z/OS 2.4 IBM Education Assistance (IEA)

Solution (Epic) Name: AT-TLS support for TLS v1.3

Element(s)/Component(s): TCP/IP

© 2019 IBM Corporation

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

© 2019 IBM Corporation

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

© 2019 IBM Corporation

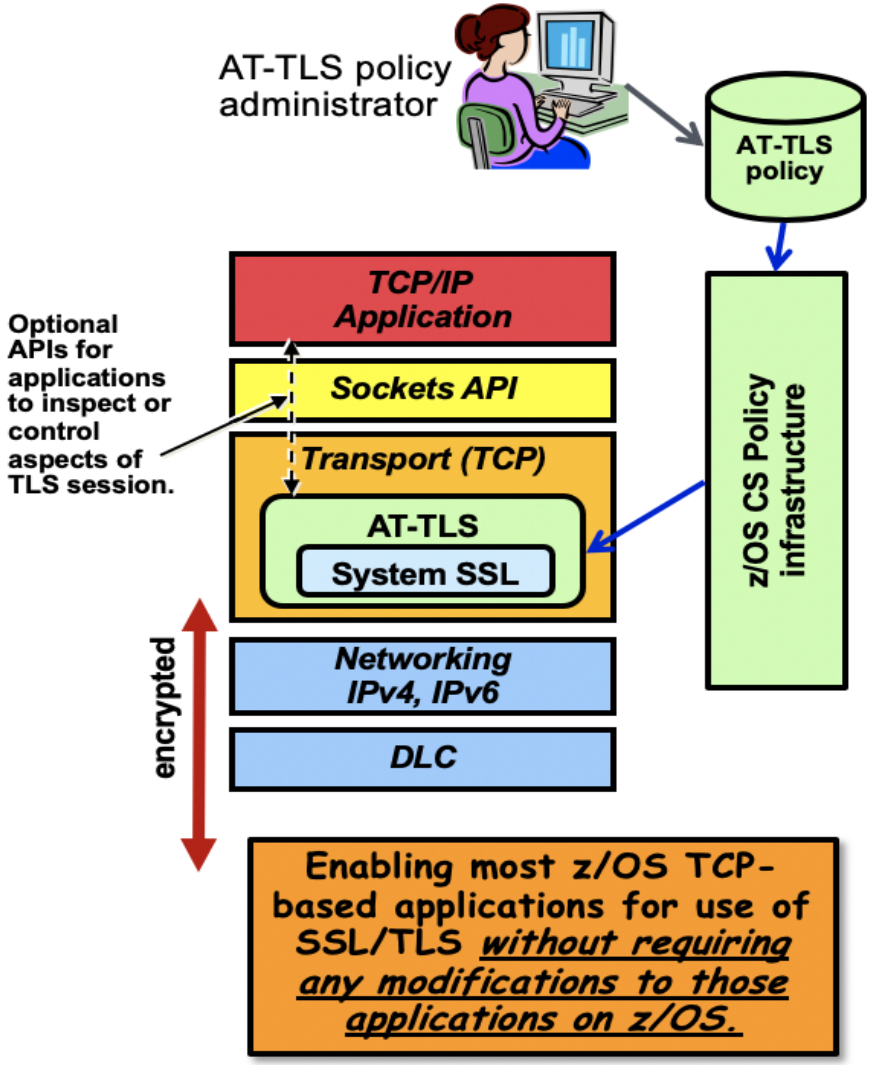
Session Objectives

- AT-TLS support for TLS v1.3

© 2019 IBM Corporation

Background information: AT-TLS and System SSL

- System SSL is the Cryptographic Services component that implements the SSL and TLS protocols natively on z/OS
- AT-TLS is a function within the TCP/IP stack that allows you to apply SSL/TLS protection to TCP traffic
  - AT-TLS is essentially a System SSL wrapper that lives in the stack
  - Applied based on policy, no need to change application source code (transparent)
  - Advantages
    - Reduces application development cost
    - Consistent TLS administration across z/OS applications
    - Allows z/OS components, middleware, and other software to transparently benefit from System SSL's support for evolving standards



