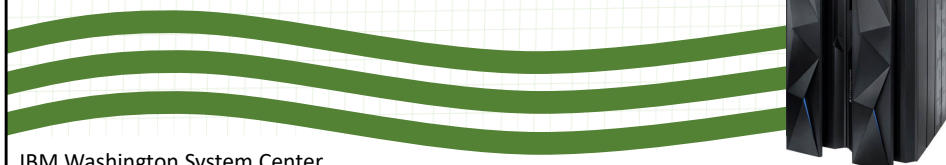


Securing and Encrypting Network Traffic with z/OS Communications Server and Policy Agent

Security Workshop

Application Transparent – Transport Layer Security (AT-TLS)



IBM Washington System Center
IBM Technical Sales Support

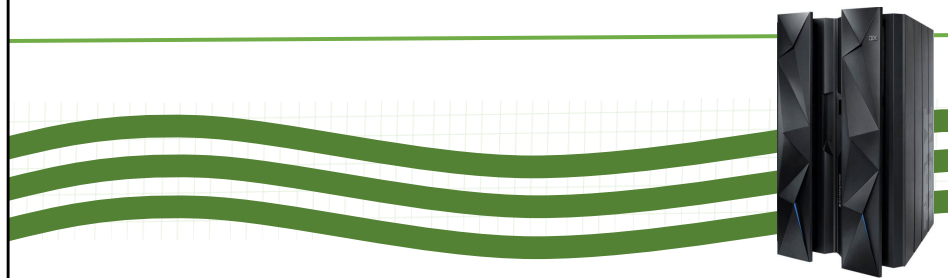
Trademarks

- **The following are Registered Trademarks of the International Business Machines Corporation in the United States and/or other countries.**
 - IBM
 - z/OS
- **The following are trademarks or registered trademarks of other companies.**
 - Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.
- All other products may be trademarks or registered trademarks of their respective companies.
- Refer to www.ibm.com/legal for further legal information.
- OSA-Express Features
- There are many different types of OSA-Express features. In this document where OSA is mentioned it refers to an OSA port on any of the OSA-Express features unless a specific OSA-Express feature is mentioned.

Agenda

- TLS Protocol
- Authentication and Encryption
- AT-TLS Usage
- Network Configuration Assistant for z/OS Communications Server
- Policy Rules and Policy Actions
- FIPS 140
- Error Codes and Commands

TLS Protocol

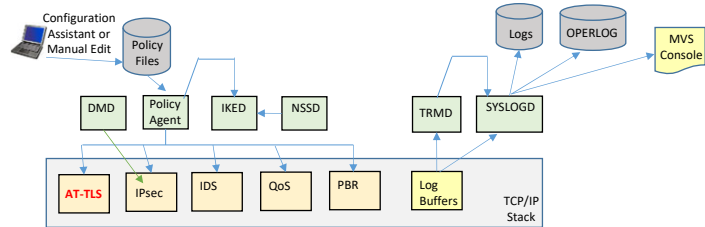


007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 4

Lots of Different Policy Types and Started Tasks



- Policy Agent
 - Installs Policies into the TCP/IP stack
- TCP/IP Stack
 - Enforces the Policies
- DMD (Defense Manager Daemon)
 - ipsec command can be used to install temporary IP Filter rules.
- IKED (Internet Key Exchange Daemon)
 - Required for IPsec Dynamic VPN (Virtual Private Network) Tunnels
- NSSD (Network Security Server Daemon)
 - Required for IKEv2
 - Provides central RACF certificate repository for remote IKED applications
 - Provides DataPower access to RACF
- TRMD (Traffic Regulation Management Daemon)
 - Required for log messages to syslogd for IP Filter, IPsec, and IDS
- SyslogD
 - Recommended for logging

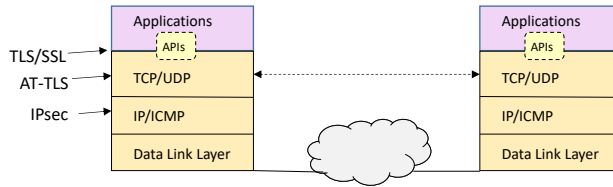
007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 5

Configuration Assistant can really help getting the whole environment setup.

Transport Layer Security (TLS) Protocol Overview



- Open standard transport layer security protocol defined by IETF in RFCs
- Provides authentication, integrity, and data privacy
- Based on Secure Sockets Layer (SSL)
- SSL originally defined by Netscape to protect HTTP traffic
- TLS defines SSL as a version of TLS for compatibility
 - TLS clients and server should drop to SSL V3 based on partner's capabilities
- TCP only
 - UDP, raw IP applications cannot be TLS enabled
- z/OS applications can be modified to support TLS
- Uses System SSL
 - System SSL is part of z/OS Cryptographic Services element
- TLS can be used with no application change by exploiting AT-TLS

007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 6

If encryption for UDP is desired then IPsec should be used instead of AT-TLS.

Using either TLS/SSL or AT-TLS you can provide secure communications for securing the userid, password, the data flows, and even the flows involving transmission of a symmetric session key.

SSL (Secured Sockets Layer) was first introduced by Netscape as a means to authenticate, encrypt, and verify the integrity of data being transferred over the network.

Secure Sockets Layer (SSL) or Transport Layer Security (TLS) requires changes to the client and server applications, and thus applies only to a select number of applications that have chosen to implement the SSL/TLS APIs within the application: WebServer, FTP Server, TN3270 Server, etc. There is an SSL and Sockets API that is invoked by the SSL/TLS-enabled application. This API sits between the application and the TCP, or Transport Control Protocol layer, of the TCP/IP stack.

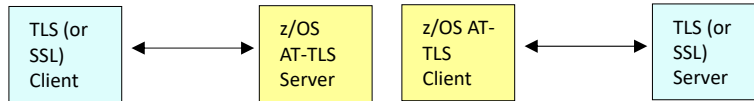
TLS/SSL-Enabled FTP and TN3270 Server and Client provide:

- Secure communication and file transfer by providing encryption, authentication, and message integrity for the FTP control and data connections and for the TN3270 connection.
- FTP can negotiate to use SSL or TLS for control connection only. The Data connection for FTP can be defined to encrypt the data or not. You can even choose to enable or disable the encryption at any time on the Control Connection (typically after the userid and password have flowed while encrypted).
- Both TN3270 and FTP enabled for SSL/TLS strong authentication using X.509 Certificates. With SSL/TLS Client authentication is optional.
- SSL/TLS can be configured in two modes for either TN3270 or FTP:
 - Unconditional - Uses separate ports for non-SSL and SSL
 - Negotiable - Based on subset of the security negotiation functions documented in RFC 2228

The application on z/OS need not be rewritten to invoke security with SSL/TLS. That is why this function is called "Application-Transparent TLS." Although both ends of such a secure connection require the invocation of the SSL APIs, one end could be operating under AT-TLS and the other end under SSL/TLS. Alternatively, both ends could be using AT-TLS.

