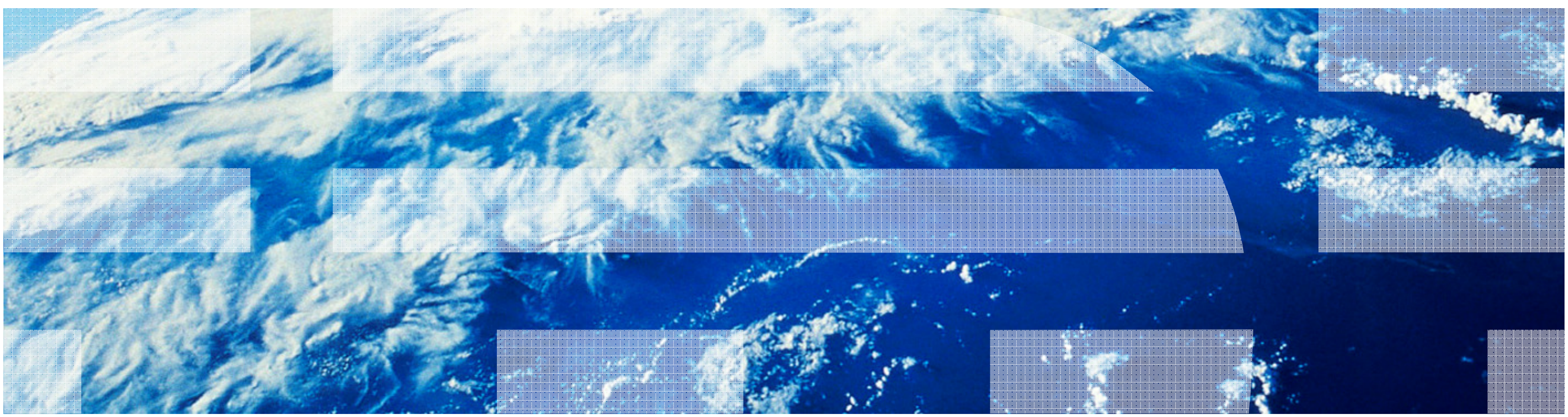
z/OS Communications Server
TCP/IP Cryptography Demystified

SHARE Session 13543

Lin Overby, CISSP – overbylh@us.ibm.com
Chris Meyer, CISSP – meyerchr@us.ibm.com
z/OS Communications Server



August 13, 2013

© 2013 IBM Corporation

Trademarks, notices, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

- Advanced Peer-to-Peer Networking®
- AIX®
- alphaWorks®
- AnyNet®
- AS/400®
- BladeCenter®
- Candle®
- CICS®
- DataPower®
- DB2 Connect
- DB2®
- DRDA®
- e-business on demand®
- e-business (logo)
- e business(logo)®
- ESCON®
- FICON®
- GDDM®
- GDPS®
- Geographically Dispersed Parallel Sysplex
- HiperSockets
- HPR Channel Connectivity
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM eServer
- IBM (logo)®
- IBM®
- IBM zEnterprise™ System
- IMS
- InfiniBand ®
- IP PrintWay
- IPDS
- iSeries
- LANDP®
- Language Environment®
- MQSeries®
- MVS
- NetView®
- OMEGAMON®
- Open Power
- OpenPower
- Operating System/2®
- Operating System/400®
- OS/2®
- OS/390®
- OS/400®
- Parallel Sysplex®
- POWER®
- POWER7®
- PowerVM
- PR/SM
- pSeries®
- RACF®
- Rational Suite®
- Rational®
- Redbooks
- Redbooks (logo)
- Sysplex Timer®
- System i5
- System p5
- System x®
- System z®
- System z9®
- System z10
- Tivoli (logo)®
- Tivoli®
- VTAM®
- WebSphere®
- xSeries®
- z9®
- z10 BC
- z10 EC
- zEnterprise
- zSeries®
- z/Architecture
- z/OS®
- z/VM®
- z/VSE

* All other products may be trademarks or registered trademarks of their respective companies.

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license there from.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- InfiniBand is a trademark and service mark of the InfiniBand Trade Association.
- Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
- IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

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.

Refer to www.ibm.com/legal/us for further legal information.

© 2013 IBM Corporation

Why this presentation?

To answer the question…

"What hardware crypto facilities get used when?"

© 2013 IBM Corporation

Agenda

- Review of basic cryptographic operations
  - Symmetric cryptography
  - Asymmetric cryptography
  - Message digests and secure message authentication codes
  - Digital certificates
  - FIPS 140
- z/OS TCP/IP network security protocols
  - SSL/TLS
  - AT-TLS
  - IPSec and IKE
- Relevant System z & z/OS cryptographic componentry
  - Hardware components
  - Software components
  - Communications Server usage
- Conclusion

© 2013 IBM Corporation

Agenda

- **Review of basic cryptographic operations**
  - **Symmetric cryptography**
  - **Asymmetric cryptography**
  - **Message digests and secure message authentication codes**
  - **Digital certificates**
  - **FIPS 140**
- z/OS TCP/IP network security protocols
  - SSL/TLS
  - AT-TLS
  - IPSec and IKE
- Relevant System z & z/OS cryptographic componentry
  - Hardware components
  - Software components
  - Communications Server usage
- Conclusion

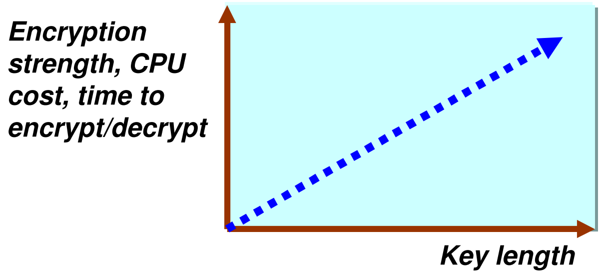
© 2013 IBM Corporation

Cryptographic Basics

- **Cryptography is the use of mathematical algorithms to transform data for the purposes of ensuring:**
  - ***Partner authentication*** – proving the other end point of the secure communication is who it claims to be (certificates and asymmetric encryption)
  - ***Data privacy*** – hiding the data (encryption/decryption)
  - ***Data integrity*** – proving the data hasn't been modified since it was sent (message digests and secure message authentication codes)
  - ***Data origin authentication*** – proving the data's origin (message digests and secure message authentication codes)

- **Cryptographic operations are compute intensive, hence the need for hardware assist technologies**

- **General rule: For a given algorithm: the longer keys, the stronger security, the more compute intensive**
  - For example, AES-128 vs. AES-256
  - Increases the amount of work an attacker needs to do to crack the code



© 2013 IBM Corporation

Glossary (1 of 2)

- AES – Advanced Encryption Standard (symmetric encryption, 128/192/256/512 bit keys)
- AH – Authentication Header (IPsec data authentication protocol)
- DES – Digital Encryption Standards (symmetric encryption, 56 bit keys)
- 3DES – Triple-DES (symmetric encryption, 168 bit keys)
- CBC – Cipher Block Chaining mode (block cipher mode that ensures either confidentiality or integrity)
- DH - Diffie-Hellman (secure key agreement algorithm)
- DSA – Digital Signature Algorithm (asymmetric encryption, 512/1024 bits*)
- ECC – Elliptic Curve Cryptography (asymmetric encryption algorithm)
- ECDH – Elliptic Curve Diffie-Hellman (an ECC-based variant of Diffie-Hellman key exchange)
- ECDSA – Elliptic Curve Digital Signature Algorithm (ECC-based variant of the asymmetric Digital Signature Algorithm (DSA))
- ESP – Encapsulating Security Payload (IPsec data privacy and authentication protocol)
- GCM – Galois Counter Mode (block cipher mode that simultaneously ensures confidentiality and integrity)
- GMAC – An authentication-only variant of GCM
- IKE – Internet Key Exchange (protocol used for setting up dynamic IPsec tunnels)
- IPsec – IP security (secure networking protocol, consists of AH and ESP)

© 2013 IBM Corporation

Glossary (2 of 2)

