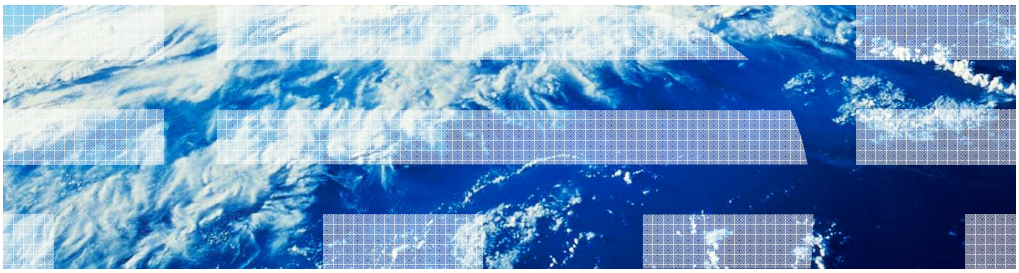
z/OS Communications Server – Security
IPSec support for cryptographic currency
IPSec support for FIPS 140 cryptographic mode



There are many new security functions in z/OS V1R12 Communications Server. This presentation covers IPSec support for cryptographic currency and IPSec support for FIPS 140 cryptographic mode.

IPSec use of cryptographic algorithms

- IPSec protection consists of the establishment of two types of security associations, or “SAs”
  - Phase 1 SA (IKEv1) or IKE SA (IKEv2)
    - Creates a secure communications channel over an insecure network
    - Used to negotiate the data protection SA in secret
  - Phase 2 SA (IKEv1) or Child SA (IKEv2)
    - Used to actually protect the application data
  - A set of SAs is sometimes referred to as a “tunnel”
- Various cryptographic algorithms are used during these processes

This slide provides a brief review of IPSec concepts.

IPSec protection consists of the establishment of two types of security associations, called “SAs.”

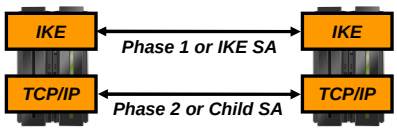
The IKE SA creates a secure channel over an insecure network, such as the public Internet. This secure channel is then subsequently used to negotiate, now in secret, the data protection SA.

The data protection SA is used to actually protect the application data flowing between the secure endpoints.

The SAs use various cryptographic algorithms to perform their duties.

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

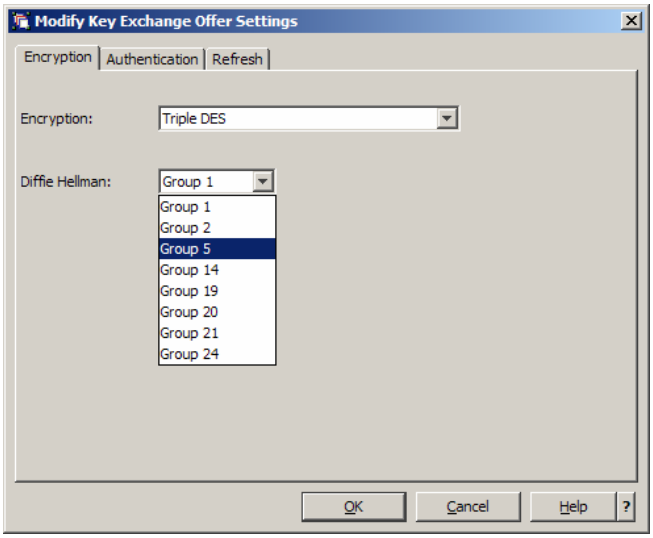
IKEv2 architecture uses certificates for digital signature authentication, like IKEv1 does. However, IKEv2 allows Hash and URL encoding of certificates, while IKEv1 does not. Use of Hash and URL encodings can reduce the size of IKEv2 messages, but has additional overhead of retrieval of the certificates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

Additional cryptographic algorithms (1 of 5)

- Configuration Assistant GUI -

- Phase 1 (IKEv1) / IKE SA (IKEv2): Encryption algorithm and DH group



This slide contains a screen capture of generating IPSec policy with the Configuration Assistant GUI.

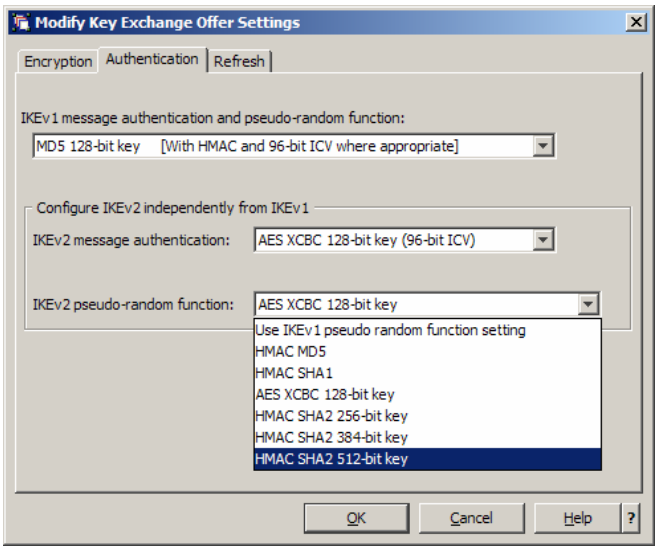
The IKEv1 phase 1 or IKEv2 IKE SA encryption algorithm and Diffie-Hellman group are specified on the Key Exchange Offer Settings panel. This panel can be accessed by following these steps:

When adding or modifying a Connectivity Rule for a particular z/OS image's stack, first click "Additional Settings". Then click "Optional advanced connectivity rule settings." Third, click the "Key Exchange" tab, and use the "Offers" link.