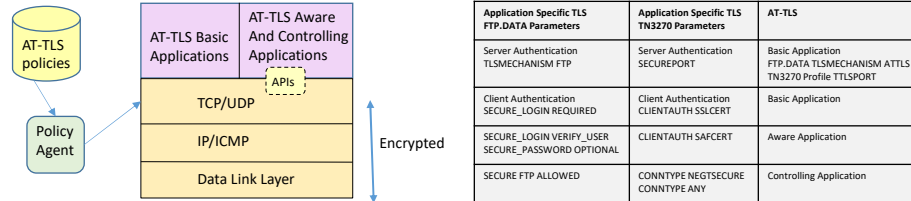
AT-TLS is the function into which new secure features will be introduced. Additional encryption algorithms, additional API functions, and so on can be more easily incorporated with AT-TLS because the applications need not be affected.

AT-TLS is TLS



- AT-TLS happens to be “where” IBM has chosen to implement TLS for various reasons:
 - Consistency between different applications.
 - Support to applications that have not implemented TLS/SSL.
 - Saves development costs.
- AT-TLS is still just seen as a TLS Server or Client to the remote partner.
 - The remote partner sees z/OS as any other TLS or SSL partner.
 - The remote partner still needs to support TLS or SSL.
- TLS, AT-TLS, and SSL use System SSL Support
 - Without System SSL Security Feature Level 3
 - Connections across secure ports are protected only by way of MD5 or SHA hashing algorithms
 - With System SSL Security Feature Level 3
 - Encryption support by way of RC2, RC4, DES, triple DES, AES, etc.
- System SSL Security Feature Level 3
 - Part of z/OS Integrated Security Services element.
 - No charge item but separately orderable feature (export restrictions).
 - TCP/IP must have APF authorized access to the System SSL DLLs (in hlq.SGSKLOAD).

Application Transparent - Transport Layer Security (AT-TLS)



- AT-TLS invokes System SSL TLS processing at the TCP layer for the application
- AT-TLS controlled through policy
 - Installed through policy agent
 - Configured through Configuration Assistant GUI or by manual edit of policy files
- AT-TLS Basic applications
 - For Server Only Authentication or Server with “plain” Client Authentication there is no application change required.
- AT-TLS Aware applications
 - Applications can optionally exploit advanced features using SIOCTLSSLCTL ioctl call.
 - Required for Client Authentication Advanced Features.
 - Extract information (policy, handshake results, x.509 client certificate, userid associated with certificate)
- AT-TLS Controlling applications
 - Required for a single port to concurrently connect to unsecure clients and secure clients
 - Control if/when to start/stop TLS, reset session/cipher

007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 8

AT-TLS is just standard TLS. It is only named AT-TLS to differentiate it from previous TLS support that already existed in FTP and TN3270 and to indicate that it can be implemented without application change for Server Only authentication or Server with “plain” Client Authentication.

AT-TLS Advantages

- Reduces development costs for application TLS exploitation
 - Support of new System SSL functions without application changes
- Single, consistent AT-TLS policy system-wide vs. application specific policy
- Allows TLS-enablement of non-C sockets applications on z/OS (ie. CICS sockets, assembler and callable sockets, etc.)
- Exploits TLS features beyond what some TLS applications choose to support
 - Certificate Revocation List (CRL)
 - Multiple keyrings per server
 - System SSL cache
 - Support for non-DEFAULT certificate by use of LABEL name
 - TLS V1.1 and later
 - FIPS 140 mode
 - RFC 3820 certificate validation
 - RFC 3546 TLS extensions:
 - Truncated HMAC
 - Maximum SSL fragment size
 - Handshake server name indication
 - Ongoing performance improvements

007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 9

Certificate Revocation List (CRL) requires LPAR server.

z/OS Communications Server (CS) FTP and TN3270 “application specific” TLS support has not been updated since z/OS V1.7 when AT-TLS was first available. So everything listed on this chart are capabilities that AT-TLS has that “application specific” TLS support in FTP and TN3270 does not have. Other applications (ie. CICS, WAS, MQ) may have some of these features. You should check with experts for those applications for the TLS support in those specific applications.

There are many advantages to using AT-TLS, including the capability to change keyrings without having to recycle a server that exploits AT-TLS.

Among the more obvious advantages is support for an updated TLS protocol – the TLS version 1.1 protocol level. In combination with System SSL, AT-TLS is also enhanced to aid in addressing FIPS 140-2 requirements – allowing such system SSL capabilities to be configured and used. FIPS 140-2 defines the Security Requirements for Cryptographic Modules. It is published by the National Institute of Standards and Technology(NIST). Security products must be certified and verified against this standard. System SSL provides a mode of operation designed to meet the NIST FIPS 140-2 Level 1 criteria. This criteria has restrictions on the cryptographic algorithms, protocols and key sizes used when securing connections with SSL. System SSL provides an API for applications to invoke System SSL as FIPS 140-2 compliant. AT-TLS has been updated to support a configuration option to allow AT-TLS to be configured as FIPS 140-2 compliant or not.

RFC 4366 defines extensions to the TLS protocol to add functionality. Most of the extensions were created to help clients on wireless networks or other bandwidth or memory restricted environments. The extensions are compatible with earlier versions, meaning TLS implementations which don’t support these extensions will ignore them. The extensions are only supported when TLSv1.0 or TLSv1.1 are negotiated as the security level. A client or server has the option to require an extension be accepted by the remote partner. The connection can be failed if the extension is not supported. This concept is configured using a Required/Optional/Off syntax with AT-TLS. Required indicates the remote partner must support the TLS extension or the TLS handshake fails. Optional indicates the connection is allowed if the remote partner doesn’t support the extension. Off indicates the extension is not supported. The various extensions relate to:

- Security of server_name
- Security of max_fragment_length
- Security of client_certificate_url
- Security of trusted_ca_keys
- Security of truncated_hmac .
- Security of status_request

FIPS 140-2 support requires additional setup for System SSL. Chapter four of the z/OS Cryptographic Services System Secure Sockets Layer Programming manual describes in detail the steps required. All the TLS extensions default to Off. Older implementations of SSL will ignore extensions which they do not support them. Caution should be used when configuring an option as Required, since connections will fail if the remote partner doesn’t support the extension.

Authentication and Encryption



007_ZCS301_AT-TLS

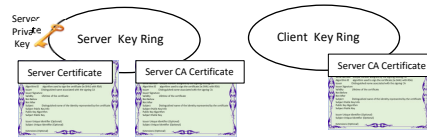
© Copyright IBM Corporation 2023

Page 10

Key Ring Contents

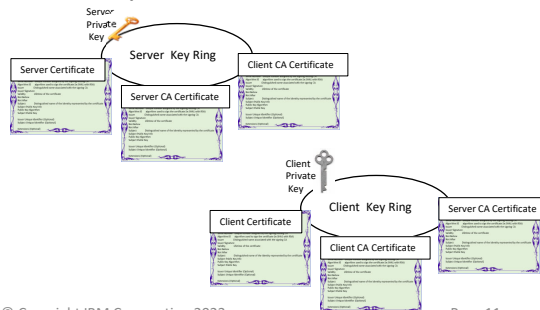
- AT-TLS Server Authentication is required.