© 2019 IBM Corporation

Background information: Some z/OS applications that use AT-TLS

- Communications Server applications
  - TN3270 server
  - FTP client and server
  - CSSMTP
  - Load Balancing Advisor
  - IKED NSS client
  - NSS server
  - Policy Agent
- DB2 DRDA
- IMS Connect
- CICS TS 5.3 and later (server side)
- IBM Copy Services Manager HyperSwap
- JES2 NJE
- IBM Tivoli applications
  - NetView
  - IBM Tivoli Manager (TEPS, TEMS)
  - OMEGAMON manager
- RACF Remote Sharing Facility
- ICSF Regional Crypto services
- CICS Sockets applications
- Other IBM software
- 3rd party applications
- Customer applications

© 2019 IBM Corporation

Overview

Who (Audience)

- z/OS Network security administrators and application owners

What (Solution)

- AT-TLS support for TLS v1.3 (RFC 8446)

Wow (Benefit / Value, Need Addressed)

- z/OS Network security administrators can enable support for the new TLS 1.3 security protocol to improve the security of TLS-protected traffic

© 2019 IBM Corporation

Usage & Invocation - Network Configuration Assistant (NCA)

Welcome × Network Configu... ×

Network Configuration Assistant (Home) ▸ AT-TLS

V2R4 Current Backing Store is MJF_ATTLS2

Select a TCP/IP technology to configure : AT-TLS

Systems | Traffic Descriptors | Security Levels | Address Groups | Requirement Maps

Actions

- View Details
- Modify...
- Copy...
- Delete
- Show Where Used
- New...
- Hide Filter Row
- Clear Sorts

her (First Choice)	Type Filter	Description Filter
ne	No security	IBM supplied: Traffic is allowed with no security
067 - _DHE_RSA_WITH_AES_128_CBC_SHA256	AT-TLS	IBM supplied: encryption for NIST z9 compliance
06B - _DHE_RSA_WITH_AES_256_CBC_SHA256	AT-TLS	IBM supplied: encryption for NIST z10 compliance

Home | Save

Welcome × Network Configu... ×

Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level

New Security Level

- Name
- Ciphers
- Advanced Settings

Name

* Name: mylevel

Description:

Version choices

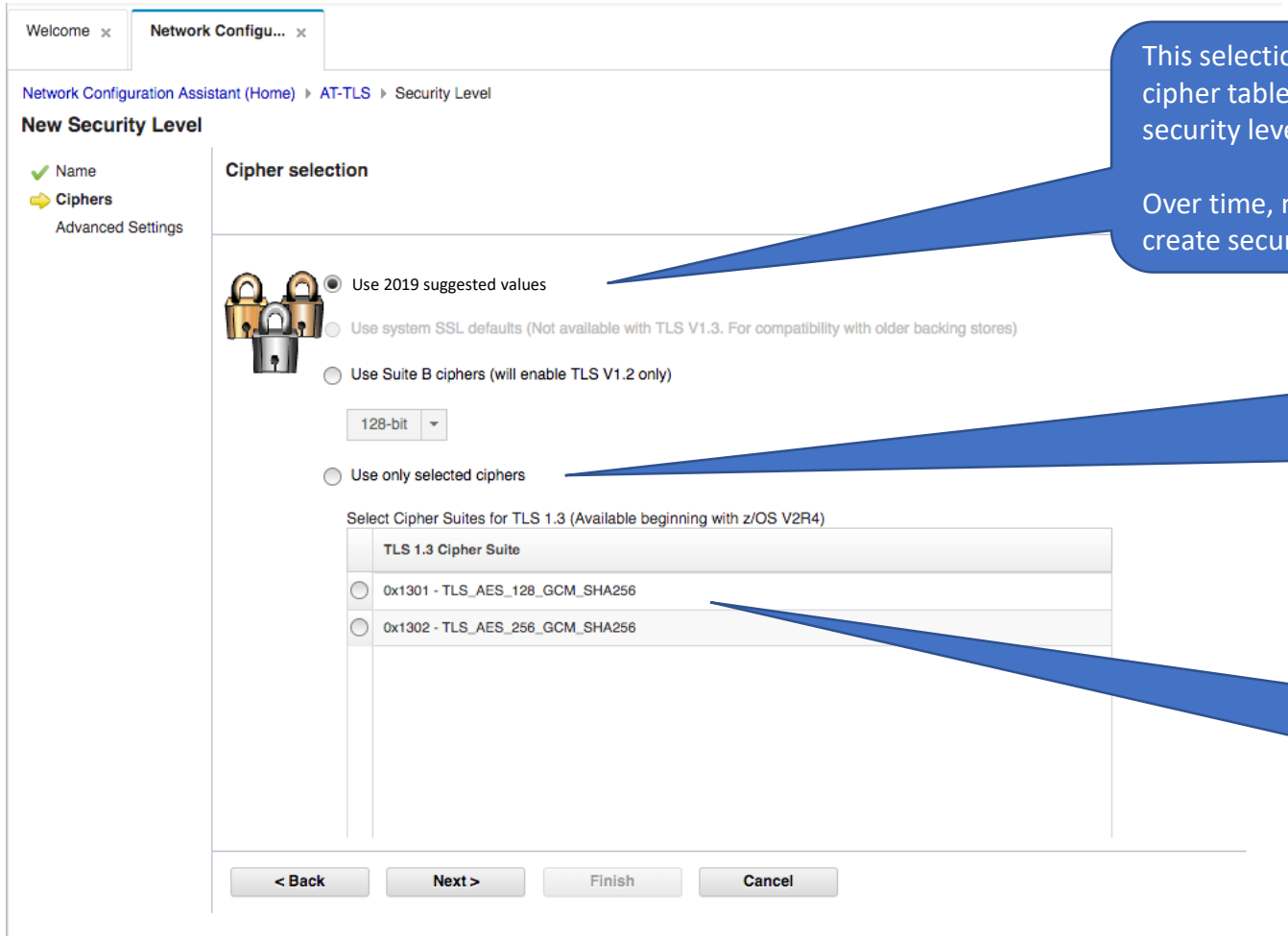
- [x] TLS V1.3 (Available beginning with z/OS V2R4)
- [x] TLS V1.2
- [ ] TLS V1.1
- [ ] TLS V1.0 (not recommended)
- [ ] SSL V3 (not recommended)

< Back | Next > | Finish | Cancel

Ciphers, named groups, signature parms, etc., are on subsequent panels in this wizard

© 2019 IBM Corporation

Usage & Invocation - NCA Cipher selection



This selection is new for V2R4. It places the currently suggested values into the cipher tables on this panel. This option is initially selected when creating a new security level.

Over time, new “suggested value” choices may be introduced to make it easy to create security levels according to current best practices.

If you have “Use 2019 suggested values” selected and change to this selection, the suggested values remain in the cipher tables and you can modify them. This allows you to start with suggested values and then update from there.

Since the cipher suites are different, there are separate tables for TLS 1.3 ciphers (shown here) and pre-TLS 1.3 ciphers (shown on the next slide).

© 2019 IBM Corporation

Usage & Invocation - NCA Cipher selection (contd.)

Welcome × | Network Configu... ×

Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level

New Security Level

- Name
- Ciphers
- Advanced Settings

Cipher selection

- Use 2019 suggested values
- Use system SSL defaults (Not available with TLS V1.3. For compatibility with older backing stores)
- Use Suite B ciphers (will enable TLS V1.2 only)
  - 128-bit
- Use only selected ciphers

Select Cipher Suites for TLS V1.3 (Available beginning with z/OS V2R4)

Actions | Move Up | Move Down

- Move Up
- Move Down
- Cut
- Paste
- Choose Ciphers...