Additional cryptographic algorithms (2 of 5)

- Configuration Assistant GUI -

- Phase 1 (IKEv1) / IKE SA (IKEv2): Authentication algorithm and pseudo-random function



This slide contains a screen capture of generating IPSec policy with the Configuration Assistant GUI.

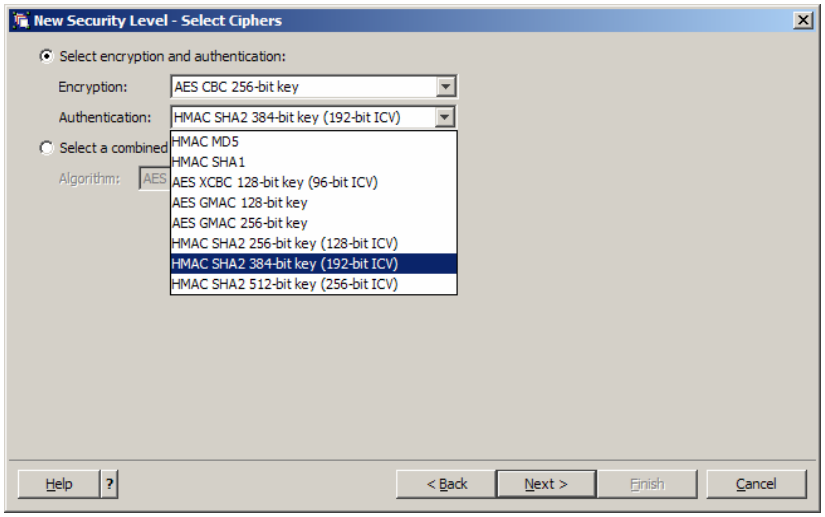
The IKEv1 phase 1 or IKEv2 IKE SA authentication and pseudo-random function algorithms are specified on the Key Exchange Offer Settings panel. This panel can be accessed by following these steps:

When adding or modifying a Connectivity Rule for a particular z/OS image's stack, first click "Additional Settings". Then "Optional advanced connectivity rule settings." Third, click the "Key Exchange" tab, and use the "Offers" link.

Additional cryptographic algorithms (3 of 5)

- Configuration Assistant GUI -

- Phase 2 (IKEv1) / Child SA (IKEv2): Encryption and authentication algorithms



This slide contains a screen capture of generating IPSec policy with the Configuration Assistant GUI.

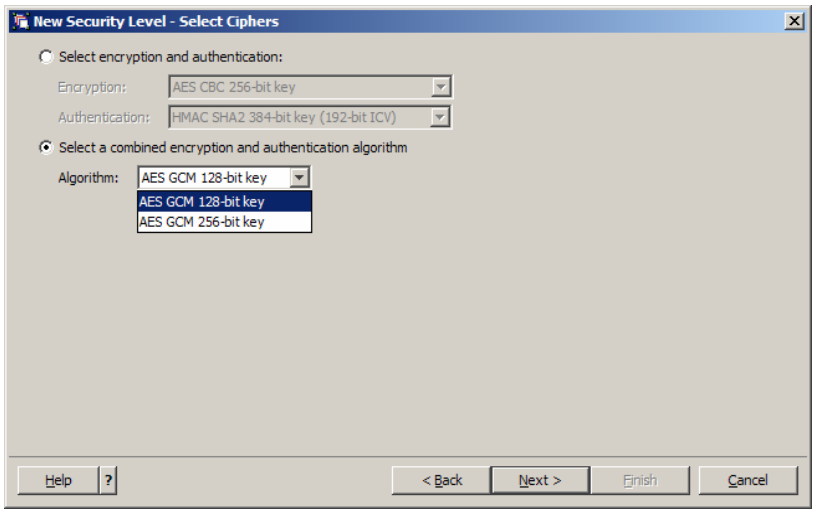
The IKEv1 phase 2 or IKEv2 Child SA encryption and authentication algorithms are specified on the Select Ciphers panel. This panel can be accessed by following these steps:

Choose a “Security Level” to add or modify under the “Reusable Objects” for the IPSec perspective. When adding a new Security Level, specify its type to be “IPSec dynamic tunnel.”

Additional cryptographic algorithms (4 of 5)

- Configuration Assistant GUI -

- Phase 2 (IKEv1) / Child SA (IKEv2): Specification of combined-mode algorithm



This slide contains a screen capture of generating IPSec policy with the Configuration Assistant GUI.

The AES_GCM combined mode algorithm provides both encryption and authentication. These operations are done in parallel, resulting in increased speed and efficiency.