- Server
 - Server Certificate
 - Server Private Key
 - Server CA Certificate
- Client
 - Server CA Certificate



- AT-TLS Client Authentication is optional.

- Server
 - Server Certificate
 - Server Private Key
 - Server CA Certificate
 - Client CA Certificate
- Client
 - Client Certificate
 - Client Private Key
 - Client CA Certificate
 - Server CA Certificate



007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

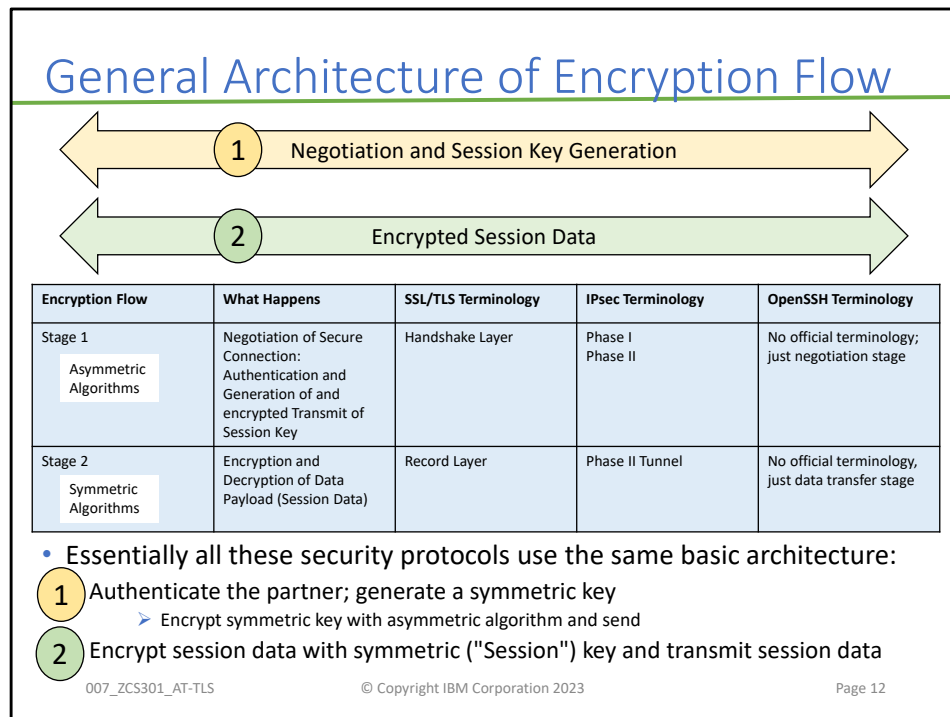
Page 11

The asymmetric algorithms are managed through the x.509 public and private keys that are stored with the x.509 certificates. Server Authentication is required for SSL/TLS or AT-TLS. When server authentication is invoked, both SSL/TLS or AT-TLS partners require a keyring or a key database to hold certificates and encryption keys.

The keyring on the server side contains the Server certificate and the Server CA certificate that has signed the Server certificate. The keyring on the client side contains the Server CA certificate that has signed the Server certificate.

If Client Authentication is invoked, note the contents of the keyrings:

- The keyring on the server side now contains the Server certificate and the Server CA certificate that has signed the Server certificate. However, now it also contains the Client CA certificate that has signed the Client certificate.
- The keyring on the client side now contains not only the Server CA certificate that has signed the Server certificate, but also the Client certificate and the Client CA certificate that has signed the Client certificate.



From the z/OS Security Server RACF Security Administrator's Guide, Chapter 21 "RACF and Digital Certificates":

"Each party, both client and server, has its own certificate, a matching private key, and a list of trusted certificate-authority (CA) certificates. When the client needs to authenticate itself to the server to be able to perform a transaction, both the server and client need to verify one another. The protocol for a secure handshake for mutual verification begins with the parties exchanging certificates. Each party then separately validates the other's certificate to make sure that its signature is valid, that the subject name in the certificate is correct, and that the certificate originated from a trusted certificate authority. If successful, each party must prove to the other that it owns the private key that matches its public key certificate. This step establishes proof of possession and can be accomplished by having each party sign a known unique value, such as a hash of the message traffic between the two parties. If each signature can be validated using the associated public key, the proofs are successful. The final step in this handshake is for one of the parties to generate a random symmetric key, encrypt it using the other party's public key, and send it to the other party. This random symmetric key may then be used to encrypt the data for the remainder of the session. Once the secure handshake is complete, secure transactions can be safely handled in the z/OS environment between this client and server."

SSL is a layered protocol. At each layer, messages may include fields for length, description, content.

There are 2 distinct bounds of communication between the client and server called the handshake layer and the record layer.

In the Handshake Layer the client contacts the server and information is exchanged to determine the capabilities of each and to come to an agreement on possible information required later.

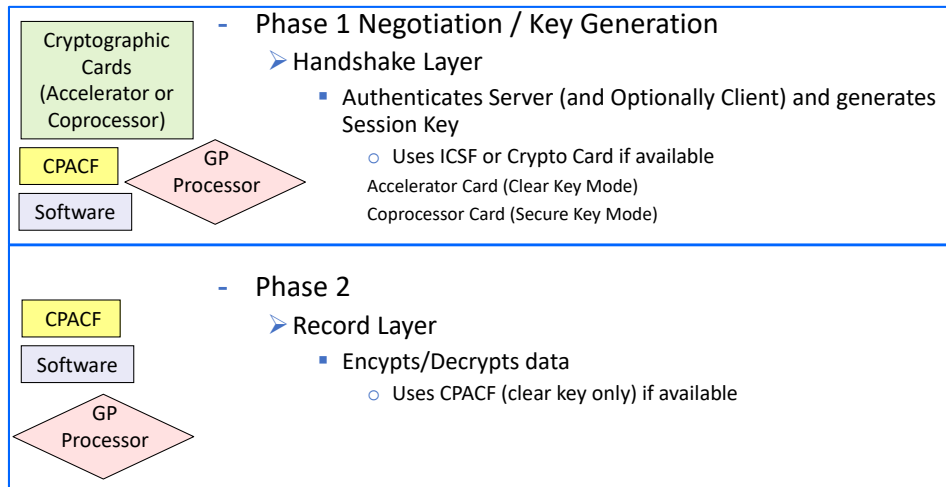
The session (symmetric) key is used to encrypt the Record Layer flows.