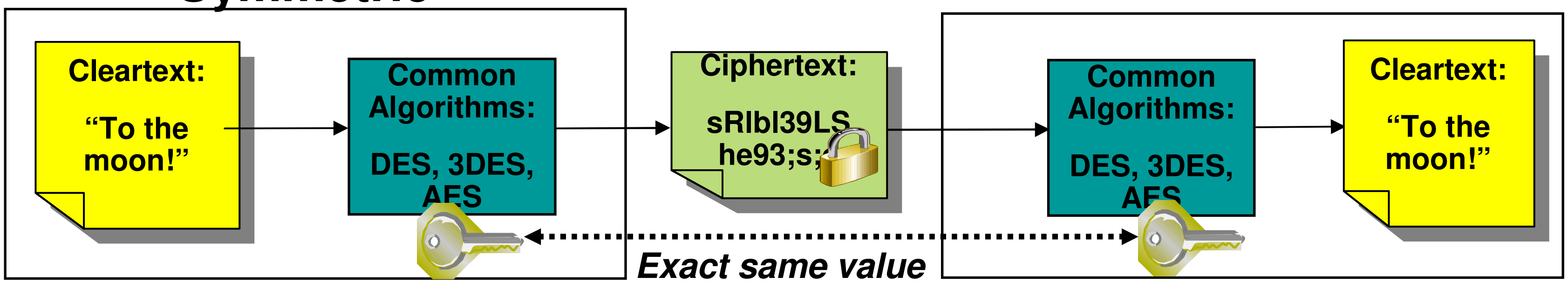
- MD5 – Message Digest 5 (message digest, 128 bits)
- NSS[D] – z/OS network security services [daemon]
- PRF – Pseudorandom functions (efficient algorithms that generate statistically random fixed-length values)
- SHA-1 – Secure Hash Algorithm-1 (message digest, 160 bits)
- SHA-2 – Secure Hash Algorithm-2 (message digest, 224/256/384/512 bits)
- SSL – Secure Sockets Layer (secure networking protocol for authentication and privacy)
- RSA – Rivest, Shamir, Adleman (asymmetric encryption, 1024/2048/4096 bit keys*)
- TLS – Transport Layer Security (IETF-adopted form of SSL)
- XCBC – Extended CBC (variant of CBC that simultaneously ensures confidentiality and integrity)

* other sizes allowed in between

© 2013 IBM Corporation

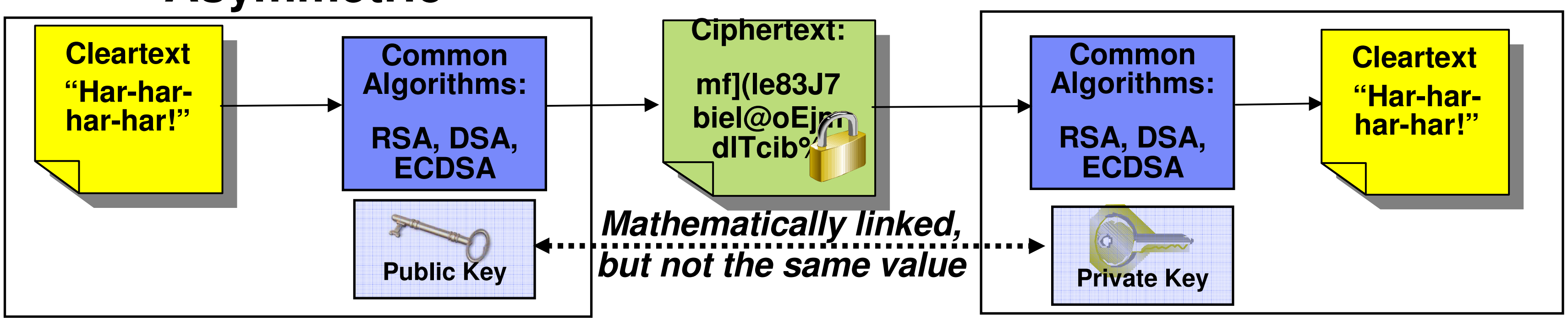
Symmetric and asymmetric encryption

Symmetric



- Only one key value - “shared secret” between both parties
  - Used for both encryption and decryption
  - Hence, the symmetry – each side has the same key
- Much faster than asymmetric cryptography
  - Symmetric cryptography typically used for most application payload encryption / decryption

Asymmetric



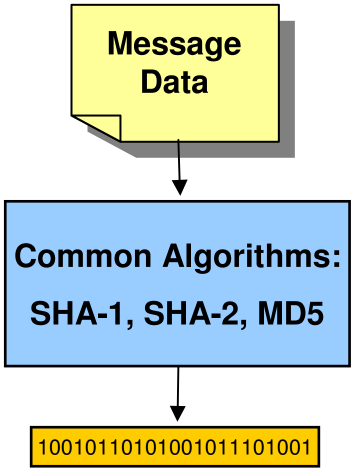
- Two different key values – no shared secrets!
  - Private key is known only to owner / Public key is freely distributed to others – typically in x.509 certs
- Data encrypted with private key can only be decrypted with public key and vice versa
- Great for authentication and non-repudiation - “digital signatures”
- Very expensive computationally compared to symmetric cryptography
  - Typically used to encrypt small data objects like message digests or symmetric keys

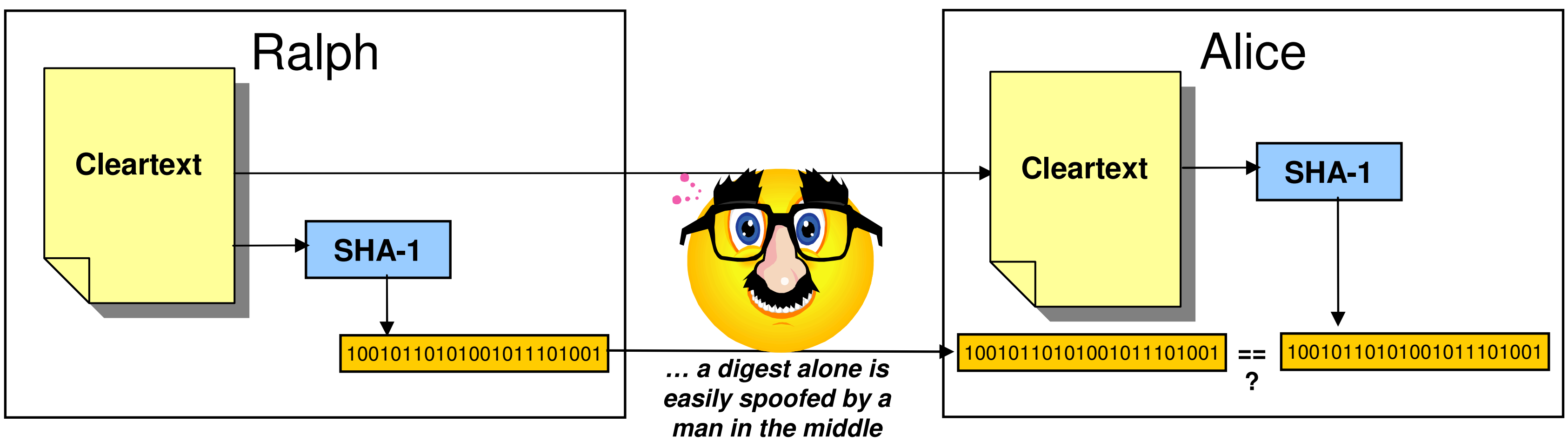
© 2013 IBM Corporation

Message digests

A message digest is…

- **NOT based on a secret key**
- **a fixed-length value generated from variable-length data**
- **unique:**
  - the same input data always generates the same digest value
  - small change in data generates a very different hash value
  - extremely difficult (and time consuming) to find two different data values that result in the same hash value
- **one-way: can't reverse a digest value back to the original data**
- **hence, also known as a "one-way hash"**
- **an element of proving data integrity and origin authentication (but not enough on its own…)**