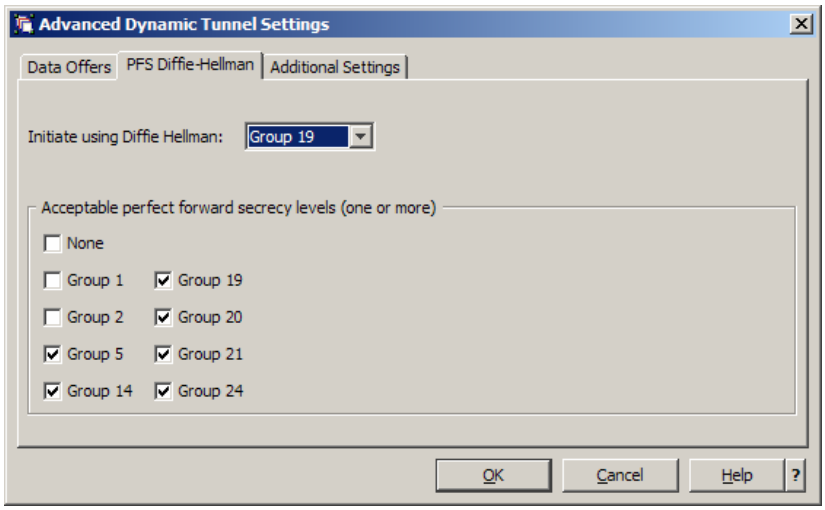
The IKEv1 phase 2 or IKEv2 Child SA combined mode algorithms are specified on the Select Ciphers panel. This panel can be accessed by following these steps:

Choose a “Security Level” to add or modify under the “Reusable Objects” for the IPSec perspective. When adding a new Security Level, specify its type to be “IPSec dynamic tunnel.”

Additional cryptographic algorithms (5 of 5)

- Configuration Assistant GUI -

- Phase 2 (IKEv1) / Child SA (IKEv2): Perfect forward secrecy groups



This slide contains a screen capture of generating IPSec policy with the Configuration Assistant GUI.

The IKEv1 phase 2 or IKEv2 Child SA perfect forward secrecy groups are specified on the Advanced Dynamic Tunnel Settings panel. This panel can be accessed by following these steps:

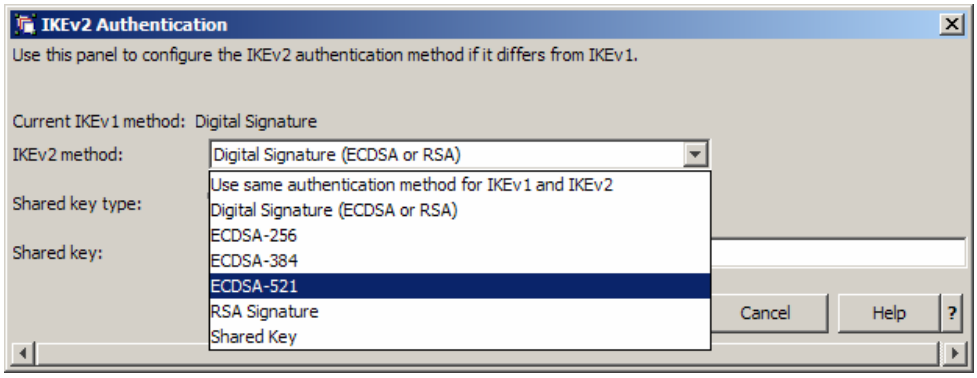
Choose a “Security Level” to add or modify under the “Reusable Objects” for the IPSec perspective. When adding a new Security Level, specify its type to be “IPSec dynamic tunnel.”

Perfect forward secrecy is optional and provides assurance of the integrity of short term derived keys if the longer term source keys are compromised.

Elliptic curve digital signature for IKEv2

- Configuration Assistant GUI -

- Remote peer's authentication of local security endpoint



This slide contains a screen capture of generating IPSec policy with the Configuration Assistant GUI.

The IKEv2 authentication method is specified on the IKEv2 authentication panel. In IKEv2, each node specifies the authentication method that remote peers should use to authenticate it.

The IKEv2 authentication panel can be accessed by following these steps:

When adding or modifying a Connectivity Rule for a particular z/OS image's stack, click the "Remote Security Endpoint" tab. Next click "Additional IKEv2 Options."

Display command examples (1 of 2)

- Phase 1 (IKEv1) / IKE SA (IKEv2): ipsec –k display

```
/u/user1 > ipsec -k display -p tcpcs4

CS V1R12 ipsec  Stack Name: TCPCS4  Mon Dec 14 13:35:50 2009
Primary:  IKE tunnel      Function: Display            Format:   Detail
Source:   IKED            Scope:    Current            TotAvail: n/a

TunnelID:                     K6
Generation:                   1
IKEVersion:                   1.0
.
.
RemoteEndPoint:               10.81.7.7
RemoteIDType:                 ID_IPV4_ADDR
RemoteID:                     10.81.7.7
ExchangeMode:                 Main
State:                        DONE
AuthenticationAlgorithm:      HMAC-SHA2-384-192
EncryptionAlgorithm:          AES-CBC
 KeyLength:                   256
PseudoRandomFunction:         HMAC-SHA2-384
DiffieHellmanGroup:           21
LocalAuthenticationMethod:    PresharedKey
.
.
*******************************************************************************
```


The ipsec –k display command is used to display information about the IKEv1 phase 1 or IKEv2 IKE SA.

This slide contains a display showing some of the new algorithm values.