In the Record Layer the client and server exchange data, based on the functions selected in the Handshake Layer. Data protected is:

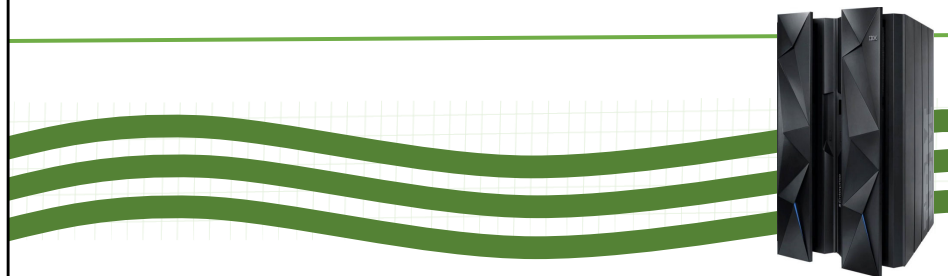
- the userid
- the password
- the actual data payload

AT-TLS

- Two Stages



AT-TLS Usage

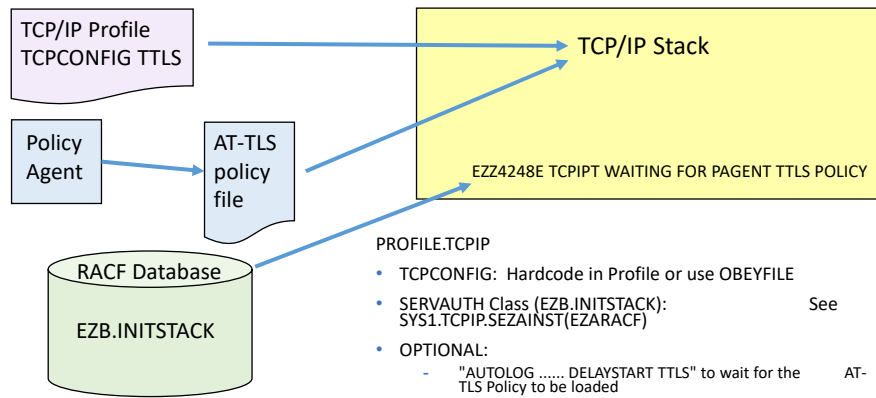


007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 14

Enable TCP/IP Stack for AT-TLS



- Reduce AT-TLS overhead by adding this to the TCP/IP proc:

`//CEEOPDS DD * HEAPPOLLS64(ON)`

007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 15

This page shows you that there are several pre-requisites for the TCP/IP stack if it is to run with AT-TLS policies:

- The SERVAUTH class of EZB.INITSTACK may be defined and users and jobs must be authorized to it.
- The TCPCONFIG statement must be coded with TTLS.

IMPORTANT: The TCPCONFIG Statement may be inserted with an OBEYFILE command:

- `V TCPIP,,O,SYS1.TCPPARMS(OBEYTTLS)`

When TCPCONFIG TTLS is defined in the initial TCPIP.PROFILE, the INITSTACK profile may be defined. Policy Agent and any socket based programs it requires, must be permitted to this resource. Other programs or users that do not need to wait for TTLS policy to be installed in the stack may be permitted to this resource. Users that are not permitted to this resource, will not be able to open sockets on this stack until TTLS policy is installed. When the resource is not defined, no stack access is permitted.

Look in hlq.SEZAINST for the EZARACF sample that will help you define SERVAUTH, also consult the IP Configuration Guide.

Once the policy files are created you would normally perform the following steps:

- FTP the files to the mainframe to an MVS dataset member or to unix files.
- Implement SYSLOG daemon.
- Implement Traffic Regulation Management Daemon.
- Implement the running Policy Agent and test with the files you configured on your workstation.

When AUTOLOG with a DELAYSTART TTLS has been coded for certain procedures, they will not start initializing until the AT-TLS policies are loaded. When this TTLS subparameter is specified, the procedure starts after the Policy Agent has successfully installed the AT-TLS policy in the TCP/IP stack and AT-TLS services are available.

RACF Sample

- SYS1.TCPIP.SEZAINST(EZARACF)

```

...
//*INITSTAC EXEC PGM=IKJEFT01
//*SYSTSPRT DD SYSOUT=*
//*SYSTSIN DD *
//* SETROPTS CLASSACT(SERVAUTH)
//* SETROPTS RACLIST (SERVAUTH)
//* SETROPTS GENERIC (SERVAUTH)
//* RDEFINE SERVAUTH EZB.INITSTACK.sysname.tcpprocname UACC(NONE)
//* PERMIT EZB.INITSTACK.sysname.tcpprocname -
//* CLASS(SERVAUTH) ID(PAGENT) ACCESS(READ)
//* PERMIT EZB.INITSTACK.sysname.tcpprocname -
//* CLASS(SERVAUTH) ID(OMPROUTE) ACCESS(READ)
//* PERMIT EZB.INITSTACK.sysname.tcpprocname -
//* CLASS(SERVAUTH) ID(OSNMPP) ACCESS(READ)
//* PERMIT EZB.INITSTACK.sysname.tcpprocname -
//* CLASS(SERVAUTH) ID(IOSNMP) ACCESS(READ)
//* PERMIT EZB.INITSTACK.sysname.tcpprocname -
//* CLASS(SERVAUTH) ID(NAMED) ACCESS(READ)
//* PERMIT EZB.INITSTACK.sysname.tcpprocname -
//* CLASS(SERVAUTH) ID(IKED) ACCESS(READ)
//* SETROPTS GENERIC(SERVAUTH) REFRESH
//* SETROPTS RACLIST(SERVAUTH) REFRESH
//*
...

```

SETROPTS CLASSACT(SERVAUTH)
 EZB.INITSTACK.sysname.tcpname
 PERMIT EZB.INITSTACK.sysname.tcpname CL(SERVAUTH) ID(userid)
 At a minimum, the following applications must be permitted to the profile:
 Policy Agent
 OMPROUTE
 SNMP subagent

SERVAUTH class EZB.INITSTACK prevents TCP/IP stack access until after the Policy Agent has come up and installed the AT-TLS policies. PERMIT must be defined for the Policy Agent and any other applications that need access to the stack prior to policy load.

007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 16

When TCPCONFIG TTLS is defined in the initial TCPIP.PROFILE, the INITSTACK profile should be defined. Policy Agent and any socket based programs it requires, must be permitted to this resource. Other programs or users that do not need to wait for TTLS policy to be installed in the stack may be permitted to this resource. Users that are not permitted to this resource, will not be able to open sockets on this stack until TTLS policy is installed. When the resource is not defined, no stack access is permitted. Checking is done only if the TCP/IP profile activates AT-TLS. If there is no profile in the SERVAUTH class covering this resource name, all socket requests fail, including those from Policy Agent. Checking ceases the first time that the Policy Agent indicates AT-TLS policy is complete, or if a TCP/IP profile change deactivates AT-TLS. When the limited access window begins, non-scrollable message EZZ4248E is written to the system console stating that TCP/IP is waiting for Policy Agent to install AT-TLS policies. The message is released when the restriction ends. You can delay the start of AUTOLOG procedures during this window of time by specifying the optional DELAYSTART parameter with the TTLS subparameter on the AUTOLOG entry for that procedure; when specified, the procedure will start after the EZZ4248E message is deleted and message EZZ4250I is issued indicating that AT-TLS services are available.

