



# Leveraging z/OS Communications Server Application Transparent Transport Layer Security (AT-TLS) for a Lower Cost and More Rapid TLS Deployment

December 15, 2011

Lin Overby – [overbylh@us.ibm.com](mailto:overbylh@us.ibm.com)  
z/OS Communications Server



## Trademarks, notices, and disclaimers

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

- |  |   |   |  |   |
|--|---|---|--|---|
| <ul style="list-style-type: none"><li>Advanced Peer-to-Peer Networking®</li><li>AIX®</li><li>alphaWorks®</li><li>AnyNet®</li><li>AS/400®</li><li>BladeCenter®</li><li>Candle®</li><li>CICS®</li><li>DataPower®</li><li>DB2 Connect</li><li>DB2®</li><li>DRDA®</li><li>e-business on demand®</li><li>e-business (logo)</li><li>e business (logo)®</li><li>ESCON®</li><li>FICON®</li></ul> | <ul style="list-style-type: none"><li>GDDM®</li><li>GDPS®</li><li>Geographically Dispersed Parallel Sysplex</li><li>HiperSockets</li><li>HPR Channel Connectivity</li><li>HyperSwap</li><li>i5/OS (logo)</li><li>i5/OS®</li><li>IBM eServer</li><li>IBM (logo)®</li><li>IBM®</li><li>IBM zEnterprise™ System</li><li>IMS</li><li>InfiniBand ®</li><li>IP PrintWay</li><li>IPDS</li><li>iSeries</li><li>LANDP®</li></ul> | <ul style="list-style-type: none"><li>Language Environment®</li><li>MQSeries®</li><li>MVS</li><li>NetView®</li><li>OMEGAMON®</li><li>Open Power</li><li>OpenPower</li><li>Operating System/2®</li><li>Operating System/400®</li><li>OS/2®</li><li>OS/390®</li><li>OS/400®</li><li>Parallel Sysplex®</li><li>POWER®</li><li>POWER7®</li><li>PowerVM</li><li>PR/SM</li><li>pSeries®</li><li>RACF®</li></ul> | <ul style="list-style-type: none"><li>Rational Suite®</li><li>Rational®</li><li>Redbooks</li><li>Redbooks (logo)</li><li>Sysplex Timer®</li><li>System i5</li><li>System p5</li><li>System x®</li><li>System z®</li><li>System z9®</li><li>System z10</li><li>Tivoli (logo)®</li><li>Tivoli®</li><li>VTAM®</li><li>WebSphere®</li><li>xSeries®</li><li>z9®</li><li>z10 BC</li><li>z10 EC</li></ul> | <ul style="list-style-type: none"><li>zEnterprise</li><li>zSeries®</li><li>z/Architecture</li><li>z/OS®</li><li>z/VM®</li><li>z/VSE</li></ul> |
|--|---|---|--|---|
- \* All other products may be trademarks or registered trademarks of their respective companies.

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

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

### Notes:

- Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
- IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
- All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
- All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
- Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

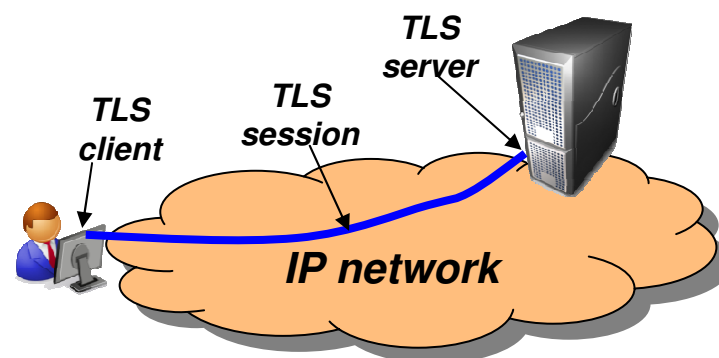
Refer to [www.ibm.com/legal/us](http://www.ibm.com/legal/us) for further legal information.

## Agenda

- **SSL/TLS Overview**
- **What is AT-TLS?**
- **Why use AT-TLS?**
- **How does AT-TLS work?**
- **Configuring AT-TLS**

# Transport Layer Security (TLS/SSL) overview

- Transport Layer Security (TLS) is defined by the IETF \*\*
  - Based on Secure Sockets Layer (SSL)
    - TLS defines SSL as a version of TLS for compatibility
- Provides secure connectivity two TLS security session endpoints
  - TLS session
- Full application payload encryption and data authentication / integrity
- TLS security session endpoint plays either a client or server role
- Session endpoint authentication typically via X.509 certificates
  - Server authentication required
  - Client authentication optional (mutual authentication)



Full application payload encryption

TLS/SSL encryption:

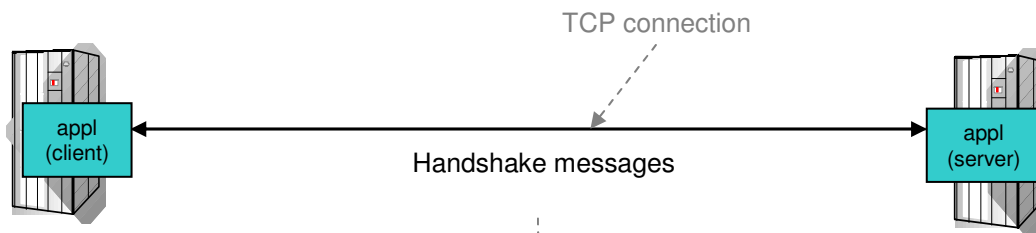
SrcIP	DestIP	SrcPort	DestPort	Data
192.168.100.1	192.168.1.1	50002	443	@%\$#*&&^^!:"J)*GVM><

**\*\* For our purposes, SSL and TLS are equivalent and one term implies the other**

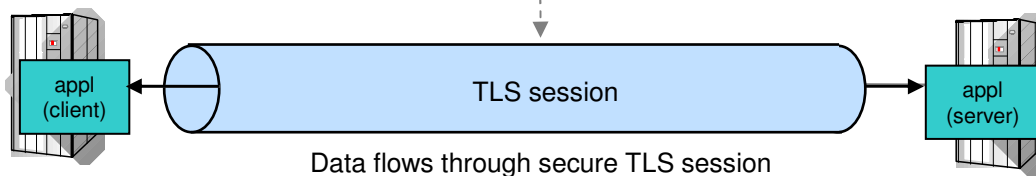
# TLS/SSL protocol basics

- 1 Client application initiates TLS handshake which authenticates the server (and, optionally, client) and negotiates a cipher suite to be used to protect data

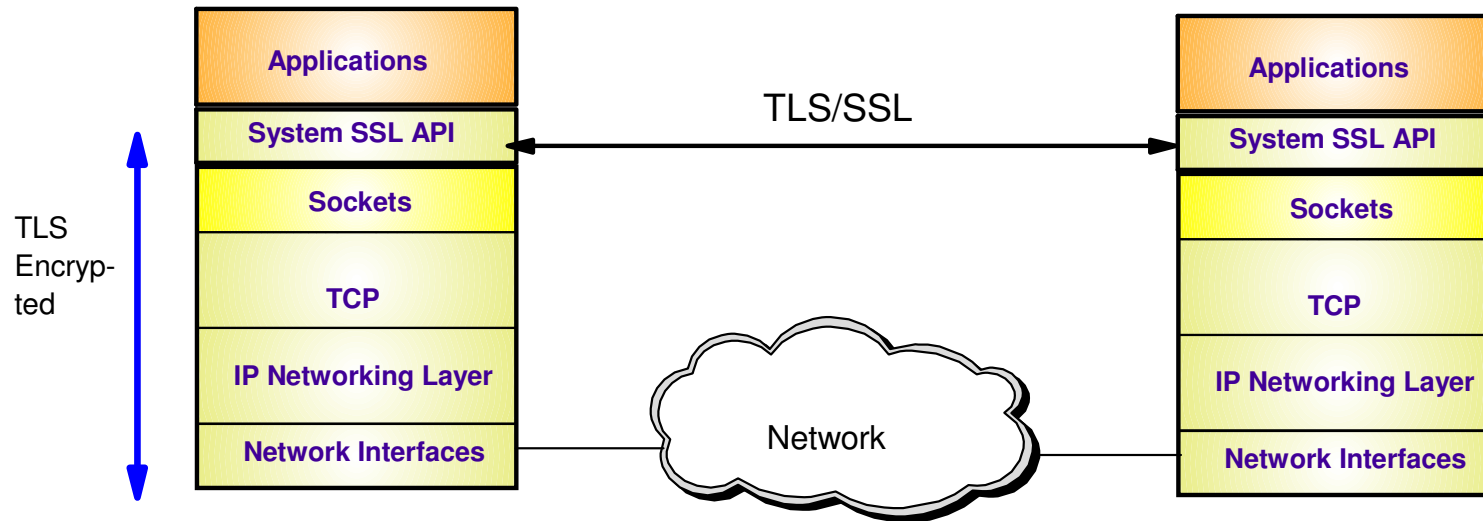
Upon successful completion of the handshake, a secure TLS session exists for the application partners



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



# Transport Layer Security enablement



- TLS traditionally provides security services as a socket layer service
  - TLS requires reliable transport layer,
    - Typically TCP (but architecturally doesn't have to be TCP)
  - UDP applications cannot be enabled with traditional TLS
    - There is now a TLS variant called Datagram Transport Layer Security (DTLS) which is defined by the IETF for unreliable transports
- On z/OS, System SSL (a component of z/OS Cryptographic Services) provides an API library for TLS-enabling your C and C++ applications
- Java Secure Sockets Extension (JSSE) provides libraries to enable TLS support for Java applications
  - However, there is an easier way...