Display command examples (2 of 2)

- Phase 2 (IKEv1) / Child SA (IKEv2): ipsec –y display

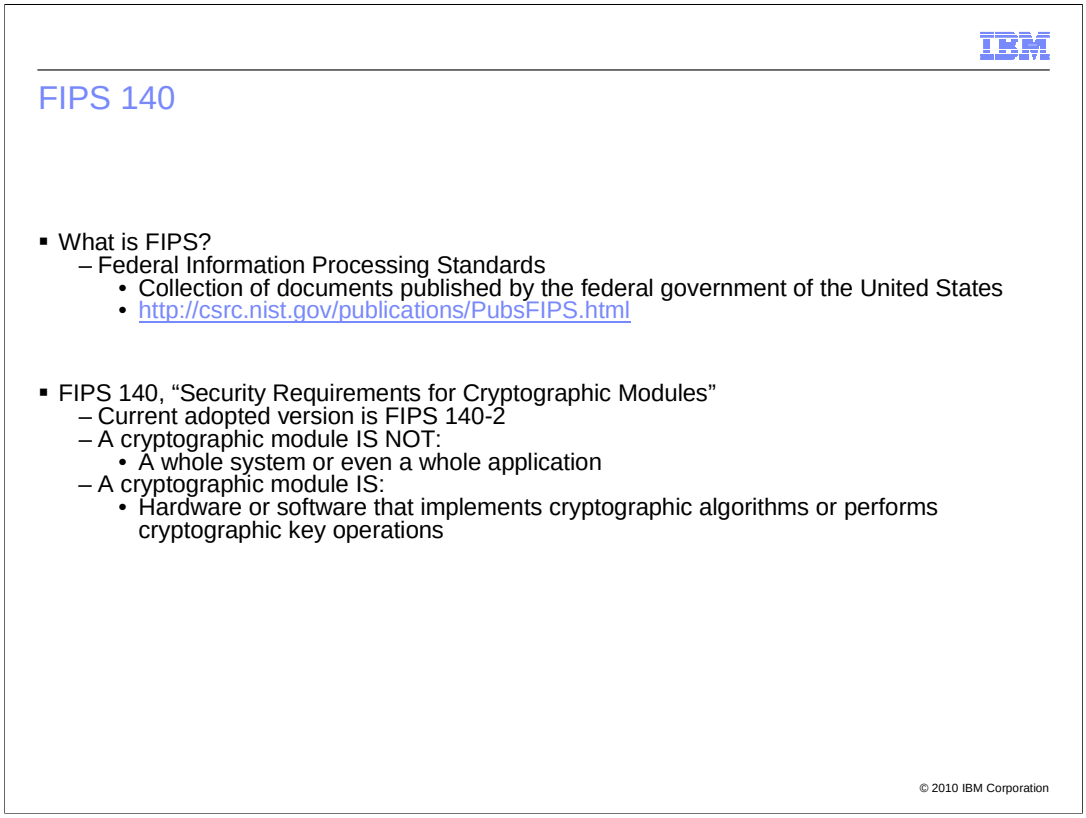
```
/u/user1 > ipsec -y display -p tcpcs4

CS V1R12 ipsec  Stack Name: TCPCS4  Tue Dec 15 12:12:07 2009
Primary:  Dynamic tunnel  Function: Display            Format:   Detail
Source:   Stack           Scope:    Current            TotAvail: 1

TunnelID:                     Y3
Generation:                   1
IKEVersion:                   1.0
ParentIKETunnelID:            K2
.
.
HowToAuth:                    n/a
 AuthAlgorithm:               n/a
 AuthInboundSpi:              0          (0x       0)
 AuthOutboundSpi:             0          (0x       0)
HowToEncrypt:                 AES-GCM-16
 KeyLength:                   128
 EncryptInboundSpi:           1964519200 (0x75182F20)
 EncryptOutboundSpi:          3028212192 (0xB47ED9E0)
Protocol:                     ALL(0)
.
.
*********************************************************************
```


The ipsec –y display command is used to display information about the IKEv1 phase 2 or IKEv2 Child SA.

This slide contains a display showing AES-GCM-16, an algorithm that combines authentication and encryption.

Since AES_GCM is a combined mode algorithm, it must be specified in combination with HowToAuth ESP NULL. This is why HowToAuth and AuthAlgorithm are shown as “n/a.”

The ipsec –y display command gets its information from the TCP/IP stack. Much of the same information can be obtained with the ipsec –y –b command, which gets its information from the IKE daemon.



FIPS stands for “Federal Information Processing Standards.” The standards cover a wide variety of topics. FIPS can be closely related to, or result in, standards published by the wider community such as ANSI, IEEE, ISO. Support of FIPS standards documents applies to a broad range of topics and is often required to do business with various government agencies.