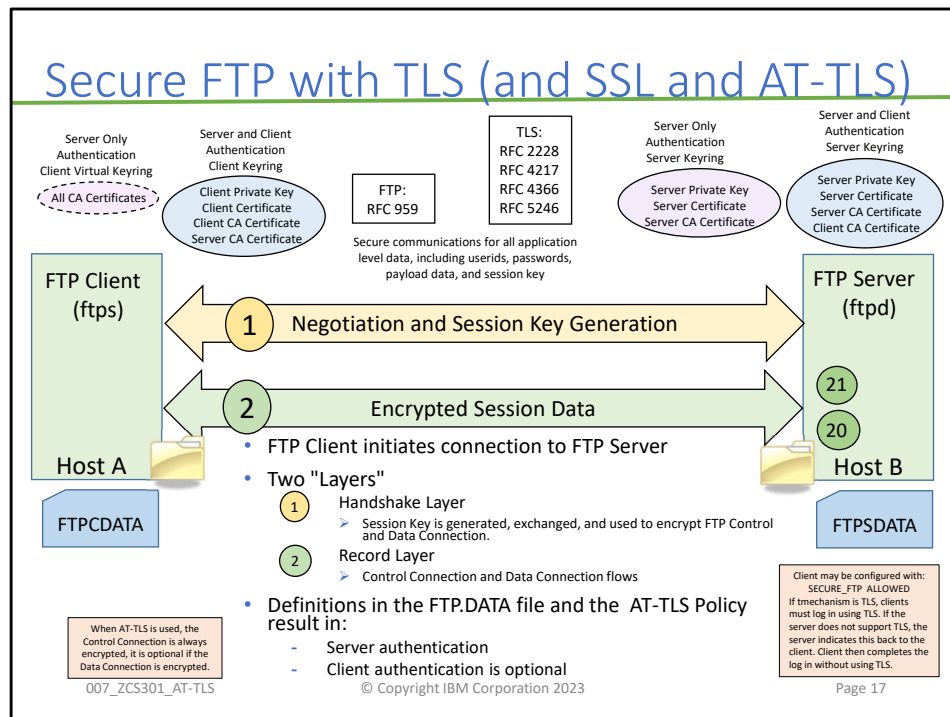
You must permit a limited set of administrative applications to the profile to ensure full initialization of the stack. If Policy Agent is dependent on other applications in your environment, they must also be permitted. You can permit other applications that do not require AT-TLS and that you want to start prior to general applications.

At a minimum, the following applications must be permitted to the profile:

- Policy Agent
- OMPROUTE
- SNMP subagent

Look in hlq.SEZAINST for the EZARACF sample that will help you define SERVAUTH for AT-TLS..

Also consult the IP Configuration Guide and the appropriate Red Books.



This diagram is a general representation of connections using SSL, TLS, or AT-TLS to secure the traffic between an FTP client and server.

The FTP Client initiates a connection to the FTP Server.

Two "Layers" or phases occur for such a secured transfer.

- Handshake Layer (negotiation of keys, other security parameters)
 - Session Key is generated, exchanged, and used to encrypt FTP Control and Data Connection.
- Record Layer (actual transfer of data payload)

If using AT-TLS, the AT-TLS Policy together with the FTP.DATA file results in:

- Server authentication
- Client authentication is optional

If Client authentication is not required, the client end of the connection can identify a Virtual RACF keyring.

If using a virtual keyring, the Server CA is found as a trusted CA certificate in the RACF DIGTCERT class of the Client end-entity.

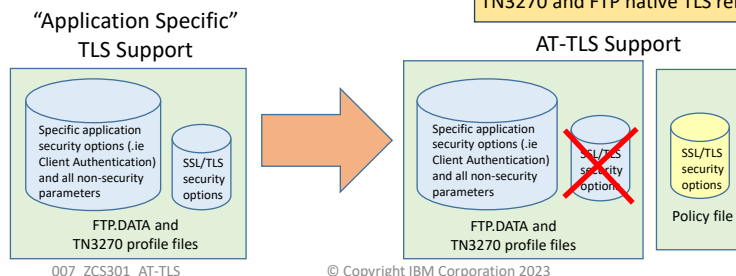
If not using Client authentication, the Client CA certificate is not necessary on the Server Ring.

If Client authentication is required by the Server, the Client Keyring contains the server CA certificate, the Client CA certificate, the Client Certificate, and the Client Private Key.

AT-TLS Enabling for TN3270 and FTP

- Both the FTP server and client, and the TN3270 server on z/OS currently (and prior to AT-TLS) have “application specific” SSL/TLS support.
 - With the advantages of AT-TLS, it is desirable to migrate that SSL/TLS support to AT-TLS.
- FTP and TN3270 are enabled for AT-TLS to be AT-TLS “Aware” and “Controlling” applications.
- “Move” the SSL/TLS-specific configuration from FTP.DATA and TN3270 profile into the common AT-TLS policy format.
- Keep application-specific security options in FTP.DATA and TN3270 profile application configuration files.

TN3270 and FTP native TLS removed in z/OS V2.5.



007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 18

FTP and TN3270 should be migrated from “application specific” TLS support to AT-TLS.

With SSL/TLS the application configuration contains ALL the SSL/TLS options and specifications.

With the advantages of AT-TLS, it is desirable to migrate that SSL/TLS support to AT-TLS.

With AT-TLS that is either aware or controlling, the application configuration contains some of the application-specific security definitions. The rest of the SSL/TLS security definitions are placed in an AT-TLS policy.

With Basic AT-TLS, all the SSL/TLS configuration statements are defined in the AT-TLS policy.

FTP and TN3270 are enabled to be AT-TLS aware and controlling.

AT-TLS requires that the TCP/IP stack enable AT-TLS and that additional controls be set up in the Security Access Facility (SAF).

Enable AT-TLS in the TCP/IP Stack: Set TCPCONFIG TTLS in PROFILE.TCPIP.

Enable INITSTACK Controls: EZB.INITSTACK.sysname.tcpname in the SERVAUTH class

Approach used for enabling FTP and TN3270 for AT-TLS

- “Move” the SSL/TLS Security Options into the AT-TLS policy format
- You can even maintain one common policy format where new options can be added without changes to all applications
- Keep application-specific security options in application configuration if you need the function of AT-TLS Aware or AT-TLS controlling.