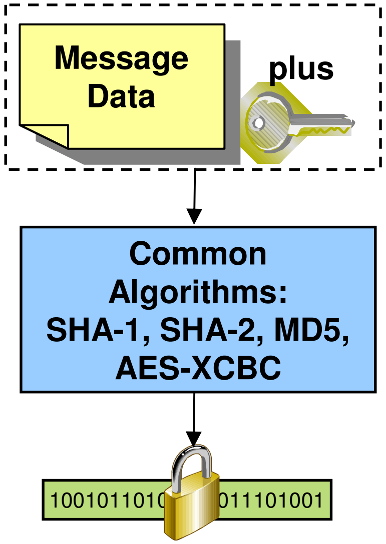


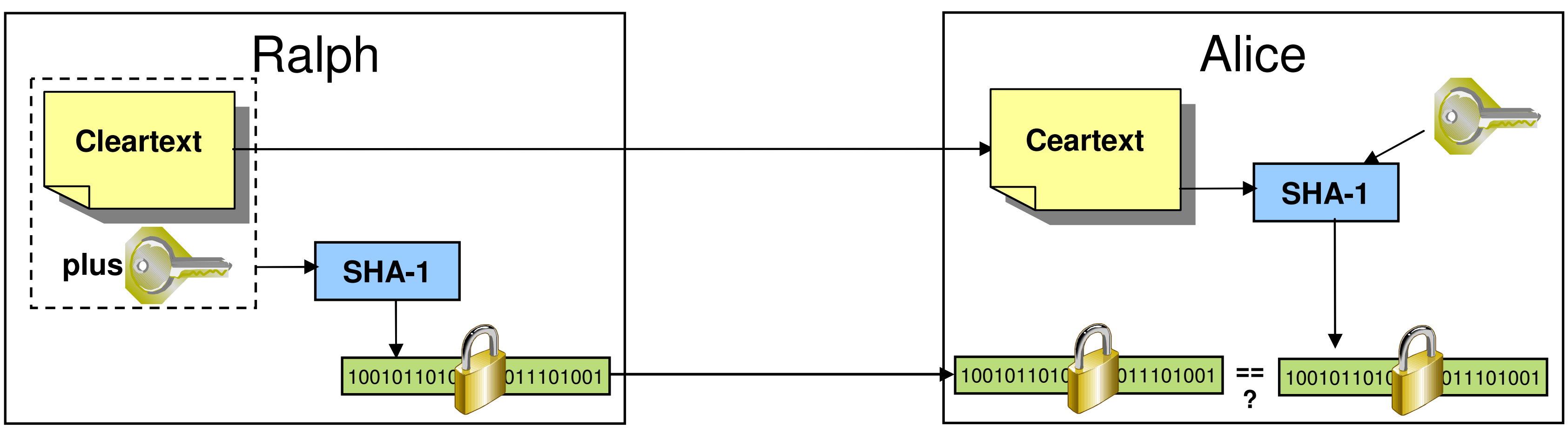
© 2013 IBM Corporation

Secure Message Authentication Codes (MACs)

A secure message authentication code is…

- **a message digest**
- **generated on a combination of**
  - **variable-length data**
  - **a secret (symmetric) key**
- **very good for**
  - **proving data integrity and**
  - **authenticating data origin**





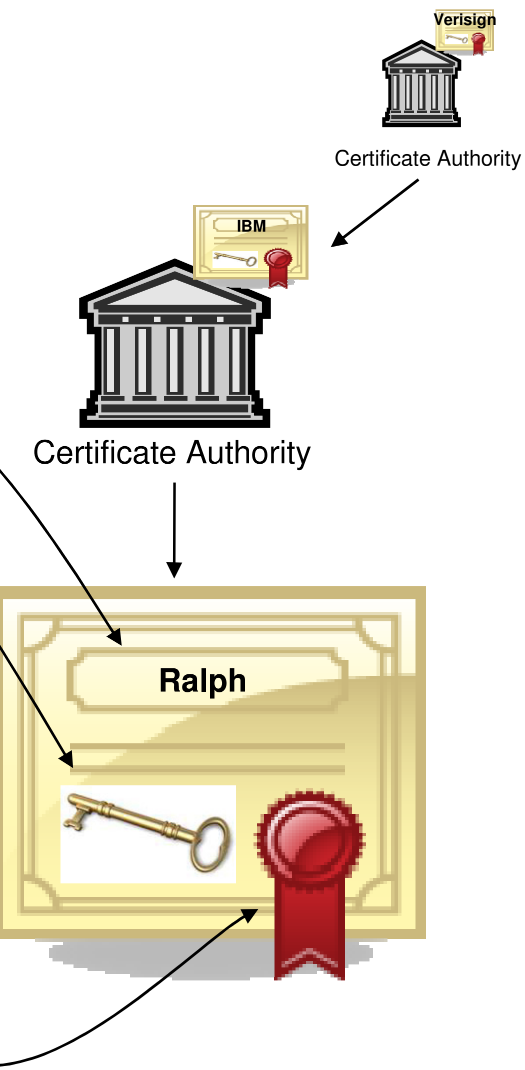
© 2013 IBM Corporation

What is a digital certificate?

- A **digital document** that…
  - Is issued by a trusted third party called a Certificate Authority (CA)
  - Identifies a subject
  - Contains:
    - cleartext (issuer, serial number, and so forth)
    - the subject's public key
    - a signed hash of the cleartext (signed by the issuer) – proves certificate's validity

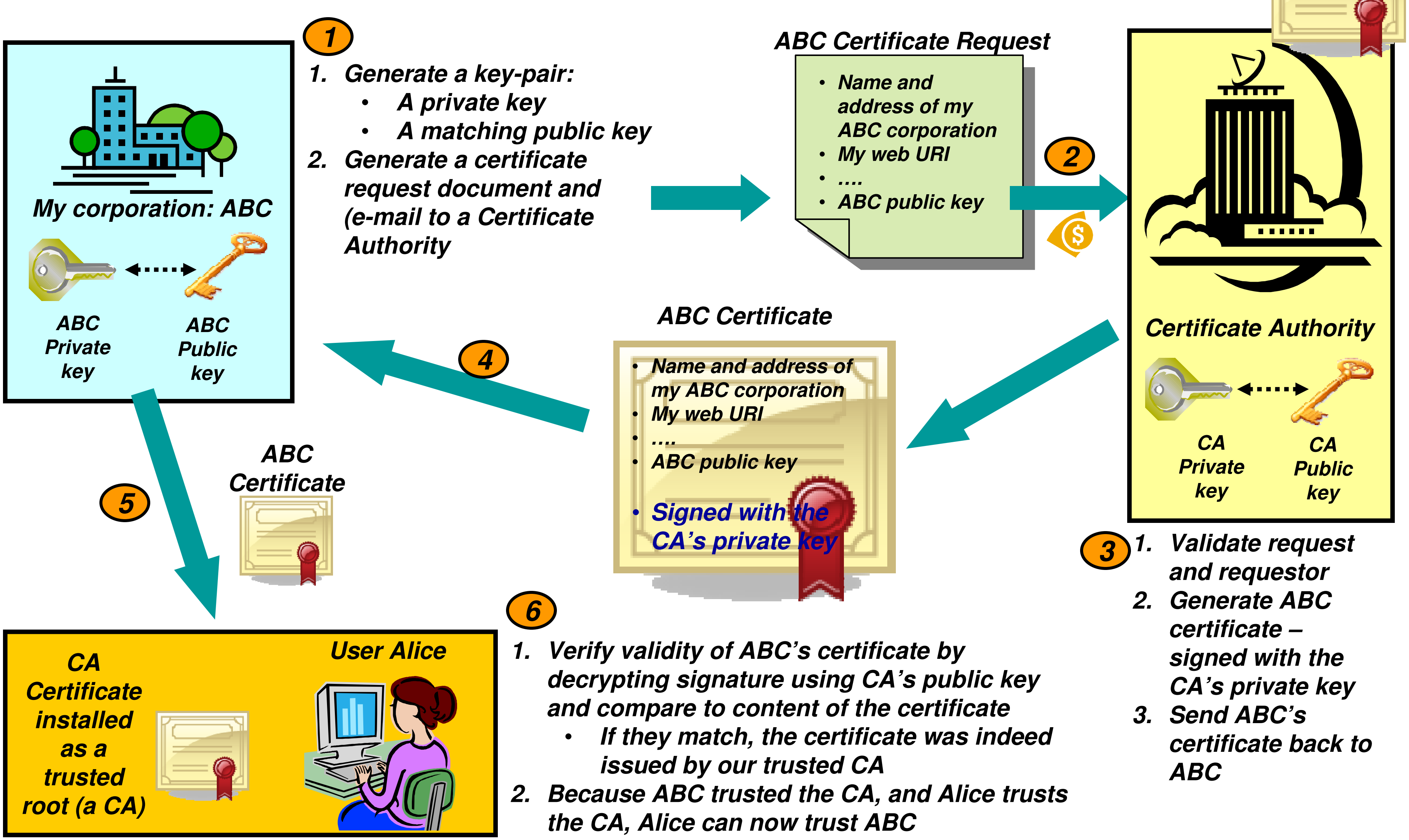
- …which is **used to**…
  - Prove the subject's identity
  - Bind that identity to an asymmetric key pair
  - Distribute the public key

- …and is **part of a trust hierarchy**
  - CA's (issuer) have their own certificates. (well-known CA certs are distributed with Web browsers).
  - CA's can be arranged hierarchically (the top of the hierarchy is the "root CA").
  - Part of a Public Key Infrastructure (PKI).
  - To prove an identity, you check the peer's certificate and verify that it was signed by a CA that you trust.