**... Application Transparent TLS!**

# z/OS Application Transparent TLS overview



## Stack-based TLS

- TLS process performed in TCP layer (via System SSL) without requiring any application change (transparent)
- AT-TLS policy specifies which TCP traffic is to be TLS protected based on a variety of criteria
  - Local address, port
  - Remote address, port
  - Connection direction
  - z/OS userid, jobname
  - Time, day, week, month

## Application transparency

- Can be fully transparent to application
- An optional API allows applications to inspect or control certain aspects of AT-TLS processing – “application-aware” and “application-controlled” AT-TLS, respectively

## Available to TCP applications

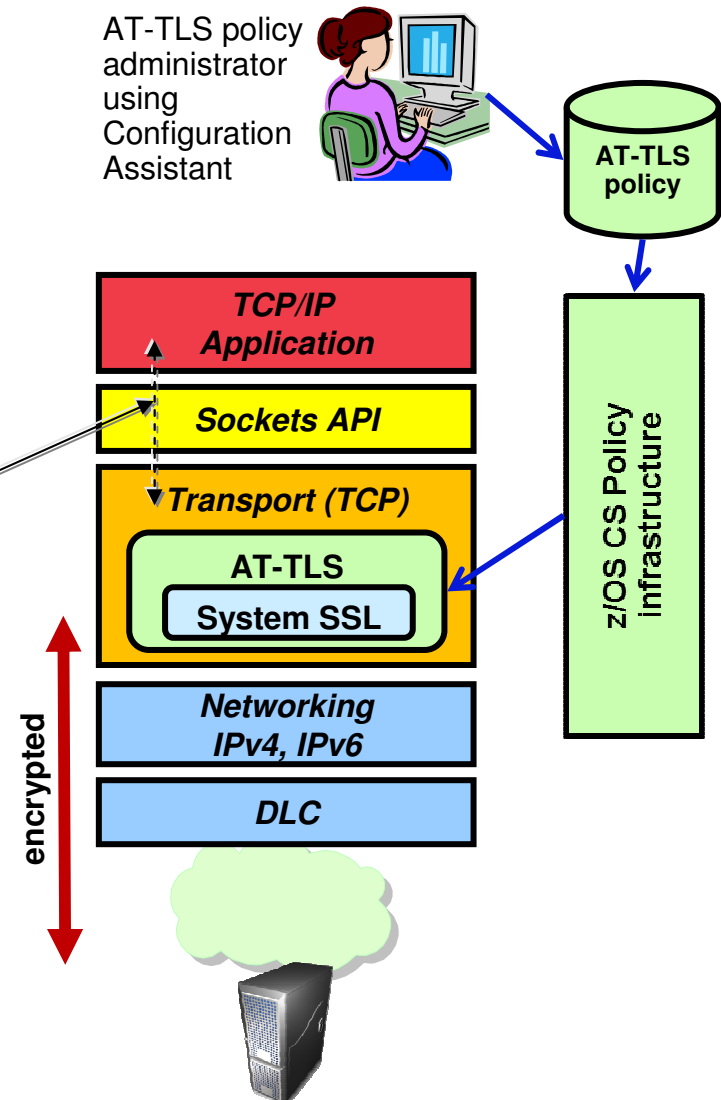
- Includes CICS Sockets
- Supports all programming languages except PASCAL

## Supports standard configurations

- z/OS as a client or as a server
- Server authentication (server identifies self to client)
- Client authentication (both ends identify selves to other)

## Uses System SSL for TLS protocol processing

- Remote endpoint sees an RFC-compliant implementation
- interoperates with other compliant implementations



## Some z/OS applications that use AT-TLS

- CommServer applications
  - TN3270 Server
  - FTP Client and Server
  - CSSMTP
  - Load Balancing Advisor
  - IKE NSS client
  - NSS server
  - Policy agent
- DB2 DRDA
- IMS-Connect
- JES2 NJE
- Tivoli Netview applications
  - MultiSystem Manager
  - NetView Management Console
- RACF Remote Sharing Facility
- CICS Sockets applications
- 3<sup>rd</sup> Party applications
- Customer applications



# Advantages of using AT-TLS



- **Reduce costs**

- Application development
  - Cost of System SSL integration
  - Cost of application's TLS-related configuration support
- Consistent TLS administration across z/OS applications
- Gain access to new features with little or no incremental development cost



- **Complete and up-to-date exploitation of System SSL features**

- AT-TLS makes the vast majority of System SSL features available to applications
- AT-TLS keeps up with System SSL enhancements – as new features are added, your applications can use them by changing AT-TLS policy, not code

- **Ongoing performance improvements**

Focus on efficiency in use of System SSL



- **Great choice if you haven't already invested in System SSL integration**

Even if you have, consider the long-term cost of keeping up vs. short term cost of conversion

## AT-TLS application types



- **Not enabled**

- No policy or policy explicitly disables AT-TLS for application traffic
- Application may optionally use System SSL directly
- Applications that use the Pascal API and Web Fast Response Cache Accelerator (FRCA) fall into this category



- **Basic**

- Policy enables AT-TLS for application traffic
- Application is unchanged and unaware of AT-TLS
- Application protocol unaffected by use of AT-TLS (think HTTP vs. HTTPS)



- **Aware**

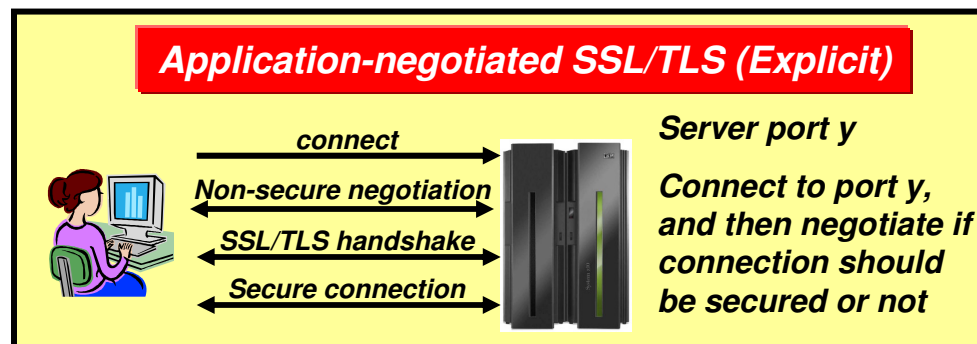
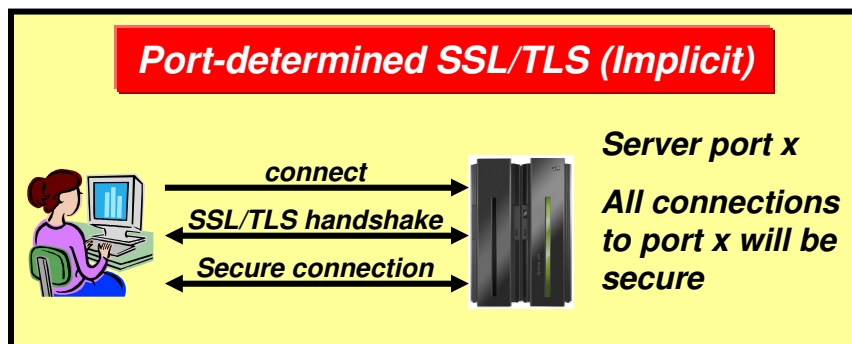
- Policy enables AT-TLS for application traffic
- Application uses the SIOCTTLSCTL ioctl to extract AT-TLS information such as partner certificate, negotiated version and cipher, policy status, etc.