Enabling FTP for AT-TLS

- FTP Server and Client

FTP.DATA

Some Security Statements Remain:
EXTENSIONS AUTH_TLS (Server only)
SECURE_CTRLCONN (Client and Server)
SECURE_DATACONN PRIVATE (Client and Server)
SECURE_FTP REQUIRED (Client and Server)
SECURE_HOSTNAME (Client only)
SECUREIMPLICITZOS (Client and Server)
SECURE_LOGIN (Server only)
SECURE_MECHANISM TLS (Client only)
SECURE_PASSWORD (Server only)
SECURE_PBSZ (Client and Server)
SECURE_SESSION_REUSE (Client and Server)
TLSMECHANISM ATTLS (Client and Server)
TLSPORT (Client and Server)
TLSRFCLEVEL RFC4217 (Client and Server)

Some Security Statements can be removed,
because they are defined in Policy:
CIPHERSUITE (Client and Server)
KEYRING (Client and Server)
TLSTIMEOUT (Client and Server)

007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 19

FTP.DATA option to instruct the FTP server or client to use AT-TLS instead of FTP's own system SSL calls is implemented:

- TLSMECHANISM (Client and Server)
 - TLS MECHANISM FTP is native SSL/TLS support
 - TLS MECHANISM TTLS is AT-TLS support

When TTLS is specified as TLS mechanism:

- FTP becomes an AT-TLS-controlling and AT-TLS-aware application
- All the FTP-specific security options will continue to impact how FTP operates
- The SSL/TLS security options in FTP.DATA will be ignored.
- Matching AT-TLS policies need to be defined before enabling AT-TLS support in FTP

FTP-specific security options:

- TLSMECHANISM
- EXTENSIONS AUTH_TLS (Server)
- SECURE_CTRLCONN (Client and Server)
- SECURE_DATACONN (Client and Server)
- SECURE_FTP (Client and Server)
- SECURE_HOSTNAME (Client)
- SECURE_LOGIN (Server)
- SECURE_MECHANISM (Client)
- SECURE_PASSWORD (Server)
- SECUREIMPLICITZOS (Client)
- TLSPORT (Client and Server)

FTP SSL/TLS security options NOW SPECIFIED IN POLICY FILE

- CIPHERSUITE (Client and Server)
- KEYRING (Client and Server)
- TLSTIMEOUT (Client and Server)

Enabling TN3270 for AT-TLS

TN3270 Profile TELNETPARMS

PORT port_num or
SECUREPORT port_num must be changed to:
TTLSPORT port_num

Some Security Statements Remain:
CONNTYPE SECURE | NEGTCURE ...
DEBUG CONN DETAIL
EXPRESSLOGON
EXPRESSLOGONMFA
RESTRICTAPPL CERTAUTH

Some Security Statements can be removed,
because they are defined in Policy:

ENCRYPTION
KEYRING
TLSTIMEOUT, SSLTIMEOUT
CRLLDAPSERVER
CLIENTAUTH SSLCERT | SAFCERT
SSLV2 | NOSSLV2
SSLV3 | NOSSLV3

- **TTLSPORT** signifies AT-TLS for this port
 - You may use SECUREPORT on other ports
- When first testing, optionally enable **DEBUG CONN**
- **BEGINVTAM** remains unchanged.

007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 20

Just as FTP has many security features outside of AT-TLS, so does TN3270. Please read up on these features in the available IBM manuals and Red Books. We discuss only AT-TLS here.

AT-TLS Support for TN3270:

- Dynamically refresh a key ring.
- Support new or multiple key rings.
- Specify the label of the certificate to be used for authentication instead of using the default.
- Support SSL session key refresh.
- Support SSL session reuse.
- Support SSL sysplex session ID caching.
- Trace decrypted SSL data for Telnet in a data trace.
- Receive more granular error messages in syslog for easier debugging.
- Policy Agent must be active.
- TLS security defined within the TN3270 profile will continue to be available and can be implemented concurrently with AT-TLS.

In the TN3270 PROFILE you code the Security parameters in the TELNETPARMS.

For testing it is sometimes helpful to enable TELNET debug options: **DEBUG CONN**

Note: If you have security parameters in a PARMSGROUP statement mapped to host names, you will not be able to emulate that mapping with AT-TLS. If you are not using PARMSGROUP to map to host names, we urge you to migrate to the use of AT-TLS as a consistent solution for all of your TCP applications.

TN3270 server option indicates use of AT-TLS instead of the TN3270 server's own system SSL calls:

- **TTLSPORT**

CONNTYPE retains its current meaning for a **TTLSPORT**.

When **TTLSPORT** is used for a TN3270 server port:

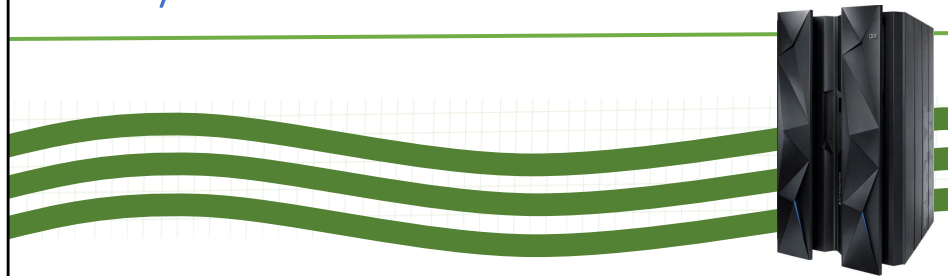
- The TN3270 server becomes an AT-TLS controlling and AT-TLS aware application
- All the TN3270-specific security options will continue to impact how TN3270 operates
- Any TN3270 server SSL/TLS security options will be ignored, but you may see conflicts if you have left them in place.

Matching AT-TLS policies need to be defined before enabling AT-TLS support for the TN3270 server

- **CIPHERSUITE** (Server)
- **KEYRING** (Server)
- **TLSTIMEOUT** (Server)

Note that the linemode **TELNET** from the ISPF Option 6 is a PASCAL operation and is unable to implement either SSL/TLS or AT-TLS.

