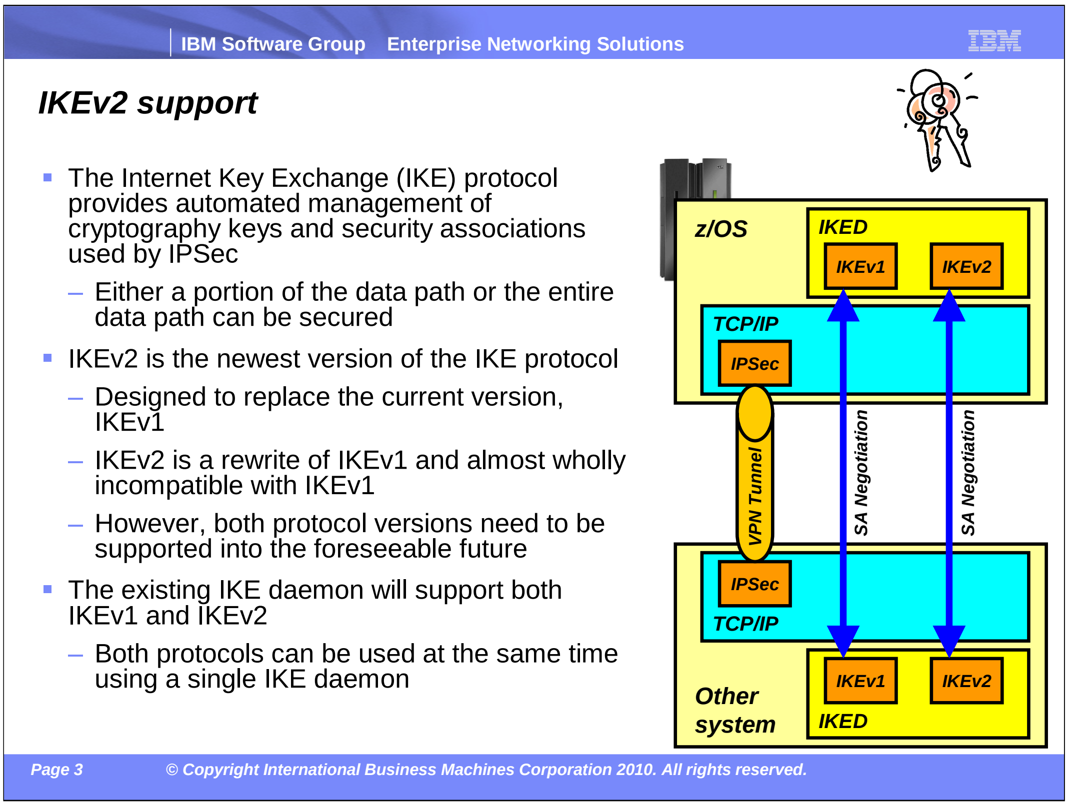
This presentation provides an overview of the new security functions in z/OS V1R12 Communications Server.

Security

- IKE version 2 support is easier to configure and deploy
- IKE and IPSec FIPS-140 mode
- IPSec support for certificate trust chains and certificate revocation lists
- IPSec support for cryptographic currency
  - IKE version 2 support for elliptic curve digital signature algorithm (ECDSA)
  - New certificate encoding types
  - Support for new encryption and authentication algorithms in IKED and IPSec - required for US Government compliance
- Enforce RFC 4301 compliance for IPSec filter rules
  - No longer possible to configure non-compliant policies in R12
- Trusted TCP connections by obtaining security credentials of connection partners within a Sysplex

There are many new security functions in z/OS V1R12 Communications Server. IKED now supports IKE version 2 in addition to IKE version 1. Both IKE and IPSec can be configured in FIPS-140 mode. IPSec has added support for certificate trust chains and certificate revocation lists. New cryptographic algorithms and encodings are supported in IKED and IPSec. z/OS no longer supports IPSec filter rules that are non-complaint with RFC 4301. And applications can exploit trusted TCP connections to obtain security credentials of connection partners within a sysplex.



IKEv2 is an improvement over IKEv1 in many ways. It has better performance characteristics because it was designed to use fewer messages to establish and rekey tunnels. It also has better operational characteristics than IKEv1 because its designers had the experience of IKEv1 to build on. It was designed to solve some of the problems that plagued IKEv1.

Industry standards for IPv6 implementations include IKEv2 support. Both the DoD and NIST require compliant systems to support IKEv2. US Government agencies, and vendors who do business with them, might be expected to use USGv6 compliant systems, and to use IKEv2 to establish secure communications with them.