M_SHA256

M_SHA384

< Back | Next > | Finish | Cancel

Welcome × | Network Configu... ×

Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Cipher Selection

TLS V1.3 Cipher Selection

TLS 1.3 | AES 256 Bit | AES 128 Bit | RC/DES/3DES | No Encryption

- 1301 - TLS_AES_128_GCM_SHA256
- 1302 - TLS_AES_256_GCM_SHA256
- 1303 - TLS_CHACHA20_POLY1305_SHA256

OK | Cancel

TLS v1.3 uses a different set of ciphers than previous versions so the ciphers must be chosen separately for TLS 1.3 and other TLS versions.

© 2019 IBM Corporation

Usage & Invocation - NCA Signature and Key Share settings

As you select client named groups, you also select if they can will be used by the client to generate at TLS v1.3 key share.

Welcome × | Network Configu... ×

Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Advanced Help

Advanced AT-TLS Settings

Client Authentication | Tuning | **Signature and Key Share** | Renegotiation | Other | SSL Version 2 Ciphers

TLS V1.3 Server Key Share Groups (Available beginning with z/OS V2R4)
If TLS V1.3 is in use, the server selects from the ordered list of key share groups provided by the client during TLS negotiation. Select which key share groups are acceptable to this endpoint when it is a server.

- (●) Accept any supported key share group from the client
- ( ) Accept only selected key share groups from the client

- Tip: if there is no overlap between this set and the client's set, the TLS handshake will fail.
- Requirement: At least one must be selected from this list if TLS V1.3 is supported for this security level.

- [ ] secp521r1
- [ ] secp384r1
- [ ] secp256r1
- [ ] X25519
- [ ] X448

Named groups supported by the client

- ( ) Use system SSL defaults
- ( ) Use any named group (not available when the security level supports TLS V1.3)
- (●) Customize

Named groups supported by the client

Actions | Move Up | Move Down

Name | generate TLS V1.3 Client Key Share

- Move Up
- Move Down
- Toggle TLS 1.3 Client Key Share
- Select Groups...

There is no data to display.

OK | Cancel

Welcome × | Network Configu... ×

Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Advanced ▸ Named Groups

Select Client Named Groups

- [ ] secp521r1
  - [ ] Use to generate TLS V1.3 Client Key Share
- [x] secp384r1
  - [ ] Use to generate TLS V1.3 Client Key Share
- [x] secp256r1
  - [ ] Use to generate TLS V1.3 Client Key Share
- [ ] secp224r1 (not supported for TLS V1.3)
- [ ] secp192r1 (not supported for TLS V1.3)
- [ ] X25519 (Available beginning with z/OS V2R4)
  - [ ] Use to generate TLS V1.3 Client Key Share
- [ ] X448 (Available beginning with z/OS V2R4)
  - [ ] Use to generate TLS V1.3 Client Key Share

OK | Cancel

© 2019 IBM Corporation

Usage & Invocation - NCA Signature and Key Share settings (contd.)

Allowed hash and signature algorithm pairs

Allowed hash and signature algorithm pairs

- ○ Use AT-TLS defaults (see help for default values)
- ◉ Customize

Allowed hash and signature algorithm pairs

Hash and Signature Algorithm Pairs
Actions ▾ Move Up Move Down
Move Up Move Down Select Algorithms...
There is no data to display.

Total: 0 Selected: 0

Allowed hash and signature algorithm pairs for digital signatures of X.509 certificates (only use for TLS 1.2 or later) (Available beginning with z/OS V2R4)

- ◉ Use the same hash and signature pairs for digital signatures of X.509 certificates as are used for handshake messages
- ○ Customize

Allowed hash and signature algorithm pairs

Hash and Signature Algorithm Pairs
There is no data to display.