Network Configuration Assistant for z/OS Communications Server

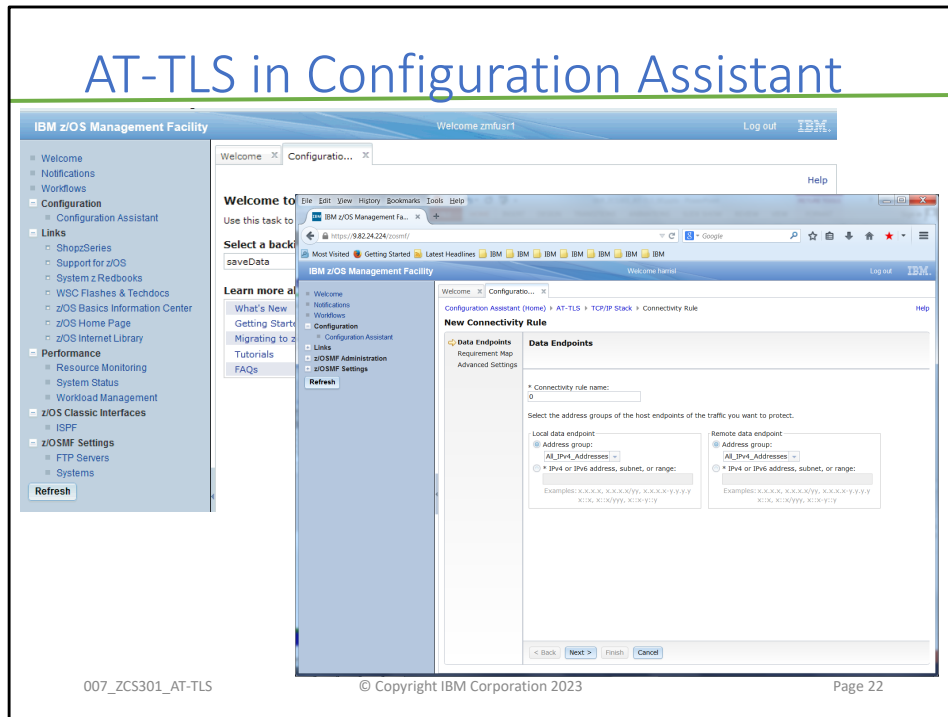


007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 21

AT-TLS in Configuration Assistant

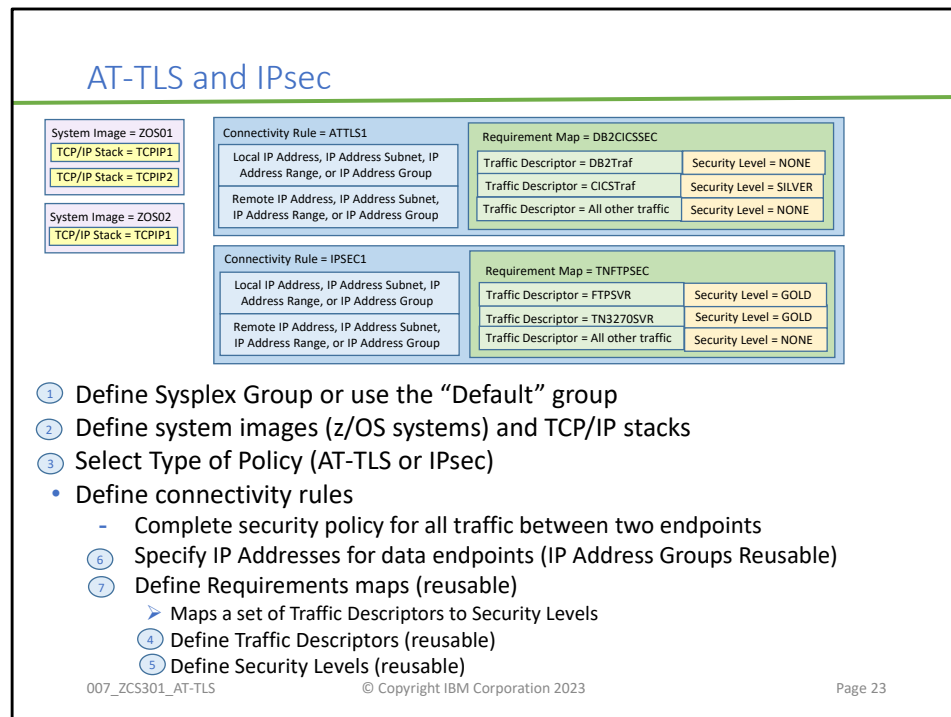


When you initialize the IBM Configuration Assistant, you are asked to define the environment for which the policy objects and rules will be built.

You define the z/OS images and the TCP/IP stacks within those images.

You are supplied with IBM-furnished Requirement Maps, Traffic Descriptors, and Security Levels.

You may also modify these or build your own.



There are Wizards that start for each section with a set of panels that must be completed to create the selected item. Wizards and dialogs guide you through a top-down approach to the configuration. The order depicted on the chart above. Navigational tree supports a bottom-up approach to allow an experienced user to bypass wizard screens. Navigational tree appears on the left hand side of the Window.

Policy Rules and Policy Actions



007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 24

Policy Definition

Criteria	Description
Resource Attributes	
Local address	Local IP Address
Remote address	Remote IP Address
Local port	Local Port
Remote port	Remote Port
Connection Type Attributes	
Connection direction	<ul style="list-style-type: none">• Inbound (applied to first Select, Send, or Receive after Accept)• Outbound (applied to Connect)• Both
Application Attributes	
User ID	User ID of the owning process or wildcard user ID.
Jobname	Jobname of the owning application or wildcard jobname.
Time Condition	
Time, Day, Week, Month	When filter rule is active.
Action	
Encryption Algorithm	Which encryption algorithm to use.
Hashing Algorithm	Which hashing algorithm to use.
Client Authentication	Designates whether Client Authentication is Required or Not

[illegible]

- 007_ZCS301_AT-TLS

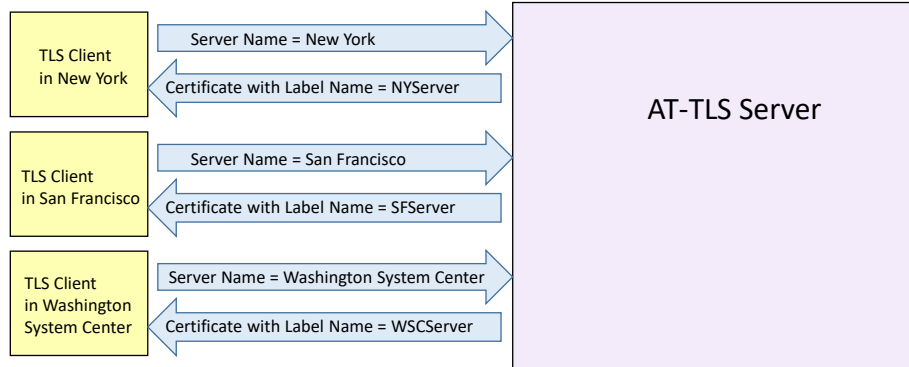
© Copyright IBM Corporation 2023

Page 26

Alternatively you can directly code this in the policy and then issue a MODIFY UPDATE:

- On `TTLSEnvironmentAction` or `TTLSEnvironmentAdvancedParms` in the flat file, specify "EnvironmentUserInstance"
- `EnvironmentUserInstance`: Defines a configurable instance identifier for this `TTLSEnvironmentAction` statement. The `n` value can be in the range 0 - 65 535. This parameter can be used to signal a change to the Policy Agent without modifying any of the other AT-TLS configuration statements. For example, when the contents of the key ring has changed, but the key ring name is unchanged. Adding or updating the `EnvironmentUserInstance` parameter would signal Policy Agent to install a new `TTLSEnvironmentAction` statement. This parameter can also be used as a field to be updated when a change is made to this `TTLSEnvironmentAction` statement. This enables the user to differentiate `TTLSEnvironmentAction` statements, based on the instance identifier.

Server Name Indication



- The server matches the server name provided by the client with a certificate label and sends that certificate to the client (RFC4366).

007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 27

A Telnet server can now host multiple customers on the same ports or IP addresses or on multiple IP addresses. This can happen when servers are consolidated or domain names changed. The certificate used by the server has a host name defined within it, which clients can validate against. If the client is using a host name which doesn't match the certificate, error or warning messages can be issued. The server has very limited options on selecting which certificate to send to a client.