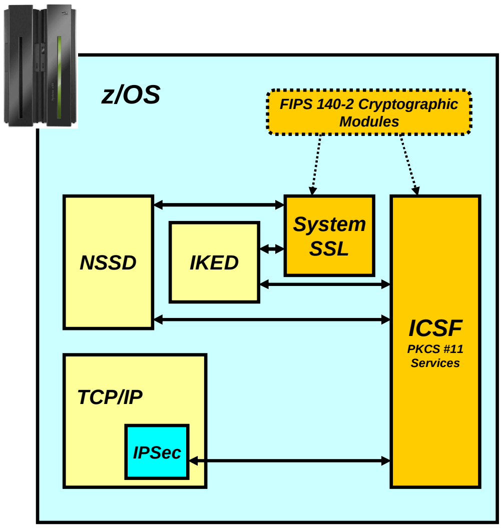
In order to include z/OS in bids for government IT projects, the z/OS IPSec function is enhanced to support IKEv2, in addition to its current IKEv1 support. The IKEv2 support for z/OS affects multiple z/OS components, as listed on this slide.

The IKE daemon (IKED) supports the IKEv2 protocol in addition to the IKEv1 protocol for dynamic management of security associations. However, it has a stronger dependence on an NSS Server for certificate services.

The Network Security Services (NSS) server daemon (NSSD) plays a larger role for IKEv2 by providing advanced certificate services to the IKE daemons. NSSD now performs HTTP retrieval of certificates and certificate bundles, and trust chain and certificate revocation processing.

IKE, IPSec, and NSS FIPS 140 mode

- FIPS 140 defines requirements and standards for cryptographic modules used within the US Government and elsewhere
  - Applies to cryptographic modules – not systems or applications
  - On z/OS, both System SSL and ICSF's PKCS #11 services are designed to address FIPS 140-2 requirements
- IKE, IPSec and NSS offer an optional FIPS 140 mode
  - When enabled, all IKE, IPSec and NSS IPSec-related crypto operations are performed through FIPS 140 mode System SSL or ICSF calls
  - TCP/IP stacks are individually enabled
  - IKED must be configured for FIPS 140 mode if any TCP/IP stack is enabled for FIPS 140 mode
- FIPS 140 mode reflected in the NMI



FIPS stands for "Federal Information Processing Standards." The standards cover a wide variety of topics.

Documents of this nature are often based on existing standards adopted by the wider IT community, or become the source of new standards for the community. FIPS 140 (currently version FIPS 140-2) deals with cryptographic modules, and imposes security requirements in 11 different areas. In z/OS V1R12, IKE, IPSec and NSS offer an optional FIPS 140 cryptographic operational mode.

There are three major components of z/OS IPSec. The primary purpose of the IKE daemon (IKED) is to negotiate SA parameters and manage cryptographic keys. The TCP/IP stack manages data protection SAs and performs some encryption and decryption. The Network Security Services daemon (NSSD) provides remote IPSec monitoring capability and certificate services.

In FIPS 140 cryptographic mode, all cryptographic operations must be performed by FIPS 140 cryptographic modules and take place inside a logical cryptographic boundary.

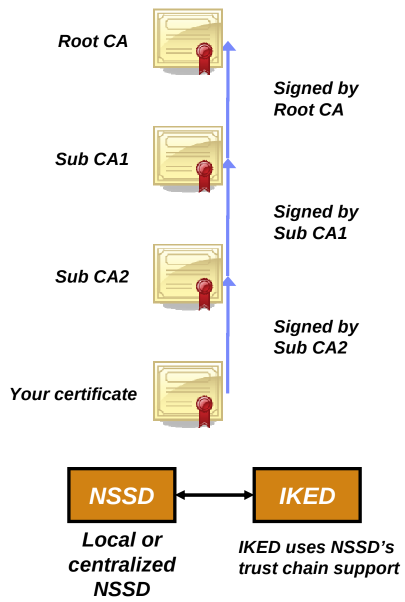
Therefore, when operating in FIPS 140 mode, the three z/OS IPSec components forward all cryptographic operation requests to cryptographic modules using FIPS 140 interfaces.

The two cryptographic modules used are z/OS System SSL and z/OS ICSF.