© 2013 IBM Corporation

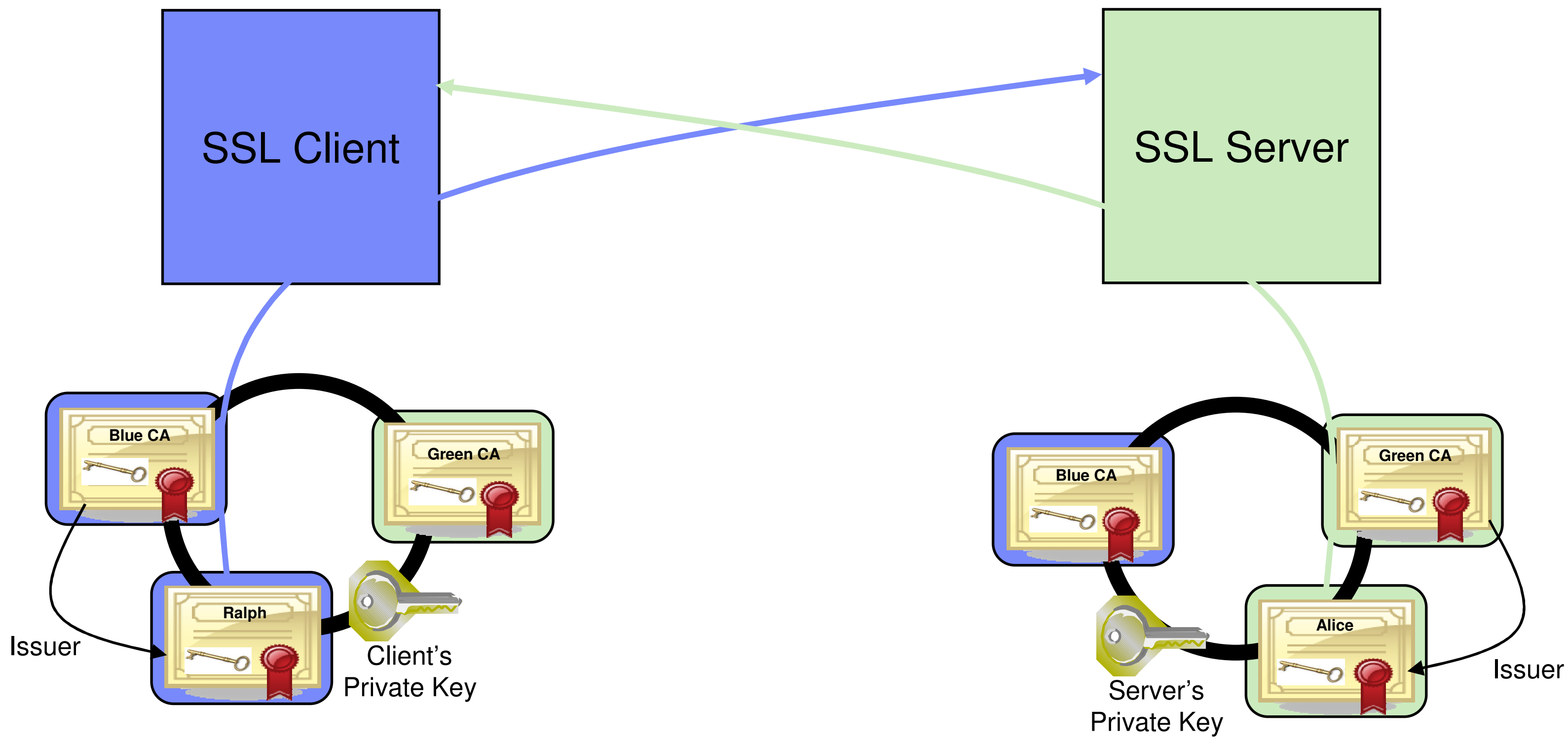
Trust relationships and Certificate Authorities
(or, where do certificates come from?)



© 2013 IBM Corporation

Certificates in action: SSL Client Authentication

- Implies SSL server authentication
- Very similar to Internet Key Exchange (IKE) authentication used for IPsec



© 2013 IBM Corporation

What is FIPS 140?

- **United States Federal Information Processing Standards (FIPS) are written for a wide variety of information technologies:**
  - From punched card codes to COBOL language standards to rules on the use of cryptographic technologies
  - Many of these standards are now focused on cryptography

- **FIPS 140: "Security Requirements for Cryptographic Modules"**
  - Applies only to "Cryptographic Modules" – not whole systems or even applications
  - Originally written for hardware devices. Later extended to software modules
  - Covers:
    - Clearly defining and documenting the boundaries and interfaces of "cryptographic modules"
    - Ensuring integrity of crypto algorithms (signed binaries, self-test, environment, and so on)
    - Limits supported algorithms (for example, MD5, DES, 512-bit RSA, some AES modes are not allowed)
    - Ensures security of keys and key management
    - Other things that don't affect this discussion, such as roles, physical characteristics of hardware modules, and so on
  - Current version is FIPS 140-2. FIPS 140-3 is out for review
  - The US government as well as others expect cryptographic modules to meet the FIPS 140 specifications.

© 2013 IBM Corporation

Agenda

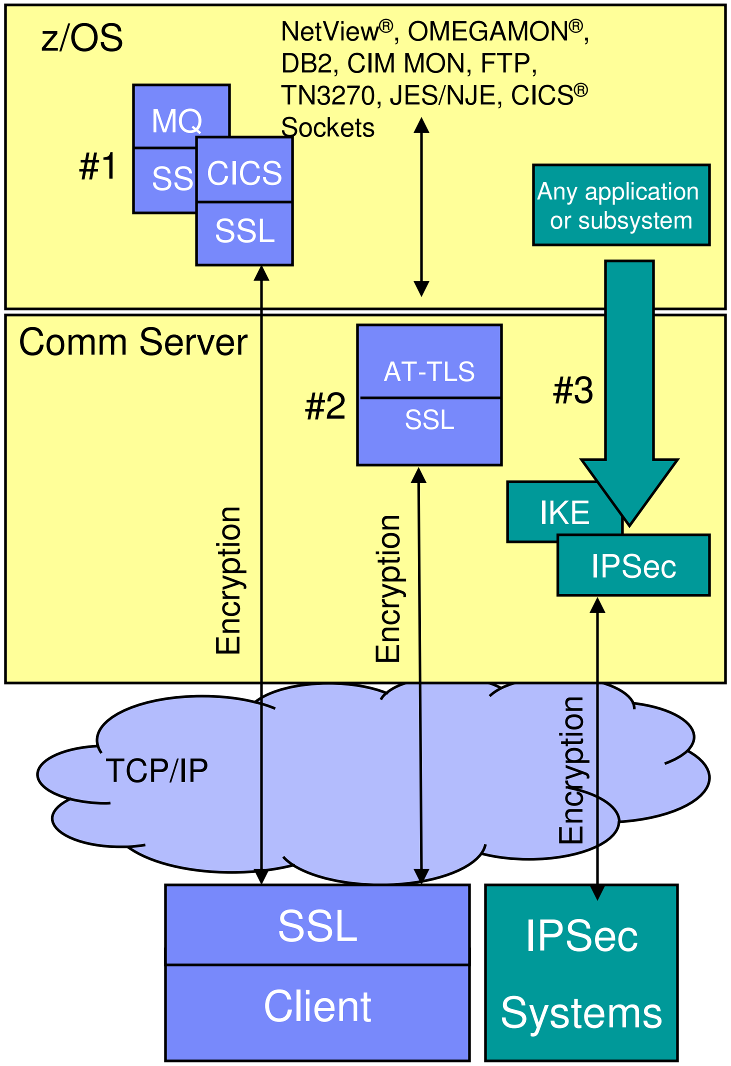
- Review of basic cryptographic operations
  - Symmetric cryptography
  - Asymmetric cryptography
  - Message digests and secure message authentication codes
  - Digital certificates
  - FIPS 140
- **z/OS TCP/IP network security protocols**
  - **SSL/TLS**
  - **AT-TLS**
  - **IPSec and IKE**
- Relevant System z & z/OS cryptographic componentry
  - Hardware components
  - Software components
  - Communications Server usage
- Conclusion

© 2013 IBM Corporation

z/OS TCP/IP secure networking protocols

- **z/OS TCP/IP cryptographically protects network data in three ways:**
  - **#1 Secure Sockets Layer (SSL) and Transport Layer Security (TLS) through System SSL**
    - Application is explicitly coded to use these
    - Per-session protection
    - TCP only
  - **#2 Application Transparent TLS (AT-TLS)**
    - TLS applied in transport layer (TCP) as defined by policy
    - Typically applied transparently to application
    - TCP/IP stack is user of System SSL services
  - **#3 IP Security (IPSec) and Internet Key Exchange (IKE)**
    - "Platform to platform" encryption
    - IPSec implemented at the IP layer as defined by policy
    - Wide variety (any to all) of traffic is protected
    - Completely transparent to application
    - IKE allows IPSec security associations to be established dynamically

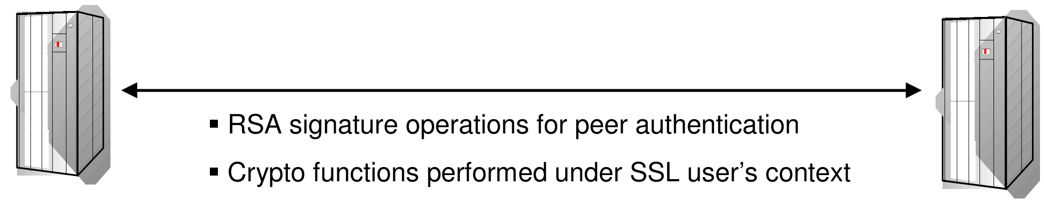
- **When do you use one form versus another?**
  - Depends on client, application, topology, performance requirements, and so forth.
  - Beyond scope of this presentation