- **Controlling**

- Policy enables AT-TLS and specifies ApplicationControlled ON for application traffic
- Application protocol may negotiate the use of TLS in cleartext with its partner
- Application uses the SIOCTTLSCTL ioctl to extract AT-TLS information (like an aware application) and to control TLS operations:
  - Start secure session
  - Reset session
  - Reset cipher

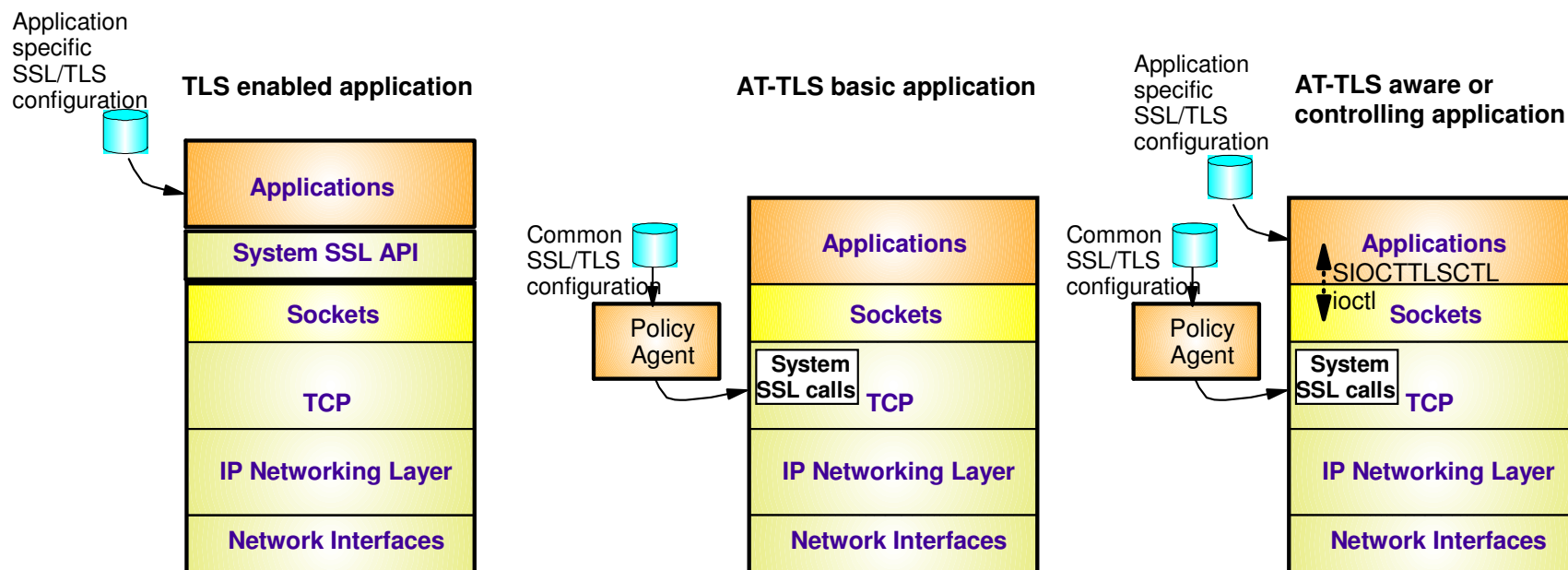
## SSL/TLS application types



- As soon as a connection has been established with the server, the SSL/TLS handshake starts
- Examples are the HTTPS port (443), and FTP's secure port (990)
- AT-TLS considerations:
  - Can be done totally transparent to application code
    - This is referred to as an AT-TLS "Basic" application
  - Optionally the application may query SSL/TLS attributes, such as client user ID (if client authentication is used, cipher suite in use, etc)
    - This is referred to as an AT-TLS "Aware" application

- Application protocol includes verbs to negotiate security protocol and options
- Examples are FTP that uses the AUTH FTP command to negotiate use of SSL/TLS or Kerberos, and in some cases a TN3270 server port (Conntype NegtSecure)
- AT-TLS considerations:
  - Application needs to "tell" AT-TLS when to start the SSL/TLS handshake
    - This is referred to as an AT-TLS "Controlling" application
  - Otherwise, use of AT-TLS is transparent to application
  - Optionally the application may query SSL/TLS attributes, such as client user ID (if client authentication is used, cipher suite in use, etc)

# TLS configuration cases by application type



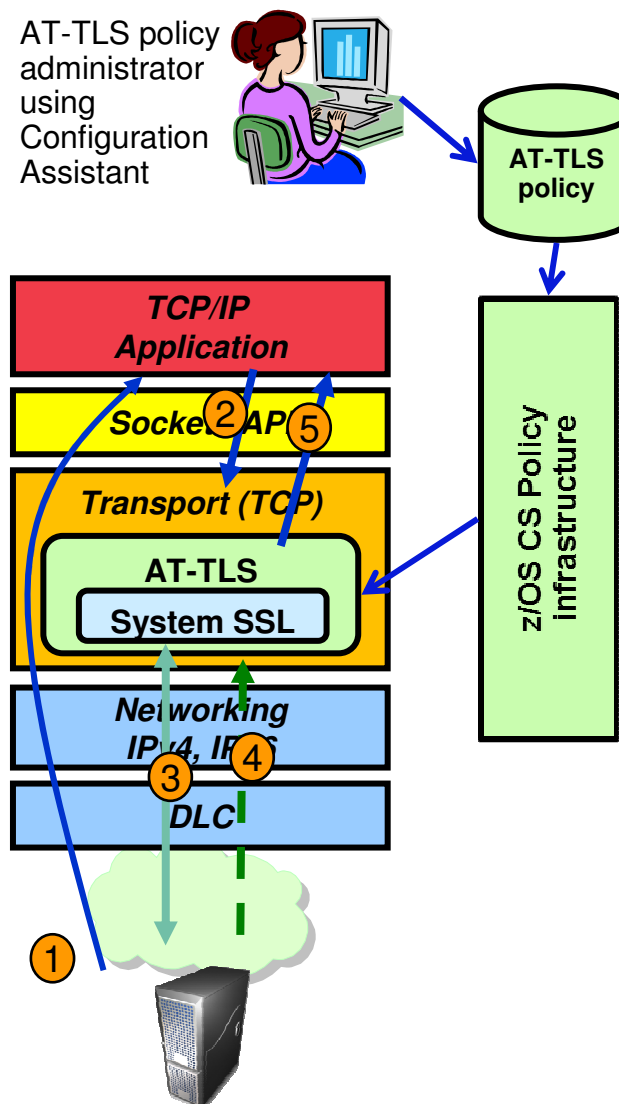
- TLS enabled application
  - Each application has its own configuration to control security policy and TLS functions
- AT-TLS basic application
  - All applications' security policy and TLS functions are governed by a single, consistent AT-TLS policy system-wide
- AT-TLS aware or controlling applications
  - Application specific policy retained but reduced to what application needs for awareness or controlling functions
  - AT-TLS policy continues to control overall AT-TLS function for the application

## AT-TLS basic operation (z/OS as server)

Setup: AT-TLS policy is configured and deployed for the TCP application and the TCP application is started.