IBM Software Group Enterprise Networking Solutions

IPSec support for certificate trust chains

- RFC 4306 requires support for trust chains
  - NSSD is updated to provide support for trust chains
  - The maximum number of certificates supported in a trust chain is 32
- IKED is updated to exploit NSSD's trust chain support
  - IKED's local certificate processing is not updated to support trust chains
  - As a result, trust chain support in IKED will only be available to stacks that are configured as a network security client
  - When a stack is configured as a network security client, IKED will use trust chain support for both IKEv1 and IKEv2 exchanges

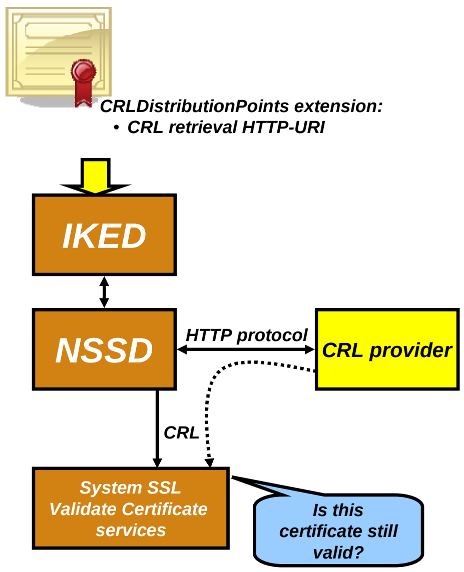


Page 5

A digital certificate is issued and signed by a certificate authority, or it can be self-signed. The **certificate authority** can be the root (originating) authority or a subordinate authority. Each certificate has a public/private key pair that is bound to its identity (the name of a person, company or an IP address). A **subordinate authority** has been delegated the responsibility to issue certificates on behalf of another certificate authority. An example is an enterprise that uses subordinate CAs to allow geographic regions to manage their own certificates. This can reduce the cost and time required to issue a new certificate. A certificate trust chain starts with the certificate that signed the end entity certificate (certificate that identifies the entity) and includes all signing certificates up to and including the trusted certificate authority (the root).

NSS is enhanced to support a certificate trust chain with a maximum number of 32 certificates. IKED using NSSD certificate services treats the payload as a request for IKEv1. Or it treats the payload as a hint for IKEv2 to select an EE certificate within the trust chain of the CA whose public key hash is contained in the certificate payload.

IPSec support for certificate revocation lists (CRLs)



- When IPSec authenticates a digital signature, it needs to ensure the signing certificate is still valid
- NSSD will retrieve CRLs using information in the CRLDistributionPoints extension in a certificate
  - HTTP-URIs only
- NSSD will pass CRLs to System SSL
- System SSL will validate the certificate against the CRL
  - To ensure the certificate is still valid
    - Has not expired or been revoked
- NSSD will not support retrieval of CRLs from LDAP servers
- For IKEv2, IKED depends on NSSD for this function

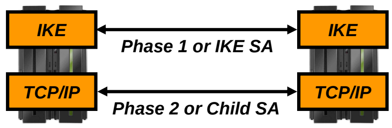
A certificate can be revoked for various reasons. For instance, the private key can be compromised, an affiliation can be terminated, or a certificate can no longer be valid for the stated purpose. In general, certificate revocation information should be consulted when validating a certificate; however, consulting revocation information can have performance implications. Certificate revocation lists (CRLs) are one method to obtain certificate revocation information.

IPsec must insure that all certificates are valid when it verifies a signature sent in the IKE flow. Support was added to NSSD to retrieve certificate revocation lists (CRLs) referenced in the certificate's CRLDistribiutionPoint extension. The retrieved CRLs along with the certificate trust chain are passed into System SSL when validating an EE certificate in order to insure the certificates have not expired or been revoked.

The NSSD provides support to check revocation information using CRLs residing in an HTTP repository. CRLs are obtained by NSSD using a certificate's HTTP CRL distribution point or a CRL in a certificate bundle. IKED must be configured as a network security client to exploit CRL checking.

IPSec algorithm support

IKEv1 Phase 1 and IKEv2 IKE SA			IKEv1 Phase 2 and IKEv2 Child SA		
Purpose	**Existing**	**New**	**Purpose**	**Existing**	**New**
Encryption algorithm	DES, 3DES, AES_CBC KeyLength 128	AES_CBC Keylength 256	Encryption algorithm	DES, 3DES, AES_CBC KeyLength 128	AES_CBC KeyLength 256, AES_GCM_16 KeyLength 128 | 256
Diffie-Hellman group	Group1, Group2, Group5, Group14	Group19, Group20, Group21, Group24	Authentication algorithm	HMAC_MD5, HMAC_SHA1	AES_GMAC_128 | 256, AES128_XCBC_96, HMAC_SHA2_256_128, HMAC_SHA2_384_192, HMAC_SHA2_512_256
KEv1 hash algorithm	MD5, SHA1	SHA2_256, SHA2_384, SHA2_512	Perfect forward secrecy group	Group1, Group2, Group5, Group14	Group19, Group20, Group21, Group24
Partner authentication	PreSharedKey, RSASignature	ECDSA-256, ECDSA-384, ECDSA-521 (these are only for IKEv2)			
KEv2 message verification algorithm	N/A	HMAC_MD5_96, HMAC_SHA1_96 AES128_XCBC_96, HMAC_SHA2_256_128, HMAC_SHA2_384_192, HMAC_SHA2_512_256			
KEv2 pseudo random unction	N/A	HMAC_MD5, HMAC_SHA1 AES128_XCBC, HMAC_SHA2_256, HMAC_SHA2_384, HMAC_SHA2_512			