© 2013 IBM Corporation

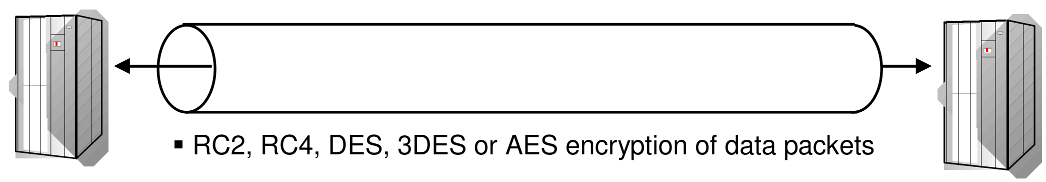
Establishing SSL/TLS sessions

1 SSL handshake identifies and authenticates SSL client and server and negotiates cipher suite to be used for data protection



- RSA signature operations for peer authentication
- Crypto functions performed under SSL user's context

2 Data flows through protected session using symmetric encryption and message authentication negotiated during handshake

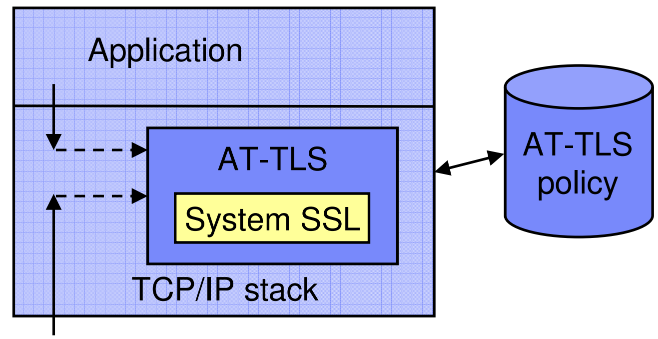


- RC2, RC4, DES, 3DES or AES encryption of data packets
- MD5 or SHA-1 for packet authentication
- All of this is performed under SSL user's context

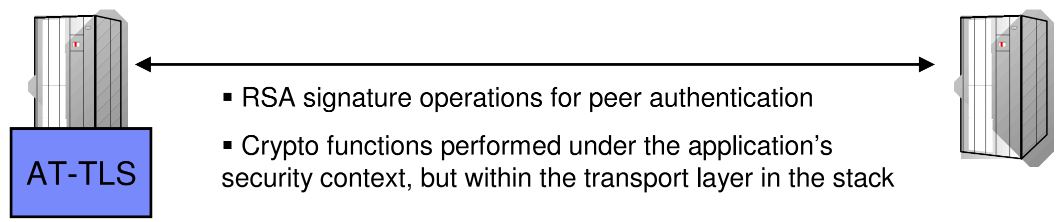
© 2013 IBM Corporation

AT-TLS sessions

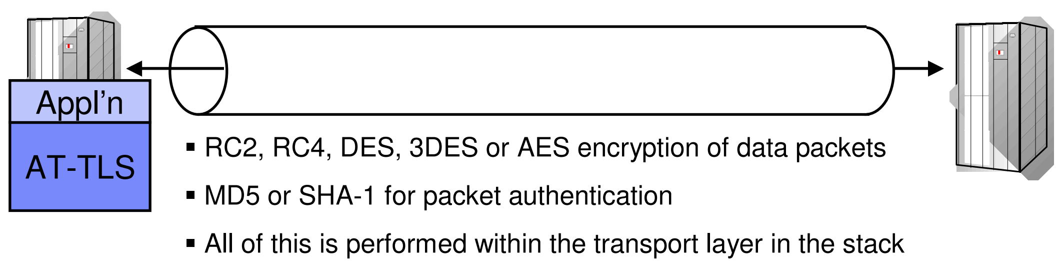
1 A z/OS application issues a connect() or accept() on a socket to establish a new outbound or inbound connection, respectively. Within the transport layer of the stack, AT-TLS policy is consulted to decide if TLS protection is configured for this traffic. If so, the stack's AT-TLS support establishes the TLS connection…



2 AT-TLS directs the SSL handshake. All identities, cipher suites, etc. are defined in AT-TLS policy. Note that sessions established by AT-TLS on z/OS interoperate seamlessly with "regular" TLS applications on remote nodes.



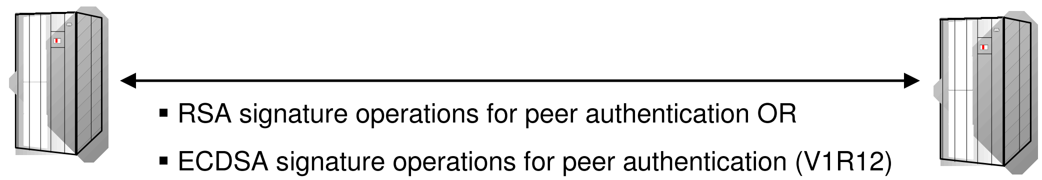
3 AT-TLS takes outbound cleartext and sends it over the TLS-protected session. Likewise, it receives encrypted data off the session and presents it to the application as cleartext. Many applications never know the TLS session exists, although some may want/need to (AT-TLS aware, AT-TLS controlling)



© 2013 IBM Corporation

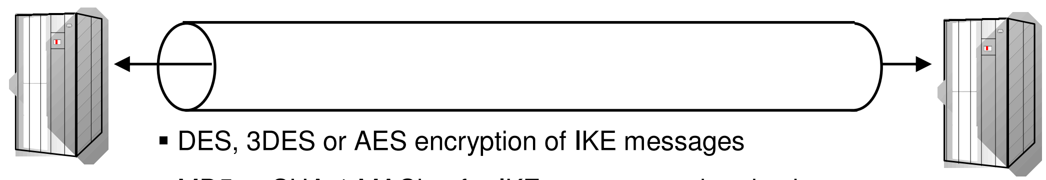
Creating IPSec Security Associations (SAs)

1 IKE peers negotiate an IKE ("phase 1") tunnel (one bidirectional SA) over an unprotected UDP socket.



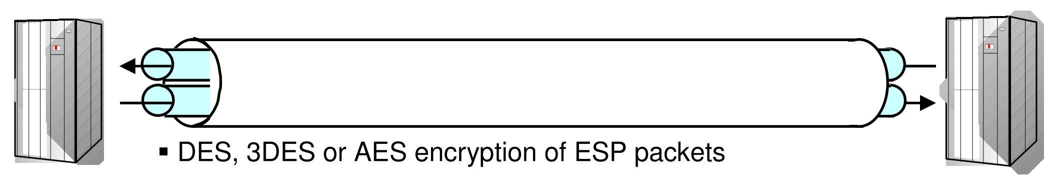
- RSA signature operations for peer authentication OR
- ECDSA signature operations for peer authentication (V1R12)
- Diffie-Hellman based symmetric key generation
- IKE and (in some cases) NSS invoke crypto operations

2 IKE peers negotiate IPSec ("phase 2") tunnel (two unidirectional SAs) under protection of the IKE tunnel



- DES, 3DES or AES encryption of IKE messages
- MD5 or SHA-1 MACing for IKE message authentication
- SHA-2 or AES-based MACing for IKE message authentication (V1R12)
- IKE and (in some cases) NSS invoke crypto operations

3 Data flows through IPSec tunnel using Authentication Header (AH) and/or Encapsulating Security Payload (ESP) protocol



- DES, 3DES or AES encryption of ESP packets
- MD5 or SHA-1 MACing for AH and ESP packet authentication
- SHA-2 or AES-based MACing for AH and ESP packet authentication (V1R12)
- TCP/IP stack invokes crypto operations

© 2013 IBM Corporation

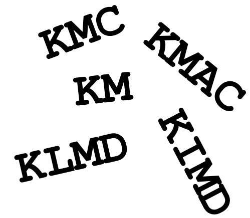
Agenda

- Review of basic cryptographic operations
  - Symmetric cryptography
  - Asymmetric cryptography
  - Message digests and secure message authentication codes
  - Digital certificates
  - FIPS 140
- z/OS TCP/IP network security protocols
  - SSL/TLS
  - AT-TLS
  - IPSec and IKE
- **Relevant System z & z/OS cryptographic componentry**
  - **Hardware components**
  - **Software components**
  - **Communications Server usage**
- Conclusion