1. Client connects to server and connection is established
2. After accepting the new connection, the server issues a read request on the socket. The TCP layer checks AT-TLS policy and sees that AT-TLS protection is configured for this connection. As such, it prepares for the client-initiated TLS handshake
3. The client initiates the SSL handshake and the TCP layer invokes System SSL to perform the TLS handshake under identity of the server.
4. Client sends data traffic under protection of the new TLS session
5. TCP layer invokes System SSL to decrypt the data and then delivers the cleartext inbound data to the server

- Unencrypted (cleartext) flows
- SSL/TLS handshake flows
- SSL/TLS-secured (encrypted) flows

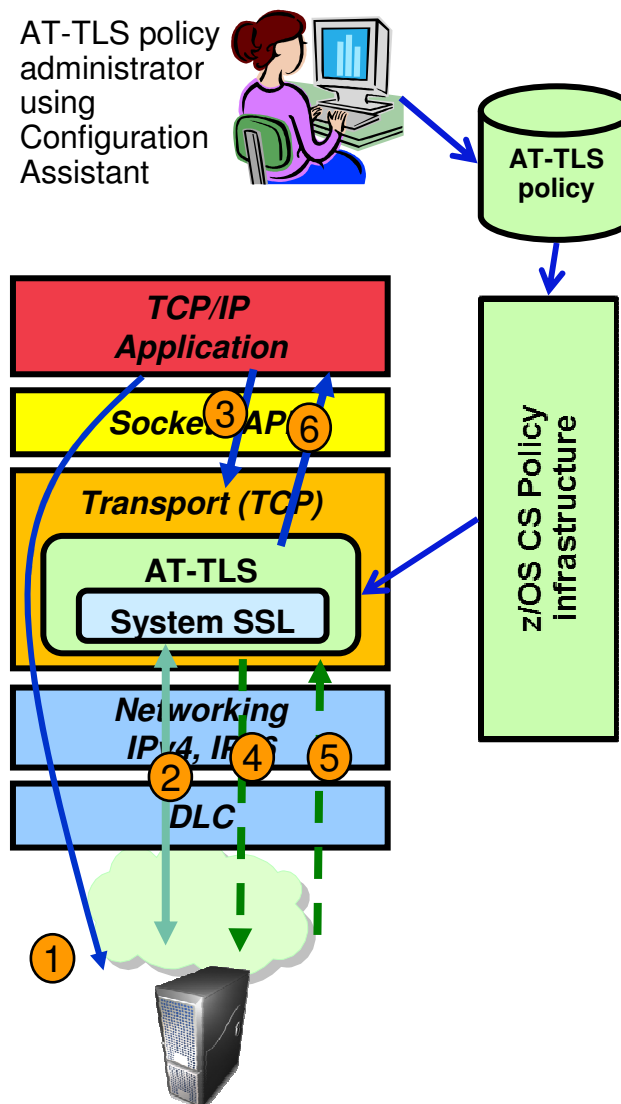


## AT-TLS basic operation (z/OS as client)

Setup: AT-TLS policy is configured and deployed for the TCP application and the TCP application is started.

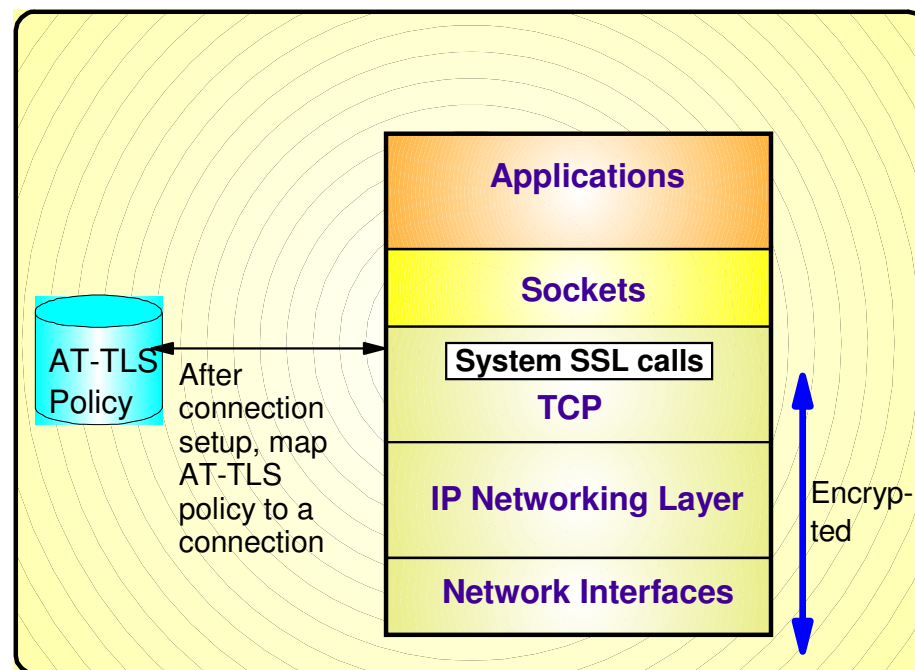
1. z/OS client connects out to server and connection is established
2. TCP layer invokes System SSL to perform the TLS handshake under identity of the client application
3. z/OS client sends data to server
4. TCP layer invokes System SSL to encrypt queued data and then sends it to server
5. Server sends encrypted data, TCP layer invokes System SSL to decrypt it
6. TCP delivers inbound data to z/OS client in the clear

- Unencrypted (cleartext) flows
- SSL/TLS handshake flows
- SSL/TLS-secured (encrypted) flows



## Mapping AT-TLS policy to a TCP connection

- An AT-TLS policy rule describes TLS requirements for a TCP connection
- Policy rule is mapped to a connection based on policy condition
  - TCP/IP resource attributes
  - Connection type attributes
  - Local application attributes
- An AT-TLS policy rule is mapped to a connection at well defined points
  - Outbound Connect
  - First Select/Send/Receive
  - SIOCTTLSCTL ioctl
- If a rule match is found, TCP/IP stack provides TLS protocol control based on the policy action
- Alternate method of mapping policy to a connection
  - Secondary Map
    - Used for applications that have one or more “secondary” connections and one “primary” connection
    - Examples: FTP, rsh, rexec



## AT-TLS policy conditions

Criteria	Description
Local address	Local IP address
Remote address	Remote IP address
Local port	Local port or ports
Remote port	Remote port or ports
Connection direction	<ul style="list-style-type: none"> <li>• Inbound (applied to first Select, Send, or Receive after Accept)</li> <li>• Outbound (applied to Connect)</li> <li>• Both</li> </ul>
User ID	User ID of the owning process or wildcard user ID
Jobname	Jobname of the owning application or wildcard jobname
Time, Day, Week, Month	When filter rule is active



## AT-TLS policy actions

Criteria	Description
TLS enablement	Specifies whether TLS is enabled for connection matching the policy rule
TLS/SSL versions allowed	SSLv2, SSLv3, TLSv1, TLSv1.1
Cipher suites	Set of potential cryptographic algorithms (in order of preference) that this TLS server or client will accept during the TLS handshake
Role	<ul style="list-style-type: none"> <li>• TLS client</li> <li>• TLS server</li> <li>• TLS server with client authentication</li> </ul>
Client authentication type	<ul style="list-style-type: none"> <li>• Passthru (bypass checking)</li> <li>• Required</li> <li>• Full (Accepted if provided by client)</li> <li>• SAFCheck</li> </ul>
Authentication information	<ul style="list-style-type: none"> <li>• Keyring identifier</li> <li>• Certificate label used for authentication</li> <li>• LDAP for certificate revocation list (CRL) processing</li> </ul>
Data trace	Specifies whether to trace cleartext in datatrace or ctrace
AT-TLS trace levels	Specifies level of tracing
Handshake timeout	Time to wait for handshake to complete
Session key lifetime	When session key has been used this specified time period, a new session key must be created
Session ID requirements	Session ID cache size, Session ID timeout, Use sysplex-wide session ID cache
Secondary map used	Specifies whether a matching connection should be used as a "primary" connection in the "secondary policy mapping method"