OK Cancel

Welcome × | Network Configu... ×

Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Advanced ▸ Hash and Signature Algorithm Pairs

Select Allowed Hash and Signature Algorithm Pairs

Available for TLS 1.2 and TLS 1.3

- ☐ SHA256_WITH_RSA
- ☐ SHA256_WITH_ECDSA
- ☐ SHA384_WITH_RSA
- ☐ SHA384_WITH_ECDSA
- ☐ SHA512_WITH_RSA
- ☐ SHA512_WITH_ECDSA

Available for TLS 1.2 and TLS 1.3 beginning with z/OS V2R4

- ☐ SHA256_WITH_RSASSA_PSS
- ☐ SHA384_WITH_RSASSA_PSS
- ☐ SHA512_WITH_RSASSA_PSS

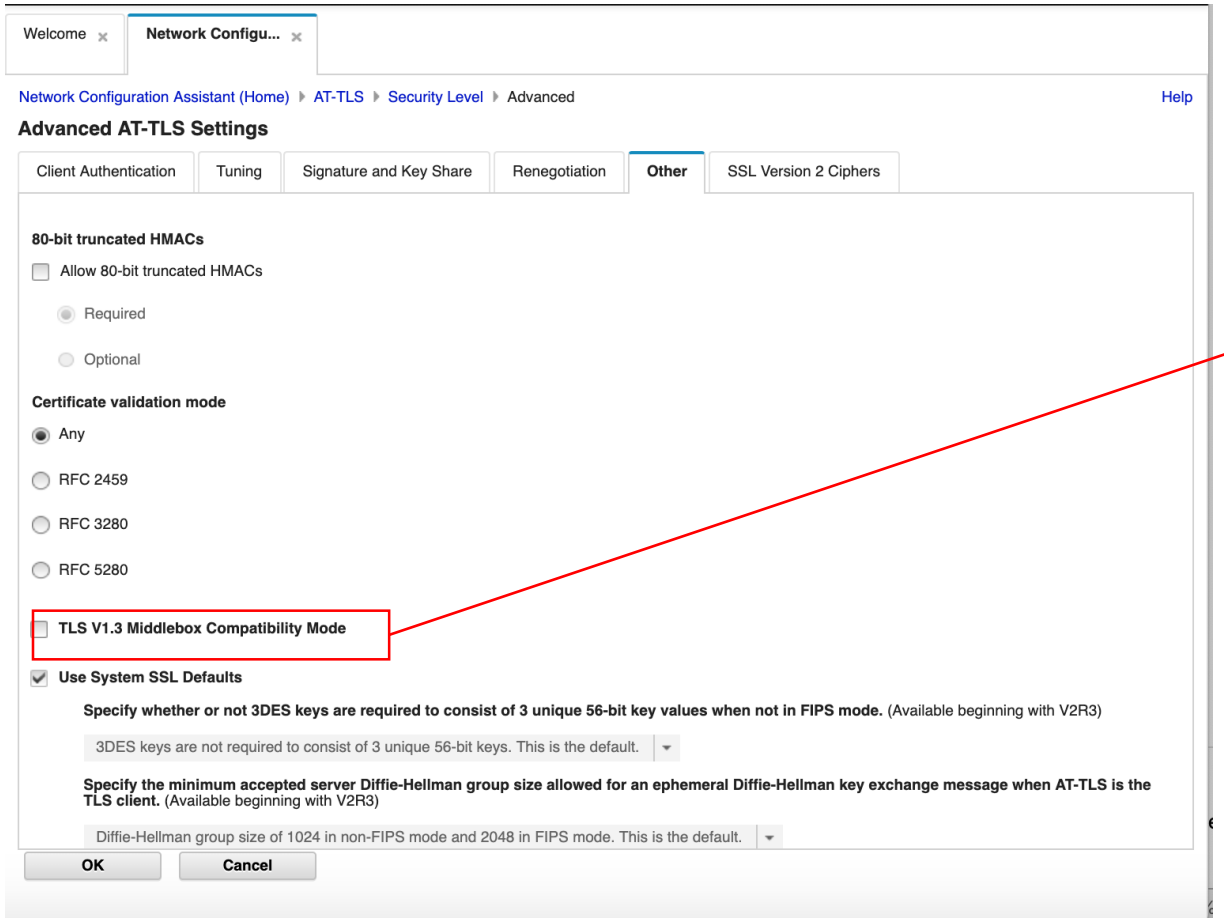
Only available for TLS 1.2

- ☐ MD5_WITH_RSA
- ☐ SHA1_WITH_RSA
- ☐ SHA1_WITH_DSA
- ☐ SHA1_WITH_ECDSA
- ☐ SHA224_WITH_RSA
- ☐ SHA224_WITH_DSA
- ☐ SHA224_WITH_ECDSA
- ☐ SHA256_WITH_DSA

OK Cancel

© 2019 IBM Corporation

Usage & Invocation - NCA Other settings



TLS v1.3 middlebox compatibility mode is set on this panel.

This mode causes the TLS V1.3 handshake process to use or tolerate handshake messages in a manner compliant with earlier TLS protocols to alleviate possible issues with middle boxes or proxies.

© 2019 IBM Corporation

Usage & Invocation - NCA Tuning settings

Network Configuration Assistant (Home) ▸ AT-TLS ▸ Security Level ▸ Advanced

Advanced AT-TLS Settings

Client Authentication | Tuning | Signature and Key Share | Renegotiation | Other | SSL Version 2 Ciphers

The following paramaters apply to SSL Version 3 and TLS Version 1.x

Reset Cipher Key Timer

- (●) Do not reset the key
- ( ) Reset the key every: 1,440 minutes (range 1-1440)

Caching session identifiers or tickets

Tip: The following parameters control session identifiers for SSL V3 and TLS versions 1.0-1.2, and they control session tickets for TLS1.3. See help for more details.

☐ Accept all defaults for caching session identifiers or tickets