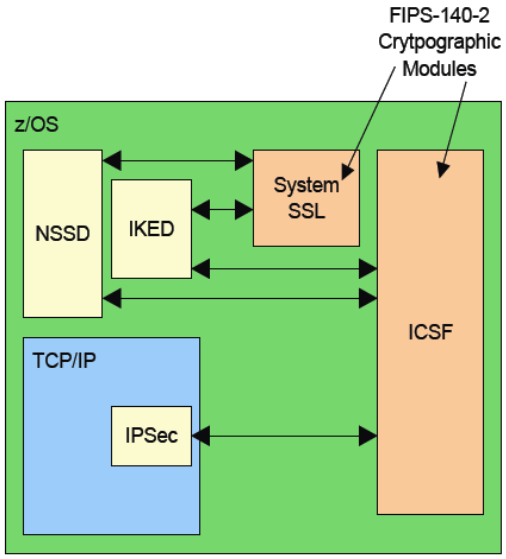
Documents of this nature are often based on existing standards adopted by the wider IT community, or become the source of new standards for the community.

FIPS 140 (current version FIPS 140-2) deals with cryptographic modules, and imposes security requirements on 11 different areas. FIPS 140 certified cryptographic modules must satisfy requirements on interfaces, authentication and roles, physical and environmental security, cryptographic key management, and others.

For example, requirements on interfaces detail how information flows into and out of the cryptographic modules, and how that information is managed. Authentication and role requirements specify who is allowed to perform what actions with the cryptographic modules. Physical security requirements include locks and other tamper-resistant features, and the ability to withstand environmental conditions. Cryptographic key management covers the generation and storage of cryptographic keys.

FIPS 140 cryptographic mode for IPSec

- z/OS IPSec major components
  - IKED (Internet key exchange)
  - TCP/IP stack
  - NSSD (network security services)
- z/OS IPSec uses two cryptographic modules
  - z/OS System SSL
    - Used for X.509 certificate management
  - z/OS ICSF (crypto services facility)
    - Used for encrypt/decrypt, hashing, Diffie-Hellman and PRF operations



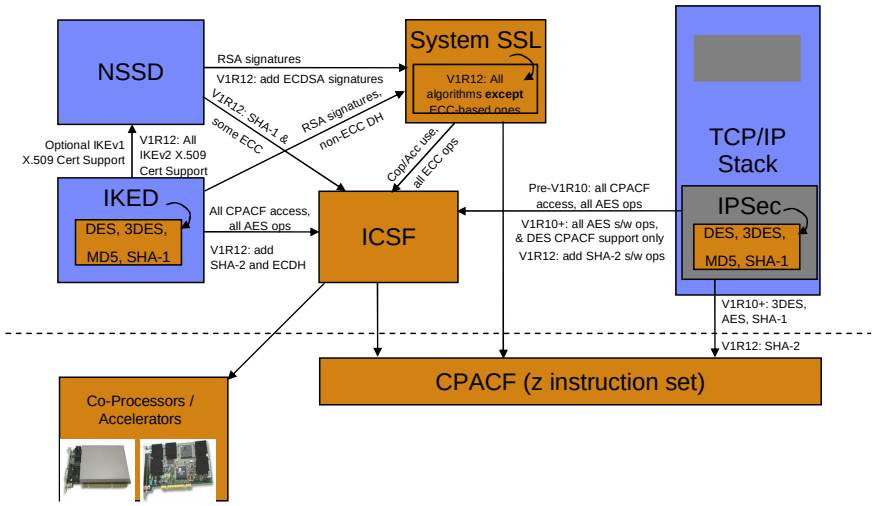
There are three major components of z/OS IPSec. The primary purpose of the IKE daemon (IKED) is to negotiates SA parameters and manage cryptographic keys. The TCP/IP stack manages data protection SAs and performs some encryption and decryption. The Network Security Services daemon (NSSD) provides remote 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 will forward all cryptographic operation requests to cryptographic modules using FIPS 140 interfaces.

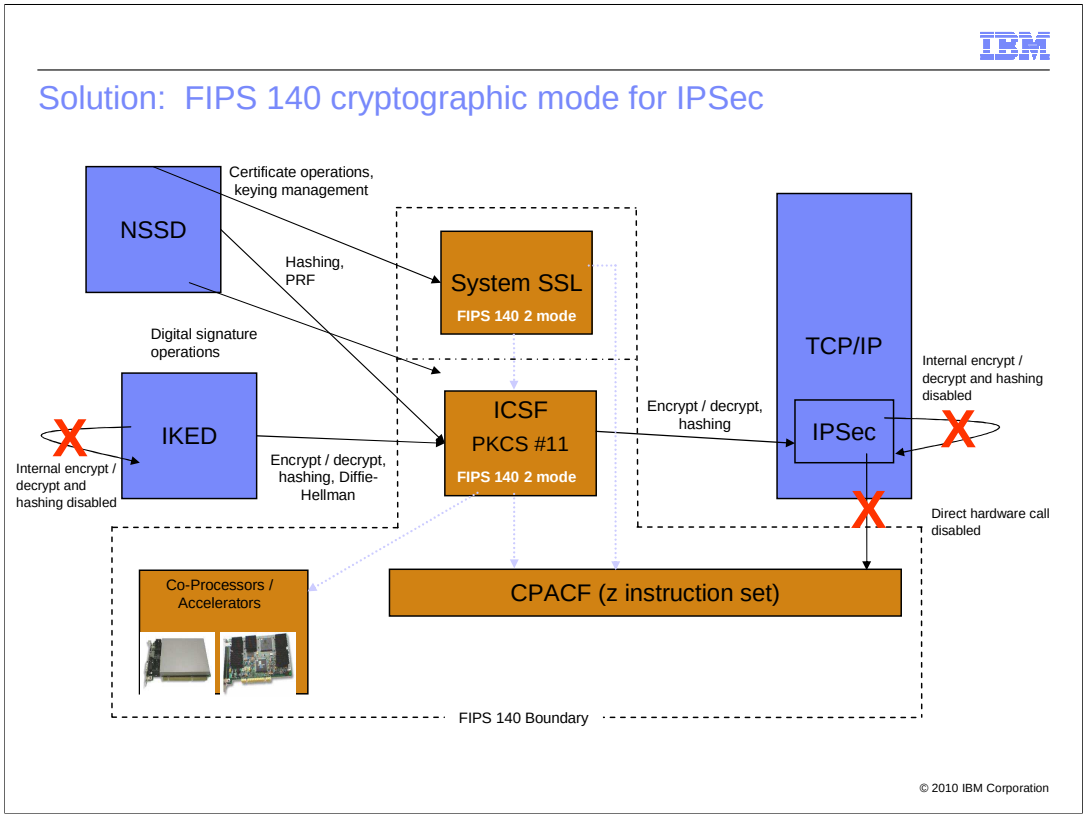
The two cryptographic modules used are z/OS System SSL and z/OS ICSF. System SSL supports FIPS 140-2 mode on z/OS V1R11 and up, and is used for X.509 certificate management. The z/OS ICSF (the crypto services facility) PKCS #11 interface has a FIPS 140-2 mode on V1R12 and up. It is used for encrypt/decrypt, hashing, Diffie-Hellman and PRF operations.