## Recent AT-TLS enhancements



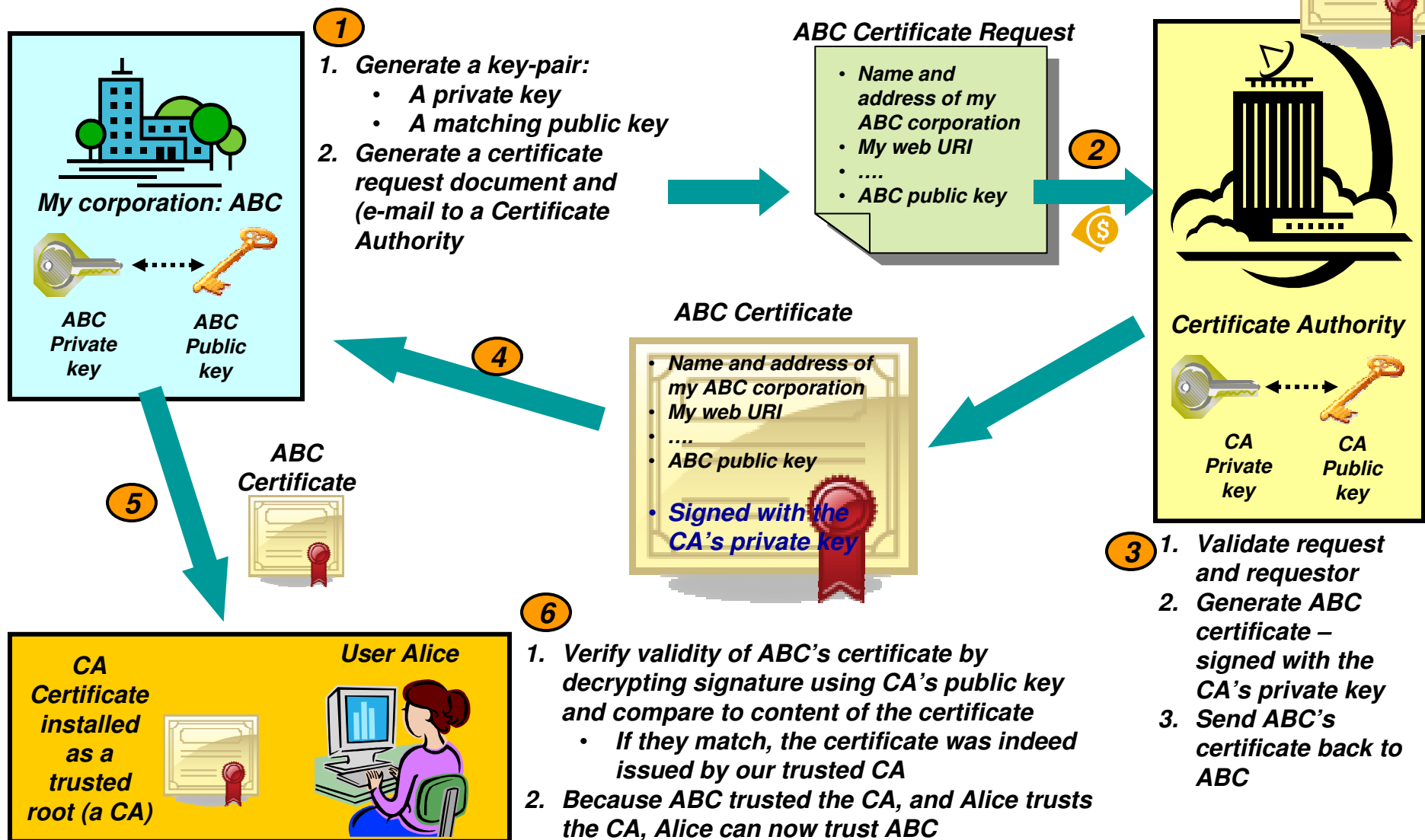
AT-TLS keeps up with System SSL enhancements – as new features are added, your applications can use them by changing AT-TLS policy, not code. Here is a list of capabilities added recently.

- TLS V1.1
- TLS Extensions (RFC 4366)
  - Negotiation and use of a truncated HMAC
  - Negotiation and use of a maximum SSL fragment size
  - Negotiation and use of handshake server name indication
- CRL LDAP server access security level
  - Option added to select security level setting for using LDAP servers with Certificate Revocation Lists (CRL)
- Certificate validation using RFC 3280
  - AT-TLS provides an option to select certificate validation method between using RFC 2459, RFC 3280, or any certificate validation method
- Accessing certificates stored in ICSF with PKCS #11 tokens
  - Accept PKCS #11 tokens in TTLSKeyRingParms statement
- FIPS 140-2
  - In z/OS V1R11, AT-TLS can be configured to invoke System SSL in the FIPS 140-2 compliant mode.
    - FIPS 140-2 can be selectively enabled in the AT-TLS policy configuration

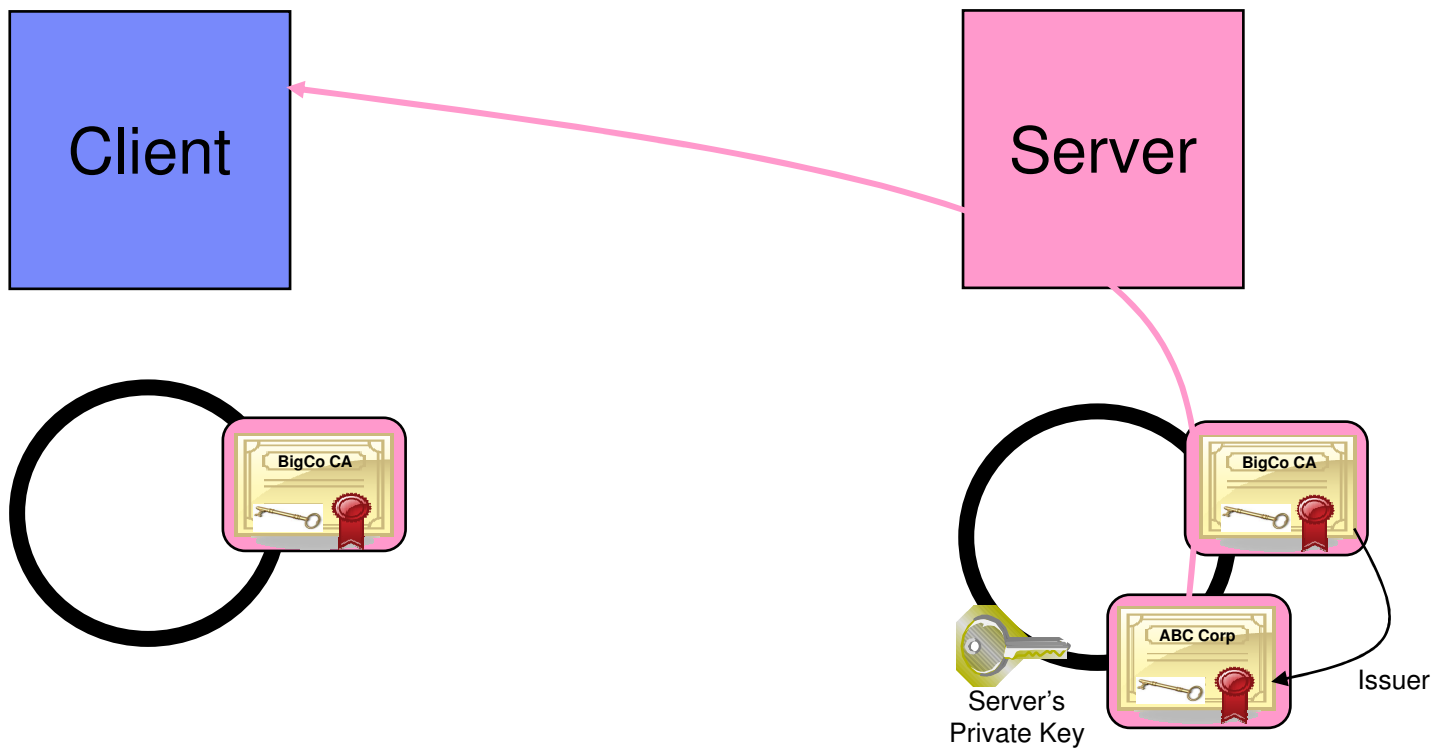
## AT-TLS configuration task steps

- Obtain x.509 certificates and update RACF keyrings
- Update any application-specific configuration files if necessary
- Enabling use of AT-TLS in the TCP/IP stack configuration
- Create AT-TLS policy using Configuration Assistant for z/OS Communications Server
- Create policy infrastructure using Configuration Assistant application setup task checklist