Caching SSL Version 3 / TLS Version 1 session identifiers

- ( ) Do not cache
- (●) Cache session identifiers

Cached identifiers expire after: 86400 seconds (range 1-86400)

Cache size: 512 entries (range 1-64000)

If you can accept defaults for the caching of session identifiers or tickets, click here and you are done with this panel

Select whether to cache session identifiers and if so, for how long. If you select not to cache, the rest of the parameters on this panel don't matter and are greyed.

© 2019 IBM Corporation

Usage & Invocation - NCA Tuning settings

The following selections apply only to TLS Version 1.3 and are available beginning with z/OS V2R4

Client caching of session tickets and session resumption attempts

- ○ Disable
- ● Enable

Maximum size of a cached session ticket: 8,192 bytes (range 0 - 2 147 483 647)

Tip: a value of 0 allows a session ticket of any size

Server sending of session tickets and support for session resumption attempts from the client

- ○ Disable
- ● Enable

Encryption/decryption algorithm for session tickets for TLS 1.3 session resumption

- ● AESCBC128
- ○ AESCBC256

Number of TLS 1.3 session tickets that will be sent by the server to the client after the initial handshake completes: 2 (range 0-16)

Refresh interval of the encryption key used by the server to encrypt session tickets for TLS 1.3 session resumption: 300 seconds (range 0-604800)

Maximum time from the initial handshake that a server will accept a session resumption request from the client: 300 seconds (range 0-604800)

OK Cancel

Select whether to cache session identifiers and if so, for how long. If you select not to cache, the rest of the parameters on this panel don't matter and are greyed.

© 2019 IBM Corporation

Usage & Invocation (contd.)