© 2013 IBM Corporation

zEC12, z196/z114, z10, z9 Hardware Cryptographic components*

- **CP Assist for Cryptographic Function (CPACF)**
  - Hardware assist for specific System z instructions that perform cryptographic primitives (DES, 3DES, AES-CBC encrypt/decrypt and SHA-1, SHA-2 hashing)
  - Available on general processors as well as zIIPs
  - Accessed directly through z series instruction set or through ICSF
  - Clear keys only (unencrypted key is kept in storage)
  - Available on zEC12, z196/z114, z10, z9 and z890/z990



- **Cryptographic adapters (Crypto Express4, for example)**
  - Accelerators (CEX4A, for example)
    - Performs RSA encrypt/decrypt and RSA signature operations
    - Accessed through ICSF
    - Clear keys only
  - Coprocessors (CEX4C, for example)
    - Focus on secure keys (no unencrypted keys in storage) and tamper detection and countermeasures
    - Provides RSA acceleration as well (slower than accelerators, though)
    - Accessed through ICSF
  - Crypto Express4 also provides a secure key PKCS#11 mode (CEX4P)

- **zEC12, z196/z114, z10 or z9 Integrated Information Processor (zIIP)**
  - Can be tasked to perform some crypto-intensive portions of IPSec processing

* - capabilities are described relative to their usage by z/OS Communications Server and by System SSL only

© 2013 IBM Corporation

z/OS Software Cryptographic components (1 of 2)

- **z/OS Cryptographic Services**

  – **Integrated Cryptographic Service Facility (ICSF)**
    - z/OS component that provides secure, high-speed cryptographic services
    - Offers a full suite of cryptographic primitives
    - Provides all application access to z/OS hardware crypto features
    - Starting in V1R12, offers a FIPS 140 mode through its PKCS #11 interface

  – **System SSL**
    - z/OS component that provides SSL, TLS implementations
    - Also provides a set of X.509 certificate-related APIs, including RSA and ECDSA (V1R12) signature generation and verification. These APIs are used by other components like IKED and NSSD
    - Contains own software implementations of most crypto algorithms
    - Makes use of cryptographic adapters through ICSF
    - Uses CPACF instructions directly
    - Starting in V1R11, offers a FIPS 140 mode

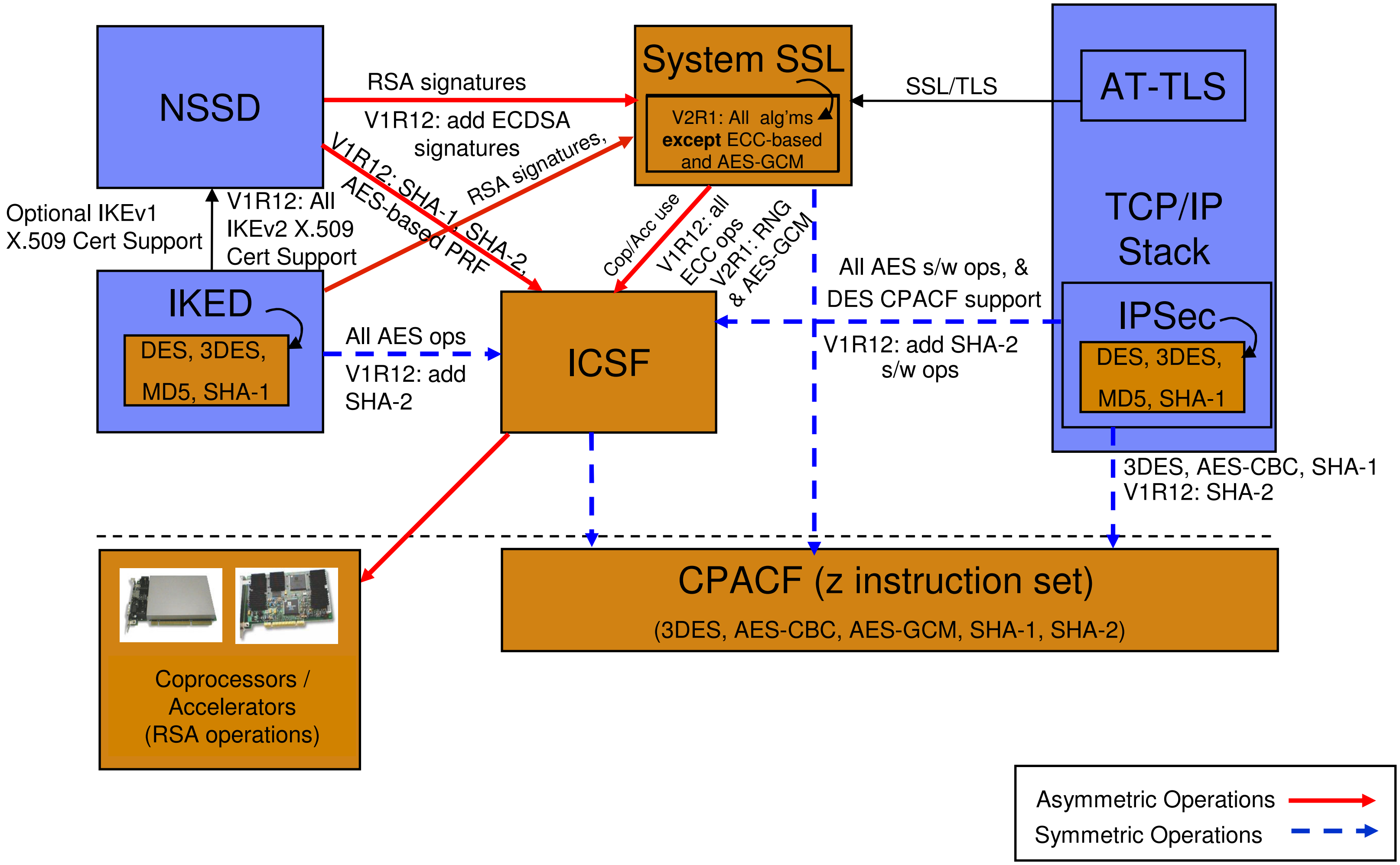
© 2013 IBM Corporation

z/OS Software Cryptographic components (2 of 2)

- **z/OS Communications Server**
  - **TCP/IP stack implements:**
    - Application Transparent TLS
    - IPsec (Authentication Header (AH) and Encapsulating Security Payload (ESP))
  - **Internet Key Exchange daemon (IKED) implements:**
    - IKEv1 and IKEv2 (V1R12) protocols
  - **TCP/IP stack's IPsec support and IKED both contain software implementations of many algorithms**
    - Both use hardware crypto facilities to varying degrees
    - Both offer a new FIPS 140 mode under which only FIPS 140 mode crypto modules are used. (V1R12)
  - **Network security services daemon (NSSD) performs certificate-based operations on behalf of IKED**
    - Optional for IKEv1, mandatory for IKEv2 (V1R12)
    - Also offers a FIPS 140 mode (V1R12)