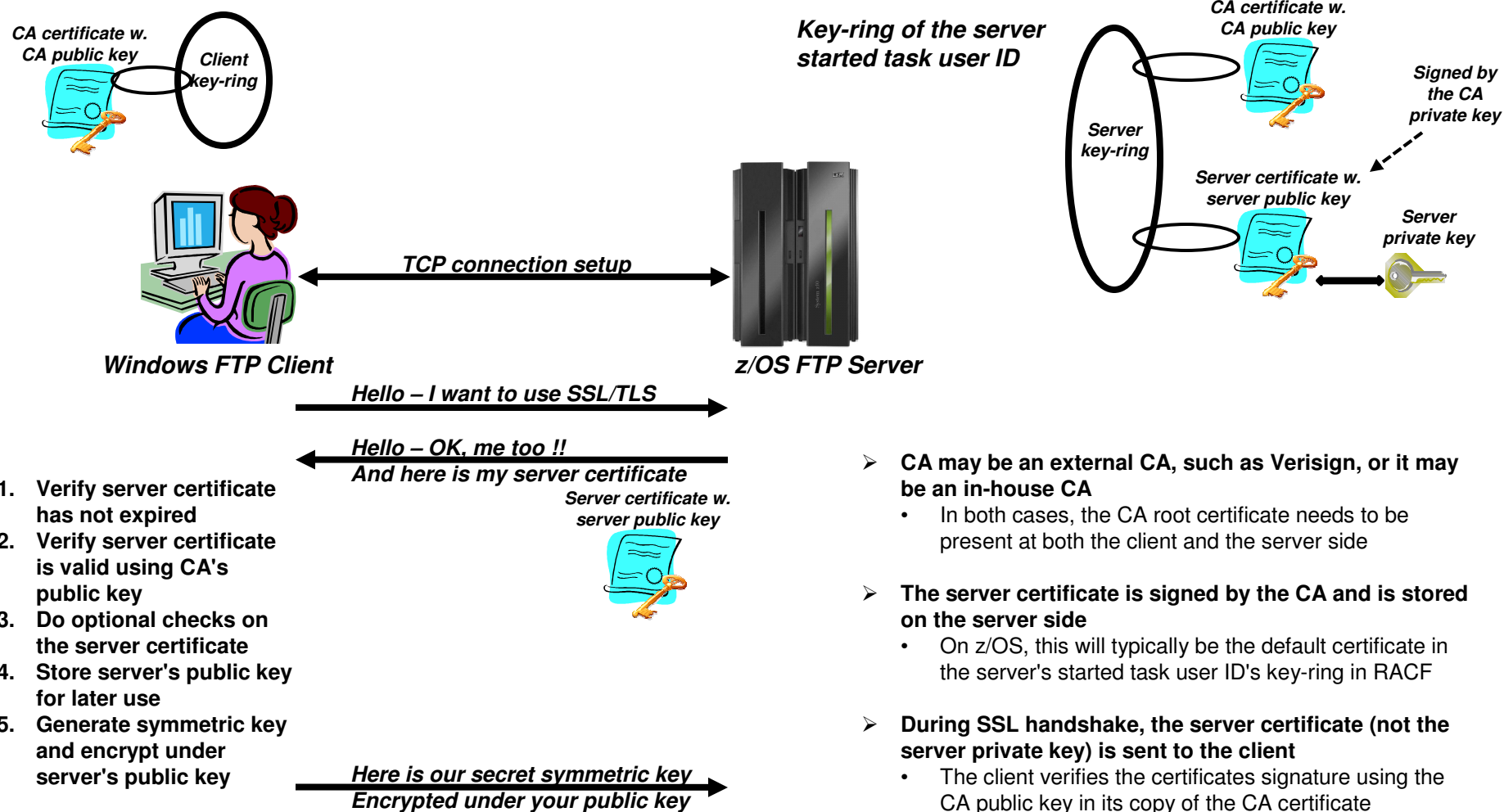
# Trust relationships and Certificate Authorities (or, where do certificates come from?)



# Certificates in action: SSL server authentication



# What is needed for z/OS Server authentication only (which is sufficient for encrypted data exchange)



1. Verify server certificate has not expired
2. Verify server certificate is valid using CA's public key
3. Do optional checks on the server certificate
4. Store server's public key for later use
5. Generate symmetric key and encrypt under server's public key

- CA may be an external CA, such as Verisign, or it may be an in-house CA
  - In both cases, the CA root certificate needs to be present at both the client and the server side
- The server certificate is signed by the CA and is stored on the server side
  - On z/OS, this will typically be the default certificate in the server's started task user ID's key-ring in RACF
- During SSL handshake, the server certificate (not the server private key) is sent to the client
  - The client verifies the certificates signature using the CA public key in its copy of the CA certificate

## Create self-signed root certificate for test purposes

```

RACDCERT CERTAUTH GENCERT +
  SUBJECTSDN( +
    CN('MVS098 Certificate Authority') +
    OU('Z/OS CS V1R9', 'ENS', 'AIM', 'SWG') +
    O('IBM') +
    L('Raleigh') +
    SP('NC') +
    C('US') ) +
  SIZE(1024) +
  NOTBEFORE(DATE(2010-02-01)) +
  NOTAFTER(DATE(2020-12-31)) + ←
  WITHLABEL('ABCTLS CA') +
  KEYUSAGE(CERTSIGN) +
  ALTNAME( +
    DOMAIN('mvs098.tcp.raleigh.ibm.com') )

```

*Create a self-signed root certificate and a private/public key-pair:*

- **CERTAUTH**
- **KEYUSAGE(CERTSIGN)**
- **Absence of a SIGNWITH option**

*It can become a nightmare when these things expire, so don't create certificates with too short a time span! (Your security czar will likely have an opinion on that)*

- In a production environment, you would not need a self-signed root certificate. To sign server and personal certificates, you would use your company root certificate or an external Certificate Authority.
- For testing, a self-signed root certificate is useful. It allows you to familiarize yourself with keys and certificates and allows you to thoroughly test your secure FTP setup on z/OS before deploying it in production.

## Create server certificate signed with your own root certificate



```
RACDCERT ID(TCPCS) GENCERT +
  SUBJECTSDN( +
    CN('MVS098 Server Certificate') +
    OU('Z/OS CS V1R11', 'ENS', 'AIM', 'SWG') +
    O('IBM') +
    L('Raleigh') +
    SP('NC') +
    C('US') ) +
  SIZE(1024) +
  NOTBEFORE(DATE(2010-02-01)) +
  NOTAFTER(DATE(2020-12-31)) +
  WITHLABEL('ABCTLS TCPSERV') +
  KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN) +
  ALTNAME( +
    DOMAIN('mvs098.tcp.raleigh.ibm.com') ) +
  SIGNWITH(CERTAUTH LABEL('ABCTLS CA'))
```

*Create a server certificate signed with your own root certificate and a private/public key pair:*

- *ID(userID) – the started task user ID of your server*
- *KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)*
- *SIGNWITH(CERTAUTH LABEL('your rot certificate'))*

- In a production environment, you would use an alternative procedure after having generated the server key pair and certificate:
  - You would generate a certificate signing request and send it to your CA
  - Your CA would process your request and create a certificate signed with the CA private key
  - You would import the signed certificate into RACF



# Alternative: use an external CA to sign your server certificate



```
RACDCERT ID(TCPCS) GENCERT +  
  SUBJECTSDN( +  
    CN('MVS098 Server Certificate') +  
    OU('Z/OS CS V1R11', 'ENS', 'AIM', 'SWG') +  
    O('IBM') +  
    L('Raleigh') +  
    SP('NC') +  
    C('US') ) +  
  SIZE(1024) +  
  NOTBEFORE(DATE(2010-02-01)) +  
  NOTAFTER(DATE(2020-12-31)) +  
  WITHLABEL('ABCTLS TCPSERV') +  
  KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN) +  
  ALTNAME( +  
    DOMAIN('mvs098.tcp.raleigh.ibm.com') )  
RACDCERT ID(TCPCS) GENREQ (LABEL('ABCTLS TCPSERV')) +  
  DSN('USER1.PKITEST.SERVERS.REQ')
```

← Create a server certificate and a private/public key pair:

- ID(userID) – the started task user ID of your server
- KEYUSAGE(HANDSHAKE DATAENCRYPT DOCSIGN)

Generate a request to have the certificate signed by an external CA

- Send the request to the CA
- Receive the response from the CA

← Add the signed certificate into RACF

```
(**** delay here while CA processes your request ****)  
  
RACDCERT ID(TCPCS) +  
  ADD('USER1.PKITEST.SERVERS.CRT') +  
  TRUST +  
  WITHLABEL('ABCTLS TCPSERV')
```

If not already there, you also need to add the CA's root certificate to RACF as a CERTAUTH certificate

# Create you z/OS server started task user ID key-ring and connect required certificates to it

```

RACDCERT CERTAUTH +
  EXPORT (LABEL ('ABCTLS CA')) +
  DSN ('USER1.ABCTLSCA.B64') +
  FORMAT (CERTB64)

RACDCERT ID (TCPCS) ADDRING (TLSRING)
RACDCERT ID (TCPCS) +
  CONNECT (CERTAUTH LABEL ('ABCTLS CA') +
  RING (TLSRING) )

RACDCERT ID (TCPCS) +
  CONNECT (LABEL ('ABCTLS TCPSEV') +
  RING (TLSRING) +
  DEFAULT)

RACDCERT ID (TCPCS) +
  LISTRING (TLSRING)
  