- Type 119 SMF records are updated to support TLS v1.3
  - Subtype 2 (TCP Connection Termination)
  - Subtype 49 (CSSMTP Connection)
  - Subtype 3 (FTP Client Transfer Completion)
  - Subtype 70 (FTP Server Transfer Completion)
  - Subtype 72 (FTP Server Login Failure)
  - Subtype 100 (FTP Server Transfer Initialization)
  - Subtype 101 (FTP Client Transfer Initialization)
  - Subtype 102 (FTP Client Login Failure)
  - Subtype 103 (FTP Client Session)
  - Subtype 104 (FTP Server Session)
  - Subtype 11 (zERT connection detail records)
  - Subtype 12 (zERT summary records)

- TCP/IP callable NMI (EZBNMIFR)
  - GetConnectionDetail (NWMTCPConnEntry/NWMConnEntry)

© 2019 IBM Corporation

Usage & Invocation (contd.)

- SNMP – ibmMvsTcpConnectionTtlsSslProt MIB object is updated
- SIOCTLSCTL ioctl is updated to return the TLSv1.3 protocol version (X’0304’) in the TTLSi_SSL_Prot field and the negotiated KeyShare in a new TTLSi_Neg_KeyShare field
- zERT Connection Detail (SMF 119-11) and zERT Summary (SMF 119-12) records are also updated to support TLS v1.3

© 2019 IBM Corporation

Dependencies & Coexistence considerations

- Software Dependencies
  - Integrated Cryptographic Services Facility (ICSF)
- Coexistence
  - FIPS 140-2 standard does not define support for TLSv1.3. Enabling both the TLSv1.3 protocol and FIPS support will result in an error

© 2019 IBM Corporation

Session Summary

Security

- AT-TLS support for TLS v.13

© 2019 IBM Corporation

Appendix

z/OS Communications Server Publications

- z/OS Communications Server: New Function Summary GC31-8771
- z/OS Communications Server: IP Configuration Guide SC27-3650
- z/OS Communications Server: IP Configuration Reference SC27-3651
- z/OS Communications Server: IP System Administrator's Commands SC31-8781
- z/OS Communications Server: IP Programmer's Guide and Reference SC31-8787
- z/OS Communications Server: IP Diagnosis Guide GC27-3652
- z/OS Communications Server: IP CICS Sockets Guide SC27-3649
- z/OS Communications Server: IP IMS Sockets Guide SC27-3653
- z/OS Communications Server: IP Sockets Application Programming Interface Guide and Reference SC27-3660

© 2019 IBM Corporation

Appendix

Other Publications

- z/OS UNIX System Services Programming: Assembler Callable Services Reference SA23-2281
- z/OS XL C/C++ Runtime Library Reference SC14-7314
- z/OS Unicode Services User's Guide and Reference SA38-0680

© 2019 IBM Corporation

Key Contacts

- Chief Product Owner
  - Gus Kassimis (kassimis@us.ibm.com)
- Release Manager
  - Doris Bunn (dbunn@us.ibm.com)
- Chief Iteration Manager
  - Navya Ramanjulu (navyaram@us.ibm.com)
- Product Owners
  - Sam Reynolds (samr@us.ibm.com)
  - Chris Meyer (meyerchr@us.ibm.com)
  - Mike Fox (mjfox@us.ibm.com)
- IDD Coordinator
  - Yi Chen Zhang (zhangyic@cn.ibm.com)

© 2019 IBM Corporation

Backup

© 2019 IBM Corporation

AT-TLS policy configuration

- New parameter on the TTLSEnvironmentAdvancedParms and TTLSConnectionAdvancedParms statements: TLSv1.3 On | Off

  Example: TTLSEnvironmentAdvancedParms

  ```
  {
      TLSv1.3 On
  }
  ```

  Default value: Off

- New parameter on the TTLSEnvironmentAdvancedParms statement: MiddleBoxCompatMode On | Off

  Example: TTLSEnvironmentAdvancedParms

  ```
  {
      MiddleBoxCompatMode On
  }
  ```

  Default value: Off

© 2019 IBM Corporation

AT-TLS policy configuration(contd.)