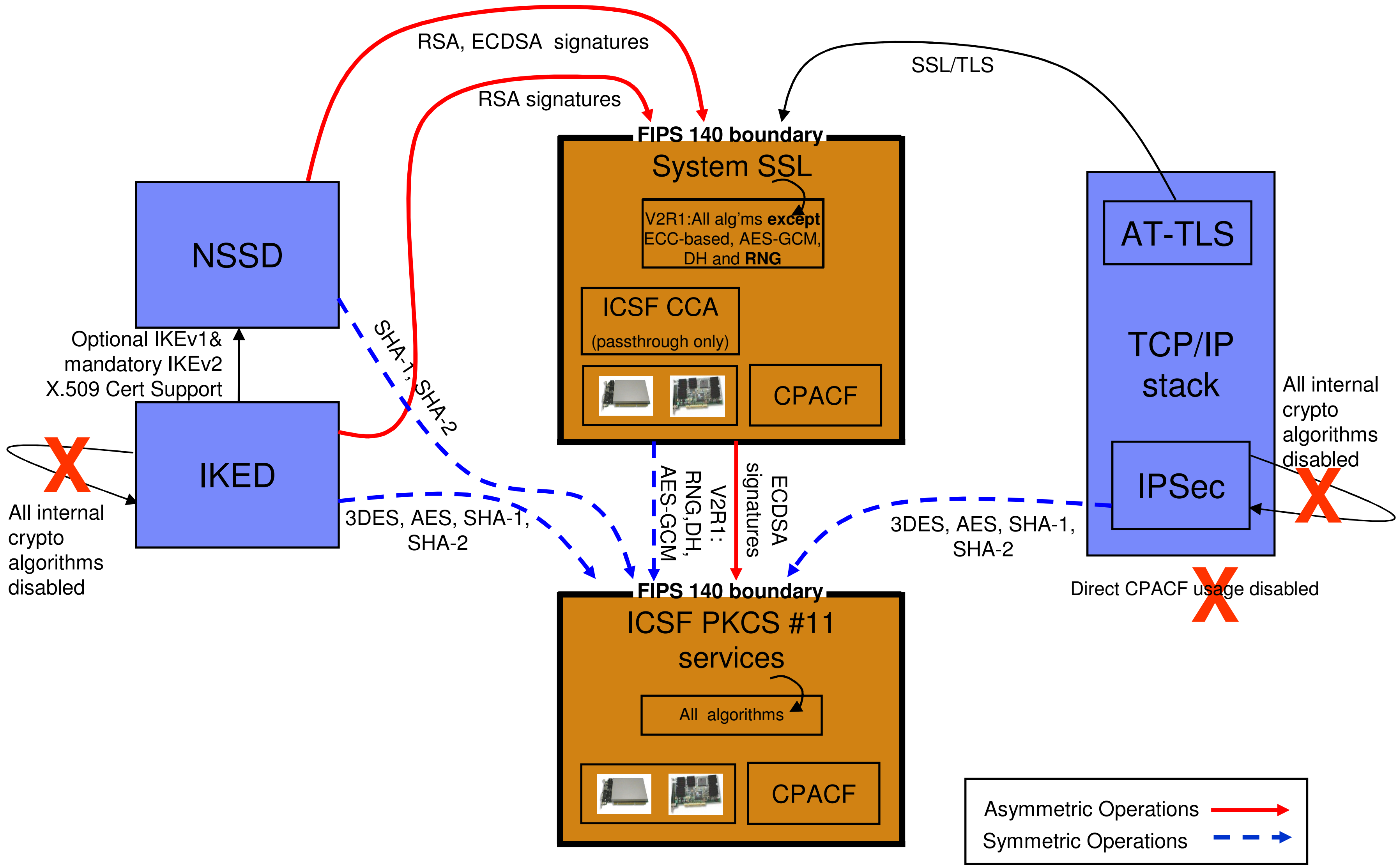
© 2013 IBM Corporation

z/OS TCP/IP Cryptographic Landscape (non-FIPS)



© 2013 IBM Corporation

z/OS TCP/IP Cryptographic Landscape (FIPS mode)



© 2013 IBM Corporation

SSL/TLS (and AT-TLS) hardware crypto usage

Crypto Type	Algorithm	CPACF only	CPACF + Crypto Express card
Asymmetric Encrypt/Decrypt	RSA signature generation	In software	In coprocessor (non-FIPS) or CEX4P (FIPS or non-FIPS), else in software.
	RSA signature verification	In software	In coprocessor or accelerator, else in software
	RSA encrypt for handshake	In software	In coprocessor or accelerator, else in software
	RSA decrypt for handshake	In software	In coprocessor, accelerator or CEX4P
	ECDSA signature generation	In software	In coprocessor on z10, z196/z114, zEC12 or CEX4P, else in software
	ECDSA signature verification	In software	In software
Symmetric Encrypt/Decrypt	DES	CPACF (non-FIPS mode only: DES not allowed in FIPS mode)	
	3DES	CPACF	
	AES-CBC-128	CPACF	
	AES-CBC-256	CPACF on z10, z196/z114, zEC12, in software on z9	
	AES-GCM-128, AES-GCM-256	CPACF on z196/z114, zEC12, in software on z9, z10	
Symm Auth	MD5	In software (non-FIPS mode only: MD5 not allowed in FIPS mode)	
	SHA-1	CPACF	
	SHA-224, SHA-256	CPACF	
	SHA-384, SHA-512	CPACF on z10, z196/z114, zEC12, in software on z9	

© 2013 IBM Corporation

IKED hardware crypto usage (IKE)

- **RSA signature generate, signature verify for peer authentication**
- **DES, 3DES, AES encryption of IKE payloads**
- **SHA-1 and MD5 HMACs for IKE message authentication**
- **SHA-2 HMACs and AES-XCBC MAC for IKE message authentication (V1R12)**

Crypto Type	Algorithm	CPACF available only	CPACF + Coprocessor/Accelerator*
Asymmetric Enc/Dec	Diffie-Hellman (MODP)	In software via System SSL	In software via System SSL
	EC Diffie-Hellman (requires ICSF) **	In software via ICSF	In software via ICSF
	RSA signature generation (clear key only)	In software via System SSL	In Coprocessor (non-FIPS mode only ***), else in software via System SSL
	RSA signature verification	In software via System SSL	In Coprocessor/Accelerator
Symmetric Enc/Dec	DES	In software (non-FIPS mode only: DES not allowed in FIPS mode) ***	
	3DES	In software (non-FIPS mode), via CPACF via ICSF (FIPS mode) ***	
	AES-CBC-128 (requires ICSF)	In CPACF via ICSF	
	AES-CBC-256 (requires ICSF) **	In software on z9, CPACF in z10, z196/z114, zEC12 all via ICSF	
Symmetric Authentication	SHA-1	In software (non-FIPS mode), via CPACF via ICSF (FIPS mode) ***	
	SHA-256 (requires ICSF) **	In CPACF via ICSF	
	SHA-384, -512 (requires ICSF) **	In software on z9, CPACF in z10, z196/z114, zEC12 all via ICSF	
	AES-XCBC (requires ICSF) **	In software via ICSF (non-FIPS mode only: FIPS 140 doesn't allow algorithm) ***	
	MD5	In software (non-FIPS mode only: FIPS 140 doesn't allow algorithm) ***	

* IKED does not support PKCS#11 tokens or CEX4P ** New algorithm for V1R12 *** New with V1R12 FIPS 140 support

© 2013 IBM Corporation

NSSD hardware crypto usage (IKE)

- **RSA and ECDSA (V1R12) signature generate, signature verify for peer authentication**
- **SHA-1 and MD5 HMACs used in digital signature operations**
- **SHA-2 HMACs and AES-XBC MAC for IKE message authentication (V1R12)**

Crypto Type	Algorithm	CPACF only	CPACF + Coprocessor/Accelerator*
Asymmetric Encrypt/Decrypt	RSA signature generation (clear key only)	In software via System SSL	In coprocessor (non-FIPS mode only ***), else in software via System SSL
	RSA signature verification	In software via System SSL	In coprocessor/accelerator
	ECDSA signature generation **	In software via System SSL	In coprocessor on z10, z196/z114, zEC12, else in software
	ECDSA signature verification **	In software via System SSL	In software via System SSL
Hashing for digital signatures	SHA-1	In CPACF via ICSF	
	SHA-256 (requires ICSF) **	In CPACF via ICSF	
	SHA-384, -512 (requires ICSF) **	In software on z9, CPACF in z10, z196/z114, zEC12 all via ICSF	
	AES-XCBC (requires ICSF) **	In software via ICSF (non-FIPS mode only: FIPS 140 doesn't allow algorithm) ***	
	MD5	In software via ICSF (non-FIPS mode only: FIPS 140 doesn't allow algorithm) ***	

* NSSD does not support PKCS#11 tokens or CEX4P   ** New algorithm for V1R12   *** New with V1R12 FIPS 140 support

© 2013 IBM Corporation

Stack hardware crypto usage (IPSec: AH, ESP): Non-FIPS 140 mode

- **DES, 3DES, AES encryption of data traffic**
- **SHA-1 and MD5 HMACs for message authentication**
- **SHA-2 HMACs, AES-XCBC, and AES-GMAC MACs for message authentication (V1R12)**
- **All SRB-based processing in stack, *including these crypto operations*, can be offloaded to zIIP to reduce cost of IPSec protection.**

Crypto Type	Algorithm	CPACF (stack doesn't use crypto adapters)
Symmetric Enc/Dec	DES	In CPACF (via ICSF)
	3DES	In CPACF
	AES-CBC-128	In CPACF
	AES-CBC-256 *	In software via ICSF on z9, CPACF in z10, z196/z114, zEC12
	AES-GCM-128, -256 *	In software via ICSF
Symmetric Authentication	SHA-1	In CPACF
	SHA-256 *	In CPACF
	SHA-384, -512 *	In software via ICSF on z9, CPACF in z10, z196/z114, zEC12
	AES-XCBC MAC and AES-GMAC-128, -256 *	In software via ICSF
	MD5	In software

* New algorithm for V1R12

© 2013 IBM Corporation

Stack hardware crypto usage (IPSec: AH, ESP): FIPS 140 mode (V1R12)