z/OS TCP/IP cryptographic landscape: non-FIPS 140 mode



This slide shows the z/OS Communications Server cryptographic landscape in non-FIPS 140 mode.

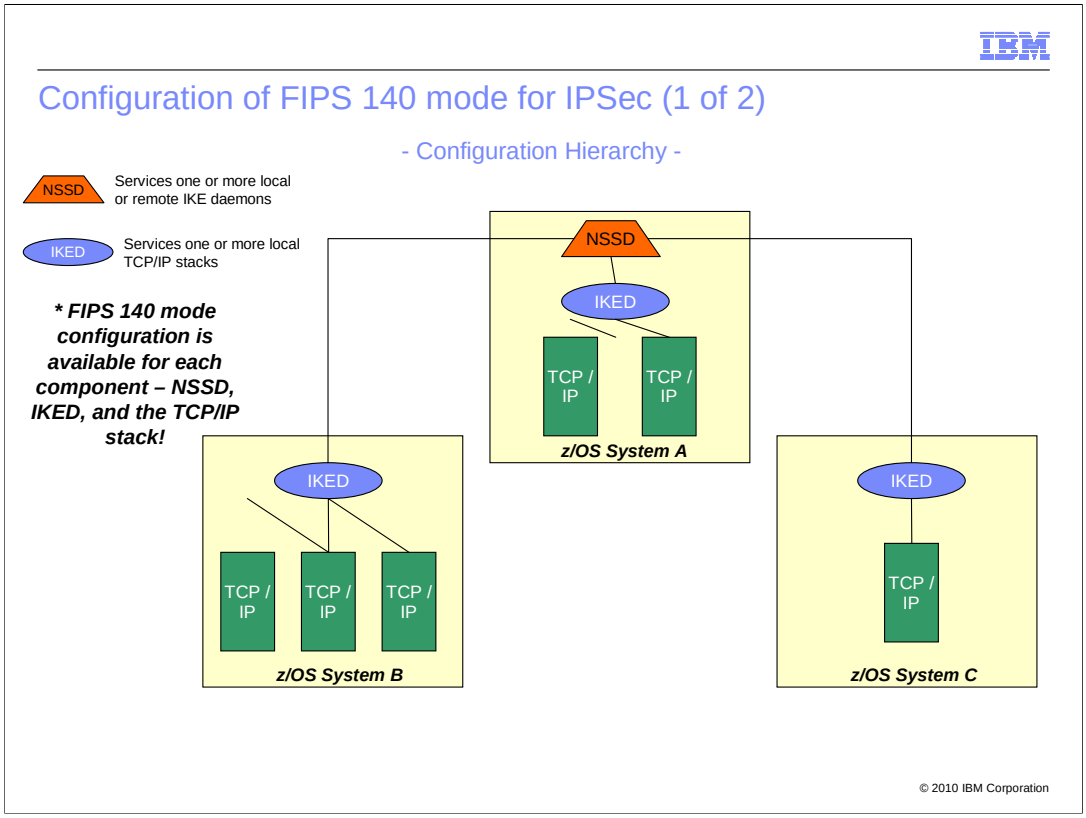
No cryptographic boundary exists, and cryptographic operations are performed by a wide variety of hardware and software.



This slide shows the z/OS Communications Server cryptographic landscape in the new FIPS 140 cryptographic mode for IPSec.

A logical cryptographic boundary is introduced that separates the cryptographic operation requestors from the cryptographic operation providers.

All cryptographic operations must be performed inside the boundary, and be initiated by cryptographic modules in FIPS 140 modes of operation.