```

*In order for the remote client to successfully authenticate server certificates that are signed with our self-signed root certificate, they need a copy of that root certificate in their local key-rings. Download as a text file to your client workstation*

*Create key-ring for your started task server user ID*

*Connect certificates to the key-ring:*

- Your root certificate
- Your server certificate

Digital ring information for user TCPCS:

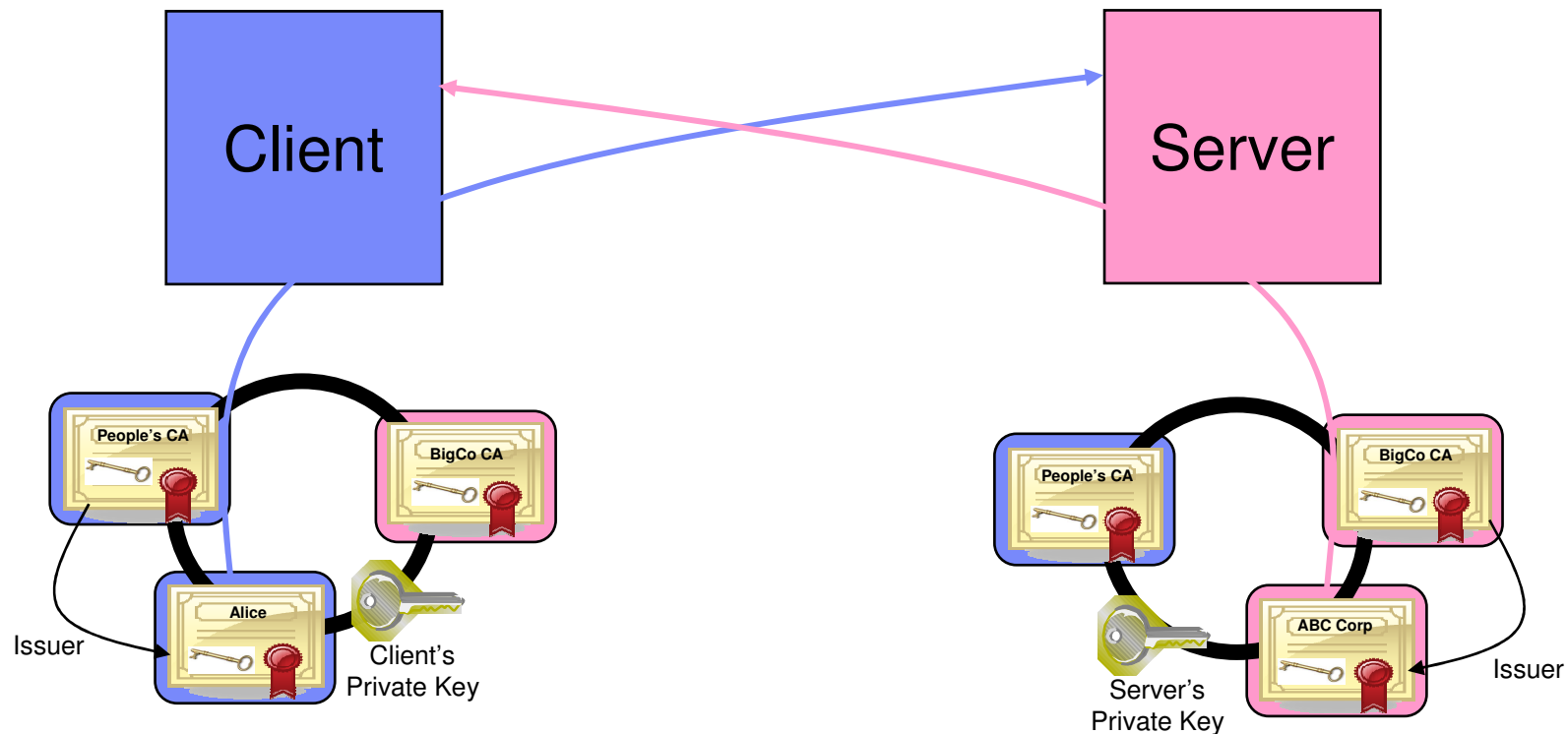
Ring:

>TLSRING<

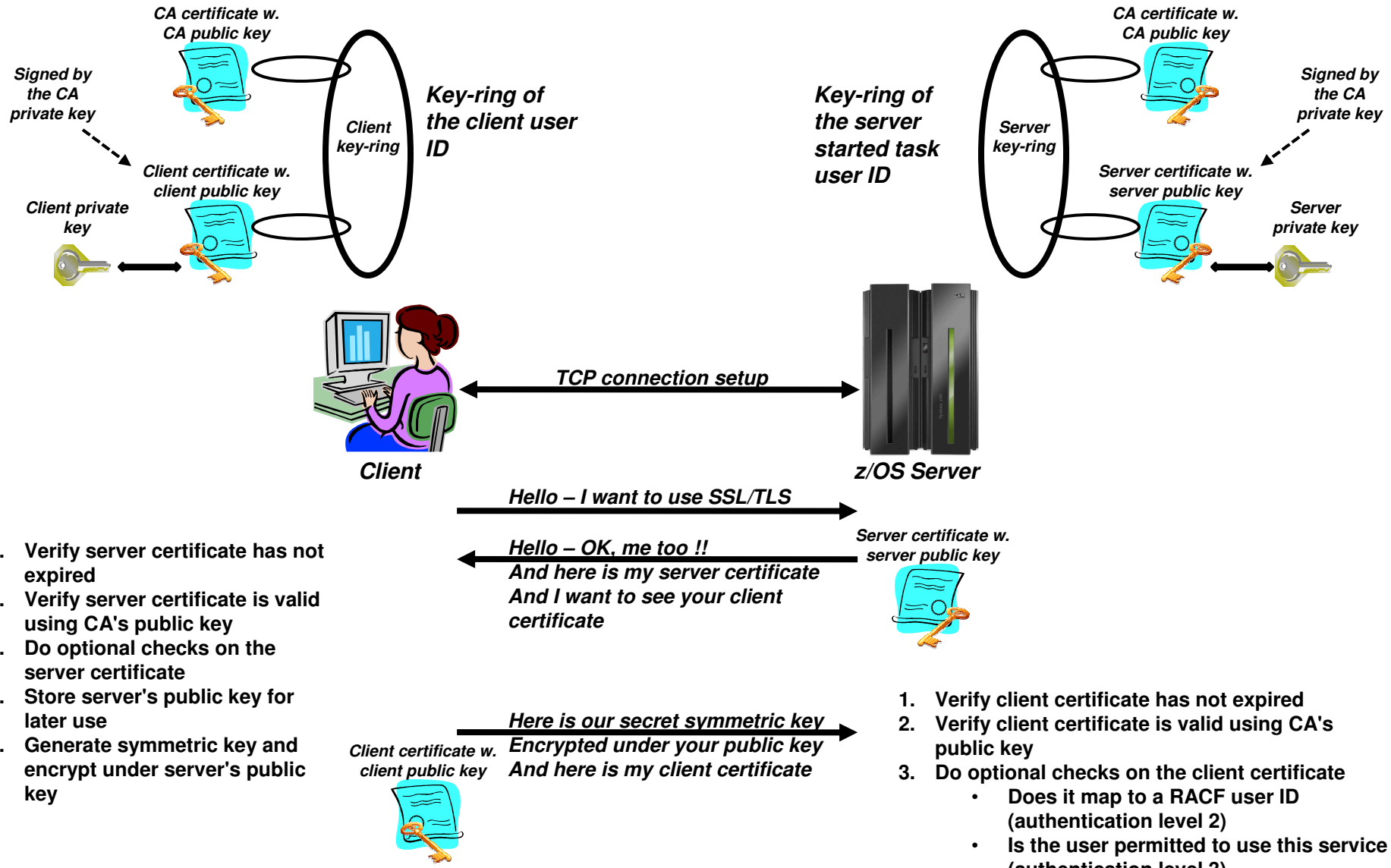
Certificate Label Name	Cert Owner	USAGE	DEFAULT
ABCTLS CA	CERTAUTH	CERTAUTH	NO
ABCTLS TCPSEV	ID (TCPCS)	PERSONAL	YES

# Certificates in action: SSL client authentication

(implies server authentication as well)