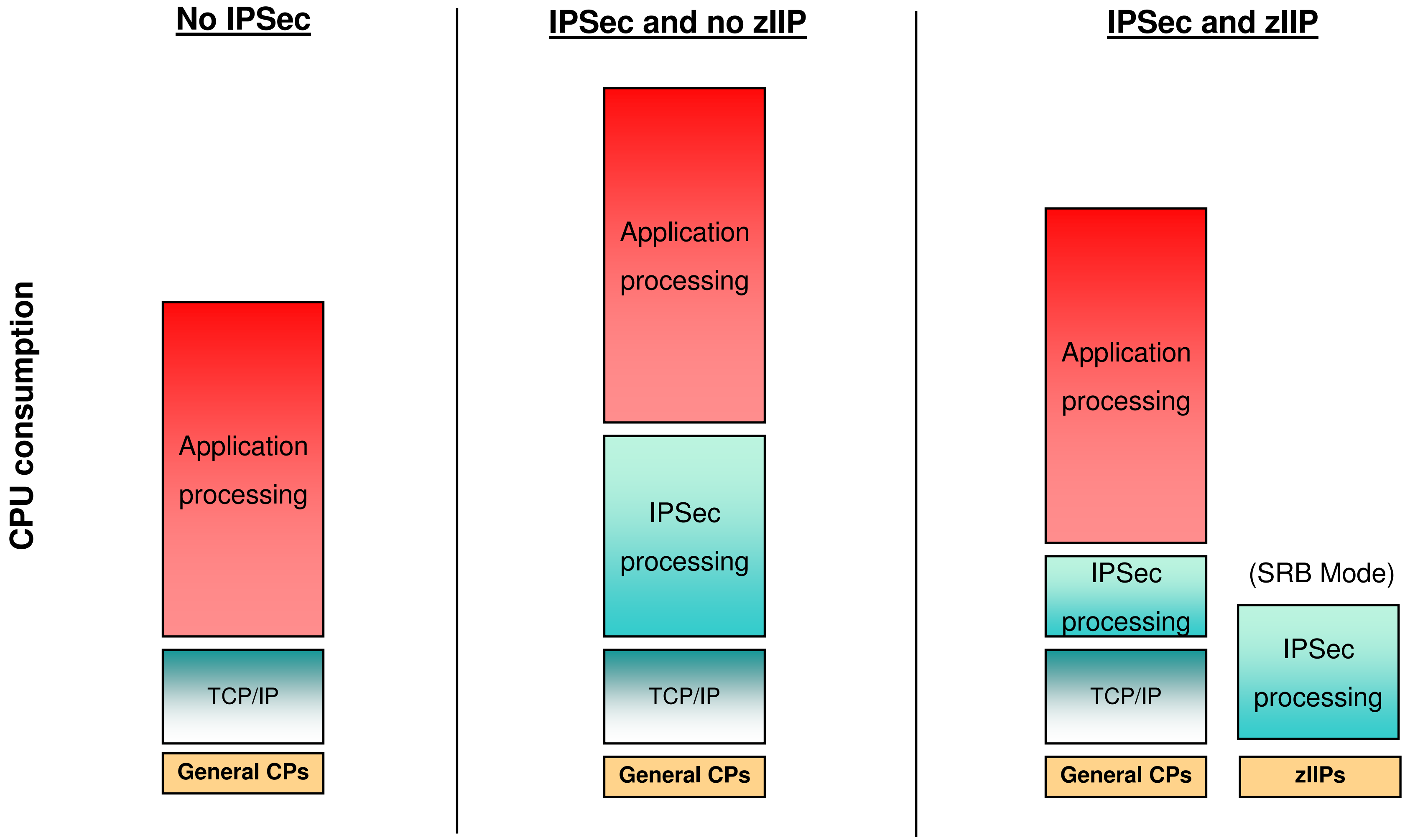
- **3DES, AES encryption of data traffic**
- **SHA-1 HMACs**
- **SHA-2 HMACs, AES-GMAC MACs for message authentication (V1R12)**
- **Note: FIPS 140 does not allow DES, MD5 or AES-XCBC**
- **All SRB-based processing in stack, *including these crypto operations*, can be offloaded to zIIP to reduce cost of IPSec protection.**

Crypto Type	Algorithm	CPACF (stack doesn't use crypto adapters)
Symmetric Enc/Dec	3DES	In CPACF via ICSF **
	AES-CBC-128	In CPACF via ICSF **
	AES-CBC-256 *	In software on z9, CPACF in z10, z196/z114, zEC12, all via ICSF **
	AES-GCM-128, -256 *	In software via ICSF **
Symmetric Authentication	SHA-1	In CPACF via ICSF **
	SHA-256 *	In CPACF via ICSF **
	SHA-384, -512 *	In software on z9, CPACF in z10, z196/z114, zEC12, all via ICSF **
	AES-GMAC-128, -256 *	In software via ICSF **

*** New algorithm for V1R12** **** New with V1R12 FIPS 140 support**

© 2013 IBM Corporation

IPSec processing using zIIP



- CPACF is exploited in the same manner on both the general CPs and the zIIPs
- Function enabled through a TCP/IP configuration keyword when zIIP hardware and pre-req software is in place

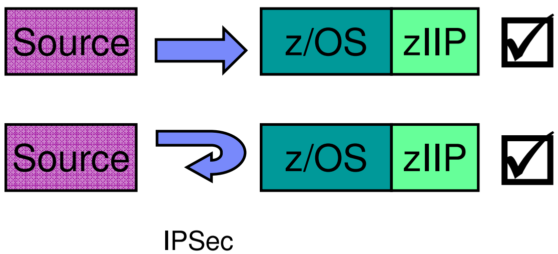
© 2013 IBM Corporation

What IPSec workload is eligible for zIIP?

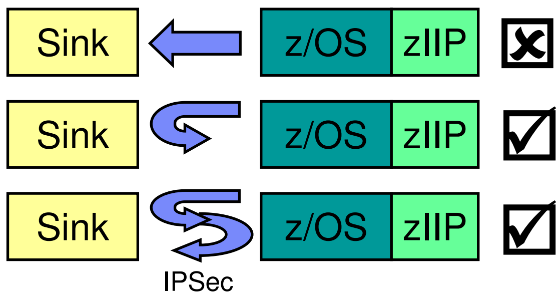
- **The zIIP assisted IPSec function is designed to move most of the IPSec processing from the general purpose processors to the zIIPs**

- **z/OS CS TCP/IP recognizes IPSec packets and routes a portion of them to an independent enclave SRB – this workload is eligible for the zIIP**

  – **Inbound operation (not initiated by z/OS)**
    - All inbound IPSec processing is dispatched to enclave SRBs and is eligible for zIIP
    - All subsequent outbound IPSec responses from z/OS are dispatched to enclave SRB.   This means that all encryption/decryption of message integrity and IPSec header processing is sent to zIIP



  – **Outbound operation (initiated by z/OS)**
    - Operation which starts on a TCB is not zIIP eligible
    - BUT… any inbound response or acknowledgement is SRB-based and therefore zIIP eligible
    - AND… all subsequent outbound IPSec responses from z/OS are also zIIP eligible



© 2013 IBM Corporation

Agenda

- Review of basic cryptographic operations
  - Symmetric cryptography
  - Asymmetric cryptography
  - Message digests and secure message authentication codes
  - Digital certificates
  - FIPS 140
- z/OS TCP/IP network security protocols
  - SSL/TLS
  - AT-TLS
  - IPSec and IKE
- Relevant System z & z/OS cryptographic componentry
  - Hardware components
  - Software components
  - Communications Server usage
- **Conclusion**

© 2013 IBM Corporation

Conclusion

- System z and z/OS offer a rich set of cryptographic features
- z/OS TCP/IP support provides a rich set of secure networking protocols
- The combination of the two provides a powerful set of capabilities for securing your TCP/IP network traffic
- The combinations are numerous
- The z platform continues to focus on improving secure TCP/IP networking capability and performance

© 2013 IBM Corporation

z/OS Communications Server on the Web

URL	Content
http://www.twitter.com/IBM_Commserver	IBM Communications Server on twitter
http://www.facebook.com/IBMCommserver	IBM Communications Server on facebook
http://www.youtube.com/user/zOSCommServer	IBM Communications Server on YouTube
http://tinyurl.com/zoscsblog	IBM Communications Server blog
http://www.ibm.com/systems/z/	IBM System z in general
http://www.ibm.com/systems/z/hardware/networking/	IBM Mainframe System z networking
http://www.ibm.com/software/network/commserver/	IBM Software Communications Server products
http://www.ibm.com/software/network/commserver/zos/	IBM z/OS Communications Server
http://www.ibm.com/software/network/ccl/	IBM Communication Controller for Linux on System z
http://www.redbooks.ibm.com	ITSO Redbooks
http://www.ibm.com/software/network/commserver/zos/support/	IBM z/OS Communications Server technical Support – including TechNotes from service
http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs	Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
http://www.ibm.com/systems/z/os/zos/bkserv/	IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server

© 2013 IBM Corporation

Please fill out your session evaluation

- z/OS Communications Server TCP/IP Cryptography Demystified
- Session # 13543
- QR Code:

© 2013 IBM Corporation