The three major components of z/OS IPSec can be independently configured for FIPS 140 cryptographic mode. When possible, FIPS 140 mode should be configured for NSSD, IKED, and the TCP/IP stacks all at once. If this is not possible, and FIPS 140 support must be implemented in stages, it should be performed in this “top down” order.

First configure FIPS 140 mode for NSSD. When operating in FIPS 140 mode, NSSD can serve both FIPS and non-FIPS IKE daemon clients. However, in both cases, NSSD will only create and verify signatures for certificates that conform to FIPS 140 requirements.

Second, configure FIPS 140 mode for IKED. When operating in FIPS 140 mode, IKED can serve both FIPS and non-FIPS TCP/IP stacks. However, in both cases, the IKE daemon will omit restricted algorithms from any proposal it builds, and only use the PKCS #11 interface to ICSF.

Third, configure FIPS 140 mode for TCP/IP stacks.

Error configurations can arise if a “bottom up” approach is attempted. If a TCP/IP stack is enabled for FIPS 140 mode but IKED is not, IKED cannot provide any cryptographic services to that TCP/IP stack. If IKED is enabled for FIPS 140 mode but NSSD is not, the NSS daemon will not provide certificate services to that IKE daemon.

Configuration of FIPS 140 mode for IPSec (2 of 2)

- ICSF
  - Start in FIPS compatibility mode
    - Compatibility mode avoids imposing restrictions on other exploiters of PKCS #11
  - See “Cryptographic Services ICSF Overview” publication at the Cryptographic Services bookshelf for more information
    - http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/CSFBKZA0

- System SSL
  - Does not need to be explicitly started in FIPS mode, callable automatically
  - See “Cryptographic Services System Secure Sockets Layer (SSL) Programming” publication at the Cryptographic Services bookshelf for more information
    - http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/CSFBKZA0

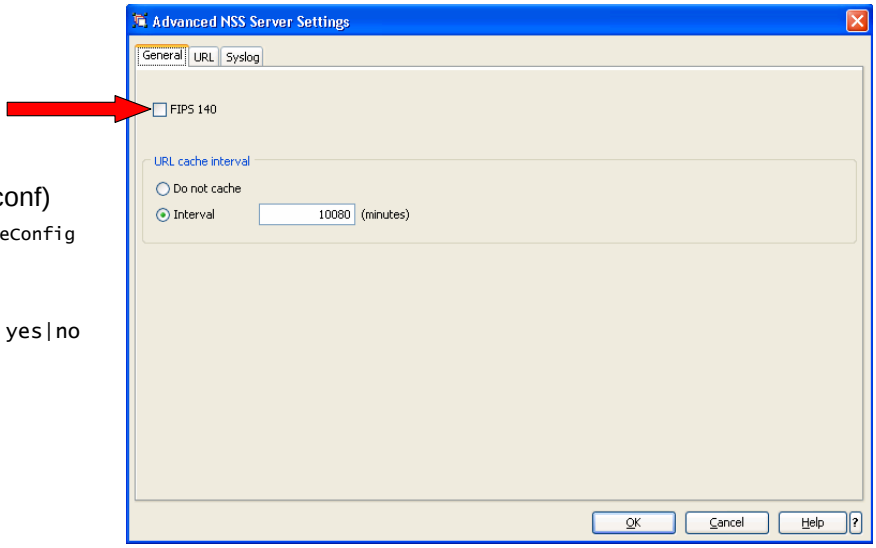
This slide contains details about ICSF and System SSL, and how they operate in FIPS 140 mode.

Starting ICSF in pure FIPS mode will impose algorithm restrictions on all daemons and users of the PKCS #11 interface into ICSF. It is therefore recommended to start ICSF in FIPS compatibility mode so that restrictions are only imposed on daemons and users wanting to comply with FIPS mode requirements.

Function externals: NSSD configuration of FIPS 140 mode for IPSec

NSSD (nssd.conf)

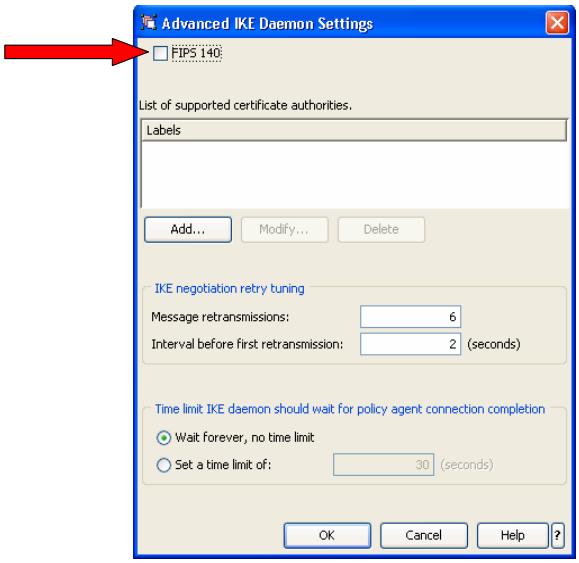
```
IPSecDisciplineConfig
   {
      …
     FIPS140 yes|no
      …
   }
```



This slide contains a screen capture of configuring FIPS 140 mode for the NSS daemon with the Configuration Assistant GUI.