SA: Security Association aka. the tunnel

Page 7

IKEv2 architecture uses certificates for digital signature authentication, like IKEv1 does. However, IKEv2 allows hash and URL encoding of certificates, while IKEv1 does not. Use of hash and URL encodings can reduce the size of IKEv2 messages, but has the additional overhead of retrieving the certificates from the HTTP server. IKEv2 peers indicate their support (and preference) for hash and URL encodings by sending a notify payload of type HTTP_CERT_LOOKUP_SUPPORTED.

z/OS Communications Server will support hash and URL encodings of certificates and bundles for IKEv2. This support includes configuration options, a new tool, and support for retrieval and use of certificates and certificate bundles from an HTTP server.

z/OS V1R12 IPSec-related RFC status – overview (list 1 of 2)

RFC	Title
3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
3948	UDP Encapsulation of IPsec ESP Packets
4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
4109	Algorithms for Internet Key Exchange version 1 (IKEv1)
4301	Security Architecture for the Internet Protocol
4302	IP Authentication Header
4303	IP Encapsulating Security Payload (ESP)
4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)
4306	Internet Key Exchange (IKEv2) Protocol
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
4308	Cryptographic suites for IPSec

This slide is the first of two slides listing the various RFCs that are related to the IPSec protocol.

z/OS V1R12 IPSec-related RFC status – overview (list 2 of 2)

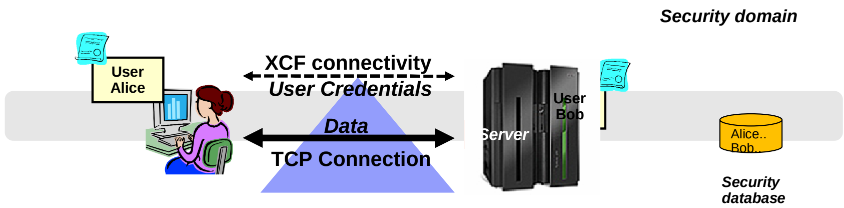
RFC	Title
4434	The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
4718	IKEv2 Clarifications and Implementation Guidelines
4753	ECP Groups For IKE and IKEv2
4754	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
4809	Requirements for an IPsec Certificate Management Profile
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
4869	Suite B Cryptographic suites for IPSec
4945	The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX
5282	Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol

This slide has the second half of the list of the various RFCs that are related to the IPSec protocol.

IBM Software Group Enterprise Networking Solutions

Trusted TCP connections

- Allow TCP connection endpoints within a Sysplex to establish a trust relationship
  - Exchanges security credentials that identify the security context of the other endpoint
    - Without the overhead and processor-related costs of SSL/TLS with client authentication
  - Requires no application protocol changes
    - Simple API call to the TCP/IP stack
    - Transparent to the client application
  - Security credentials exchanged using secure XCF messaging
    - Application traffic can take any network path between the client and server
- Support these new socket API options for C/C++ (LE), UNIX System Services Callable (BPXxxxx), and JAVA



Page 10

When client/server communication requires end-point authentication, the TCP protocol in itself does not provide such support transparently.

SNA/APPC does provide such capabilities by way of the conversation attach request. For SNA applications, the SNA LU 6.2 communication can return the user-specific security credentials in an LU 6.2 transaction initiation request, such as the user ID and group. This information can be used to authenticate the transaction user. It can also be used to establish a user-specific security environment.

For TCP, there are in general two methods available. The first is to add exchange of end-user credentials to the TCP payload protocol (application protocol), where each application protocol implements exchange of end-user credentials – in the clear, or if combined with various security extensions. The other method is to extend the TCP protocol with one or more security protocols, such as SSL/TLS, kerberos, or SSH. SSL/TLS protocols combined with operating-system specific support for mapping X.509 certificates to user definitions are widely used.

Trusted TCP connections provide a way to exchange security credentials between partners. If the partners are on different TCP/IP stacks, the exchange is across an XCF connection. This trusted relationship can be used for one-way or two-way communication. This exchange is not part of the TCP/IP connection setup, and only the applications requesting credentials need modification. The exploiting socket partners can use the partner security credentials to perform access control checks.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_wnsec.ppt

This module is also available in PDF format at: ../wnsec.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, copyrights, and disclaimers

IBM, the IBM logo, ibm.com, IBM, and z/OS 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. 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.

© Copyright International Business Machines Corporation 2010. All rights reserved.