Server Named Indication(SNI) allows the client to include a host name in the extended TLS handshake, indicating the host name the client is connecting to. The server can then select a certificate based on the host names provided by the client. The server is configured with a list of host names and a certificate labels for each host name. The server selects the certificate which matches the host name used by the client.

If the SSL server needs to support multiple host names and multiple certificates, you can use the Server Name Indication function.

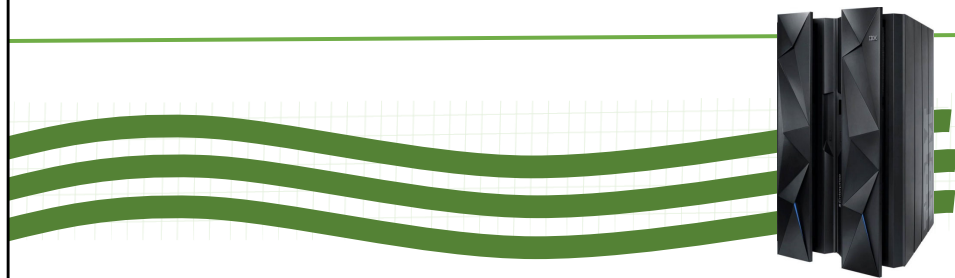
The Server Name Indication function enables you to define pairs of certificate labels and host names. Use the

ServerHandshakeSNIList parameter to specify these pairs.

The SSL client must support the Server Name Indication function as well. The SSL client includes a host name during the SSL handshake, which allows the matching certificate to be used.

When AT-TLS supports a client, you can use the HandshakeServerName parameter to specify the host name to be included in the SSL handshake.

FIPS 140



007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 28

FIPS 140 Requirements

- You can configure AT-TLS to support FIPS 140.
 - Specify On for the FIPS140 statement of the TTLSGroupAction statement, or
 - Specify on a Configuration Assistant panel
- Understand System SSL Restrictions for FIPS 140
 - Consult z/OS System SSL Programming Guide
 - Restricted to specific encryption and hashing algorithms
 - No DES, no MD5, etc...
 - SSL V2 and SSL V3 are not supported.
 - System SSL requires Security Level 3 FMID (JCPT3C1)
 - Recommended: Initialize ICSF

007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 29

Hardware cryptographic functions allowed in FIPS mode support clear keys only. Secure keys stored in ICSF's PKDS are not supported.

Nevertheless, it is recommended for ease of implementation to initialize ICSF on behalf of FIPS 140.

System SSL Algorithm Support for FIPS 140

Non-FIPS					FIPS			
Algorithm	Sizes	System SSL software	Direct calls to CPACF	Support through ICSF	Sizes	System SSL software	Direct calls to CPACF	Support through ICSF
3DES	168	X	X		168	X	X	
AES	128 and 256	X	X		128 and 256	X	X	
AES-GCM	128 and 256			X	128 and 256			X
DES	56	X	X					
DH	512-2048	X			2048			X
DSA	512-2048	X			1024-2048	X		
ECC Brainpool	160-521			X				
MD5	48	X						
NIST ECC	192-521				192-521			X
RC2	40 and 128	X						
RC4	40 and 128	X						
RSA	512-4096	X		X	1024-4096	X		X
RSASSA-PSS	2048-4096			X	2048-4096			X
SHA-1	160	X	X		160	X	X	
SHA-2	224, 256, 384, and 512	X	X		224, 256, 384, and 512	X	X	

See z/OS Cryptographic Services System Secure Sockets Layer Programming, SC14-7495, for the latest support.
007_ZCS301_AT-TLS © Copyright IBM Corporation 2023 Page 30

When executing in FIPS mode, System SSL continues to take advantage of the CP Assist for Cryptographic Function (CPACF) when available. Cryptographic functions performed by ICSF-supported hardware when running in non-FIPS mode continue to be exploited when executing in FIPS mode apart from RSA signature generation which must be performed in software. Hardware cryptographic functions allowed in FIPS mode support clear keys only. Secure keys stored in ICSF's PKDS (Public Key Data Set) are not supported.

Error Codes and Commands



007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 31

AT-TLS Error Codes

- Return codes between 5001 and 5999 describe AT-TLS errors that can be corrected by the user.
- Return codes between 6001 and 6999 describe internal AT-TLS errors.
- Table 53 lists some common System SSL return codes and possible causes.

Return code	Event	Possible cause and solution
202	Environment Init	<p>The key ring cannot be opened because the user does not have permission. Check the following:</p> <ul style="list-style-type: none"> - Look at message ESD1281 to verify the user ID being used for this connection and the TLSEnvironmentAction statement mapped to this connection. If you are configuring using the z/OS Configuration Assistant for z/OS Communications Server, you can specify the key ring on either the AT-TLS Image Level Settings panel or on each Traffic Descriptor. - Ensure that the correct key ring has been specified. - If using RACF key ring, verify that all the steps in z/OS Communications Server: IP Configuration Guide have been followed for this user ID.

- Consult IP Diagnosis for z/OS (GC27-3652)
 - Lists common SSL/TLS Error Codes
- Consult Cryptographic Services Secure Sockets Layer Programming for z/OS
 - Lists all the SSL/TLS Error Codes

007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 32

The System SSL Error Codes and the z/OS Communications Server messages are helpful for resolving SSL/TLS errors. Below you see the full text of a section of the IP Diagnosis manual, which contains a listing of the most common SSL errors. You will find the same error codes and more described in the SSL Programming manual.

"AT-TLS error message ESD1286I is issued to syslogd to report any errors that occur on a AT-TLS connection when the trace level 2 (Error) is set.

AT-TLS error message ESD1287I is issued to the TCP/IP joblog to report any errors that occur on an AT-TLS connection when the trace level 1 (Error) is set.

These messages include the event that AT-TLS was processing and the return code indicating a failure.

Return codes between 5001 and 5999 describe AT-TLS errors that can be corrected by the user.

Return codes between 6001 and 6999 describe internal AT-TLS errors.

Contact IBM with the error message and syslog information, if available. Any other return code is defined by System SSL. Refer to z/OS Cryptographic Service System Secure Sockets Layer Programming for additional information on these return codes.

Commands for AT-TLS

- UNIX commands
 - pasearch -t
- MVS Commands
 - D TCPIP,,N,TTLS
 - D TCPIP,<tnproc>,T,PROF,DETAIL
 - D TCPIP,<tnproc>,T,CONN
 - D TCPIP,<tnproc>,T,CONN,CONN=<connection number>
 - D TCPIP,<tnproc>,T,CONN,CONN=<connection number>,DETAIL

Please consult the IP System Administrator's Guide for more examples. Also use the IBM Red Books for hints and tips.

End of Topic



007_ZCS301_AT-TLS

© Copyright IBM Corporation 2023

Page 34