Function externals: IKED configuration of FIPS 140 mode for IPSec

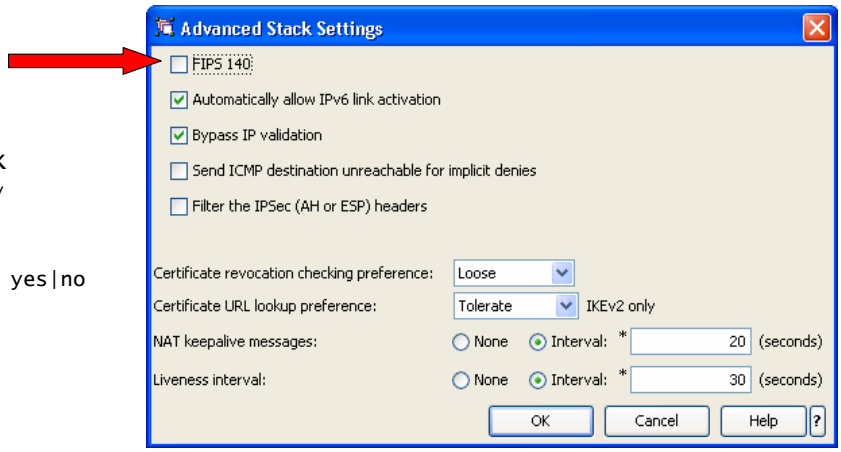
IKED (iked.conf)
FIPS140 yes|no



This slide contains a screen capture of configuring FIPS 140 mode for the IKE daemon with the Configuration Assistant GUI.

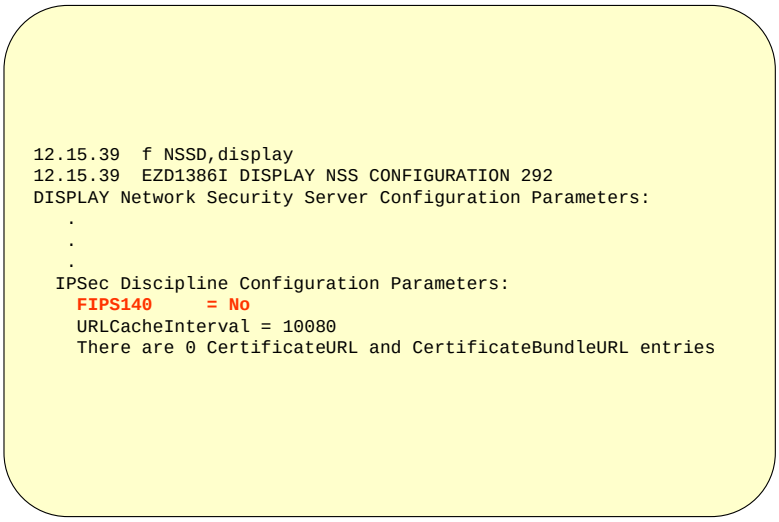
Function externals: TCP/IP configuration of FIPS 140 mode for IPSec

```
TCP/IP stack
   IpFilterPolicy
      {
        …
        FIPS140 yes|no
        …
      }
```



This slide contains a screen capture of configuring FIPS 140 mode for the TCP/IP stack with the Configuration Assistant GUI.

Function externals: F NSSD,DISPLAY



The F NSSD,DISPLAY command is used to display information about the NSS daemon.

A new field has been added to indicate the FIPS 140 mode setting.

Function externals: F IKED,DISPLAY

```
12.09.47  f iked,display
12.09.47  EZD1158I DISPLAY IKE CONFIGURATION 276
DISPLAY IKE configuration parameters:
  Values loaded from /etc/security/iked.conf
  IkeSyslogLevel = 15
  PagentSyslogLevel = 31
  SMF119 = IKETunnel
  SMF119 = DynTunnel
  Keyring = IKED/IKEDRING
  IkeRetries = 6
  IkeInitWait = 2
  FIPS140 = yes
  Echo = no
  PagentWait = 0
  NssWaitLimit = 60
  NssWaitRetries = 3
  SupportedCertAuth 1 = IPSEC_VIC007_CACERT
  .
  .
  .
```


The F IKED,DISPLAY command is used to display information about the IKE daemon.

A new field has been added to indicate the FIPS 140 mode setting.

Function externals: ipsec –f display –p stackname

```
/u/user1 > ipsec -f display -p tcpcs4

CS V1R12 ipsec  Stack Name: TCPCS4  Thu Dec 17 12:19:43 2009
Primary:  Filter          Function: Display            Format:   Detail
Source:   Stack Policy    Scope:    Current            TotAvail: 36
Logging:  On              Predecap: Off                DVIPSec:  Yes
NatKeepAlive:  20         FIPS140:  Yes
Defensive Mode: Inactive

FilterName:                   IKE_Allow
FilterNameExtension:          1
GroupName:                    n/a
LocalStartActionName:         n/a
VpnActionName:                n/a
TunnelID:                     0x00
Type:                         Generic
DefensiveType:                n/a
State:                        Active
Action:                       Permit
Scope:                        Local
Direction:                    Outbound
OnDemand:                     n/a
.
.
.
```


The ipsec –f display command is used to display information about the TCP/IP stack's filter rules.

A new field has been added to the header of the display to indicate the TCP/IP stack's FIPS 140 mode setting.

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 email feedback:

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

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

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

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, Current, 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.