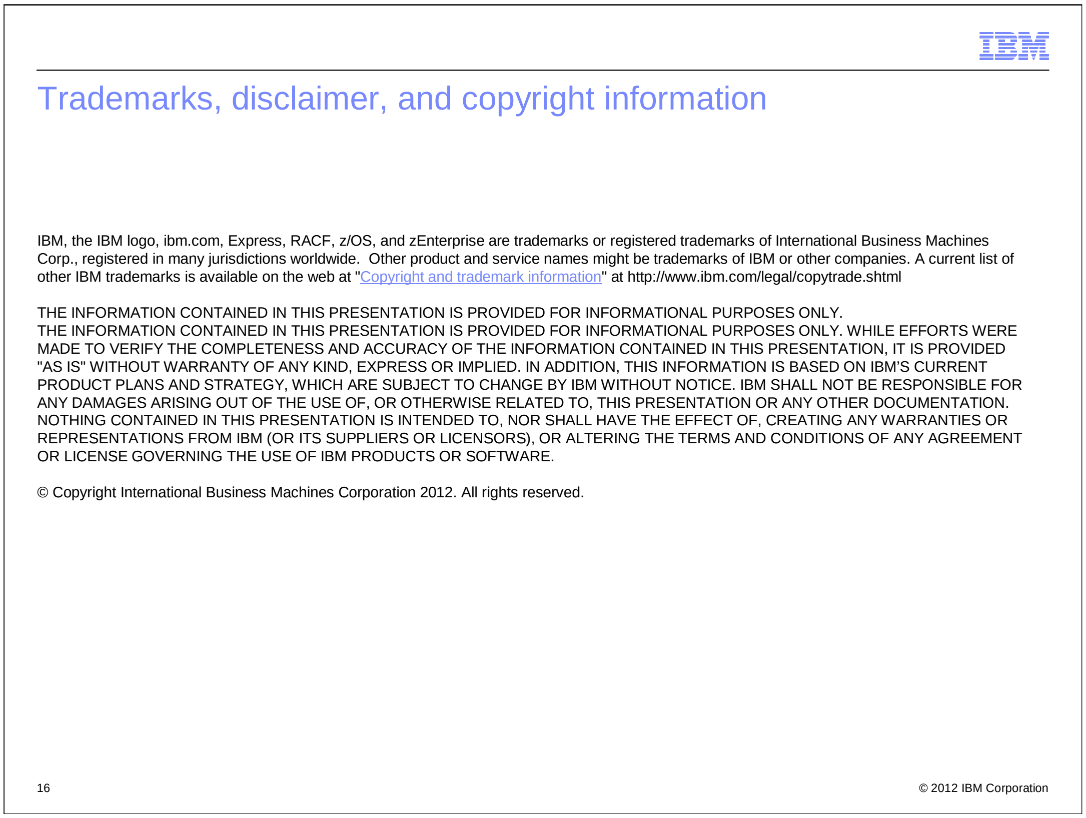
Session Summary

- 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.