- New V3CipherSuites4Char values on the TTLSCipherParms statement: TLS_AES_128_GCM_SHA256 (1301), TLS_AES_256_GCM_SHA256 (1302) and TLS_CHACHA20_POLY1305_SHA256 (1303)

  Example: TTLSCipherParms

```
{
    V3CipherSuites4Char TLS_AES_128_GCM_SHA256
}
```

- New values and AT-TLS defaults for ClientECurves parameter on the TTLSSignatureParms statement: X25519 (0029) and X448 (0030)

  Defaults when TLSv1.3 is NOT enabled:

  - secp224r1 (0021), secp256r1 (0023), secp384r1 (0024), secp512r1 (0025), secp192r1 (0019)

  Defaults when TLSv1.3 IS enabled:

  - secp224r1 (0021), secp256r1 (0023), secp384r1 (0024), secp512r1 (0025), secp192r1 (0019), X25519 (0029)

© 2019 IBM Corporation

AT-TLS policy configuration(contd.)

- New parameter on the TTLSSignatureParms statement: ClientKeyShareGroups

  Example: TTLSSignatureParms

  ```
  {
      ClientKeyShareGroups secp521r1
  }
  ```

  New AT-TLS Defaults: first one valid for TLSv1.3 from the ClientECurves values (defaulted or configured)

- New parameter on the TTLSSignatureParms statement: ServerKeyShareGroups

  Example: TTLSSignatureParms

  ```
  {
      ServerKeyShareGroups secp521r1
  }
  ```

  New AT-TLS Defaults:

  - secp256r1 (0023), secp384r1 (0024), secp512r1 (0025), X25519 (0029) and X448 (0030)

© 2019 IBM Corporation

AT-TLS policy configuration (contd.)

- New values for SignaturePairs parameter on the TTLSSignatureParms statement: TLS_SIGALG_SHA256_WITH_RSASSA_PSS (0804), TLS_SIGALG_SHA384_WITH_RSASSA_PSS (0805), and TLS_SIGALG_SHA512_WITH_RSASSA_PSS (0806)

  Example: TTLSSignatureParms

  ```
  {
      SignaturePairs TLS_SIGALG_SHA256_WITH_RSASSA_PSS
  }
  ```

  New AT-TLS defaults: Equivalent to System SSL defaults. If TLSv1.3 is enabled, then the three RSASSA_PSS pairs listed above are added to the default list.

- New parameter on the TTLSSignatureParms statement: SignaturePairsCert
  - Values for SignaturePairsCert: Same as SignaturePairs parameter

    Example: TTLSSignatureParms

    ```
    {
        SignaturePairsCert TLS_SIGALG_SHA256_WITH_RSASSA_PSS
    }
    ```

    No defaults

- The above new values are supported on OcspRequestSigAlg and OcspResponseSigAlgPairs also

© 2019 IBM Corporation

AT-TLS policy configuration(contd.)

- Seven new parameters are added to the TTLSGskAdvancedParms specific to Session tickets:
  - GSK_SESSION_TICKET_CLIENT_ENABLE On | Off - Enables session ticket caching when acting as a TLS client
  - GSK_SESSION_TICKET_CLIENT_MAXSIZE *value* - Specifies largest session ticket that can be cached
  - GSK_SESSION_TICKET_SERVER_ENABLE On | Off - Enables the use of session tickets when acting as a TLS server
  - GSK_SESSION_TICKET_SERVER_ALGORITHM *AESCBC128* - Specifies which symmetric encryption algorithm to use to encrypt session tickets
  - GSK_SESSION_TICKET_SERVER_COUNT *value* - Indicates how many session tickets the server uses to send to the client after a successful TLSv1.3 handshake
  - GSK_SESSION_TICKET_SERVER_KEY_REFRESH *value* - Specifies how often in seconds the session ticket encryption key should be refreshed
  - GSK_SESSION_TICKET_SERVER_TIMEOUT *value* - Specifies how long in seconds a session ticket should be honored by the server

© 2019 IBM Corporation