# What is needed for z/OS Server and client authentication?



1. Verify server certificate has not expired
2. Verify server certificate is valid using CA's public key
3. Do optional checks on the server certificate
4. Store server's public key for later use
5. Generate symmetric key and encrypt under server's public key

1. Verify client certificate has not expired
2. Verify client certificate is valid using CA's public key
3. Do optional checks on the client certificate
  - Does it map to a RACF user ID (authentication level 2)
  - Is the user permitted to use this service (authentication level 3)

# Enabling use of AT-TLS in the TCP/IP stack



- AT-TLS is enabled via a TCPCONFIG parameter

```
TCPConfig TTLS ; Enable AT-TLS policies
```

- There may be a short time period between TCP/IP parsing this configuration option and the actual AT-TLS policies being installed into the stack by Policy Agent
  - Since the stack doesn't yet have an AT-TLS policy, it doesn't know which connections to secure
  - What should it do if a new connection is being set up during this short time window?
  - You control that via a SERVAUTH profile:
    - **EZB.INITSTACK.system.stackname**
- When TCP/IP starts with TCPCONFIG TTLS specified, it will issue message EZZ4248E

```
EZZ4248E TCPCS WAITING FOR PAGENT TTLS POLICY  
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPCS : TTLS  
EZZ4250I AT-TLS SERVICES ARE AVAILABLE FOR TCPCS
```

- Between messages EZZ4248E and EZZ4250I, the TCP/IP stack will only allow users permitted to the EZB.INITSTACK.system.stack SERVAUTH profile to establish TCP connections.
  - **Note:** make sure all your pertinent server address spaces (including PAGENT and OMROUTE) run under user IDs that are permitted to this profile.

## Update any application configuration if needed - FTP example



- Some application configuration changes may be necessary if the application is either AT-TLS aware or AT-TLS controlling
- The FTP server is both AT-TLS aware and controlling
- Example below defines an FTP server that supports SSL/TLS connections, but does not require it
  - It depends on the client sending an AUTH command or not
- SSL/TLS is done by ATTLS in this example

```
EXTENSIONS          AUTH_TLS          ; Enable TLS authentication
TLSMECHANISM        ATTLS          ; Server-specific or ATTLS
SECURE_FTP          ALLOWED        ; Security required/optional
SECURE_LOGIN        NO_CLIENT_AUTH ; Client authentication
SECURE_PASSWORD     REQUIRED        ; Password requirement
SECURE_CTRLCONN     PRIVATE       ; Minimum level of security CTRL
SECURE_DATACONN     PRIVATE       ; Minimum level of security DATA
TLSRFCLEVEL        RFC4217        ; SSL/TLS RFC Level supported
```

# Policy-based network security on z/OS: Configuration Assistant



Download the Windows version at <http://tinyurl.com/cgoqsa>

- **Configures:**
  - AT-TLS
  - IPSec and IP filtering
  - IDS
  - Quality of Service
  - Policy-based routing
- **Separate perspectives but consistent model for each discipline**
- **Focus on concepts, not details**
  - what traffic to protect
  - how to protect it
  - De-emphasize low-level details (though they are accessible through advanced panels)
- **z/OSMF-based web interface (strategic) or standalone Windows application**
- **Builds and maintains**
  - Policy files
  - Related configuration files
  - JCL procs and RACF directives
- **Supports import of existing policy files**

## Configuration Assistant policy creation approach

- Wizards and dialogs guide you through a top-down approach to configuration

- ▶ Navigational tree supports a bottom-up approach

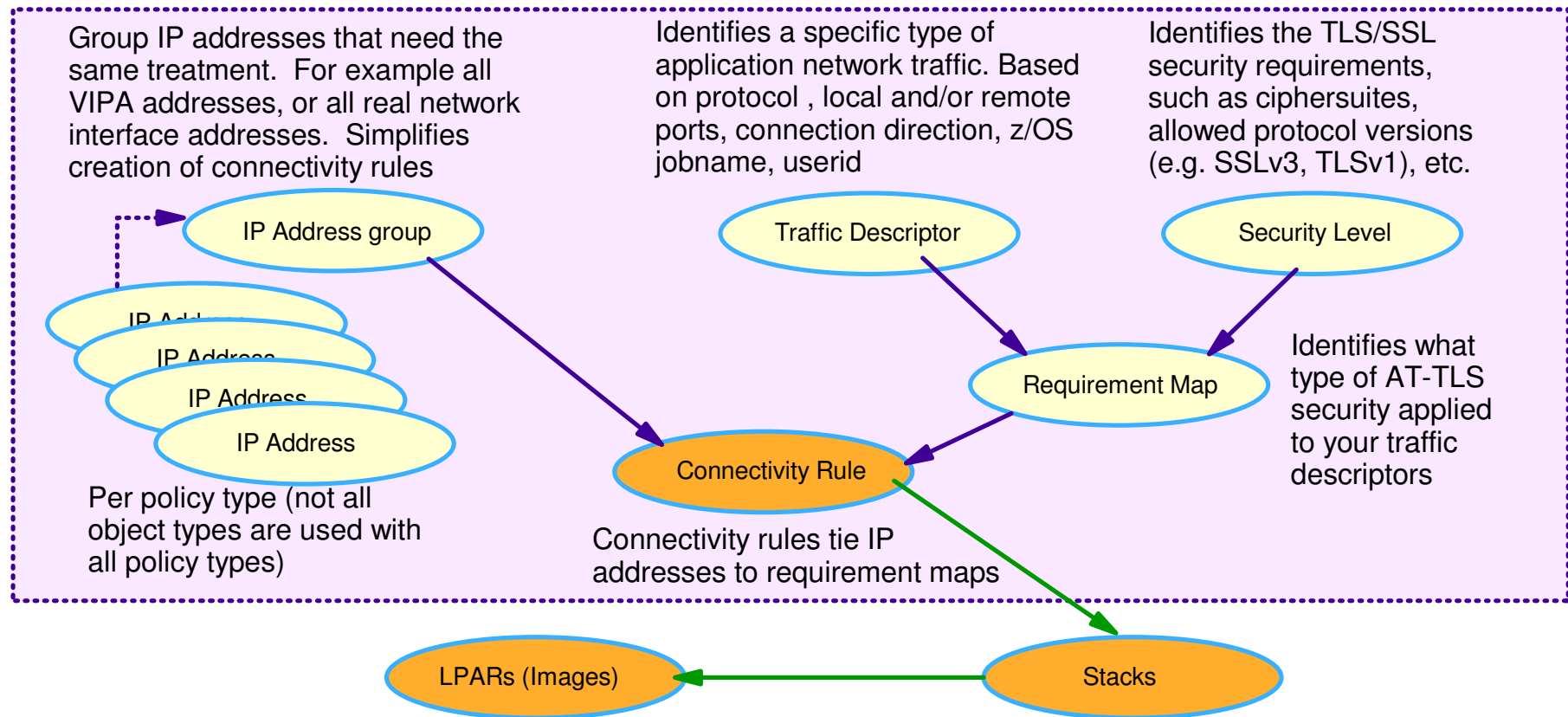
- Allows an experienced user to bypass wizard screens

- Define system images and TCP/IP stacks
- Define security levels (reusable)
  - Protection suites (e.g. gold, silver, bronze)
- Define requirements map (reusable)
  - How to protect common scenarios (e.g. intranet, branch office, business partner)
  - Set of traffic descriptors linked to security level
- Define connectivity rules
  - A complete security policy for all traffic between two endpoints
  - Specified data endpoints linked to a requirements map

*Optimizations to this approach are provided for common applications!*



# Configuration Assistant reusable object model



1. Create system image and TCP/IP stack image
2. Create one or more Requirement Maps to define desired security for common scenarios (e.g. intranet, branch office, business partner)
  - Create or reuse Security Levels to define security actions
  - Create or reuse Traffic descriptors to define application ports to secure
3. Create one or more Connectivity Rules between Data Endpoints (IP addresses) and associate with a configured Requirement Map

## AT-TLS rule simplification with “pre-defined rules”

- In z/OS V1R11, configuration of AT-TLS policy definition was simplified so that policy rules for common applications can be configured in a few clicks
- The Configuration Assistant provides predefined AT-TLS connectivity rules for common applications configured for each stack .
- In most cases, these rules need no modification and can be enabled for immediate use.
- Each rule defines an application with default port settings, key ring, and is associated with a default security level.
- The administrator can easily enable the rules they want to have in their policy and install the generated flat file.

*The examples that follow use the pre-defined rule approach....*

# Add a z/OS image



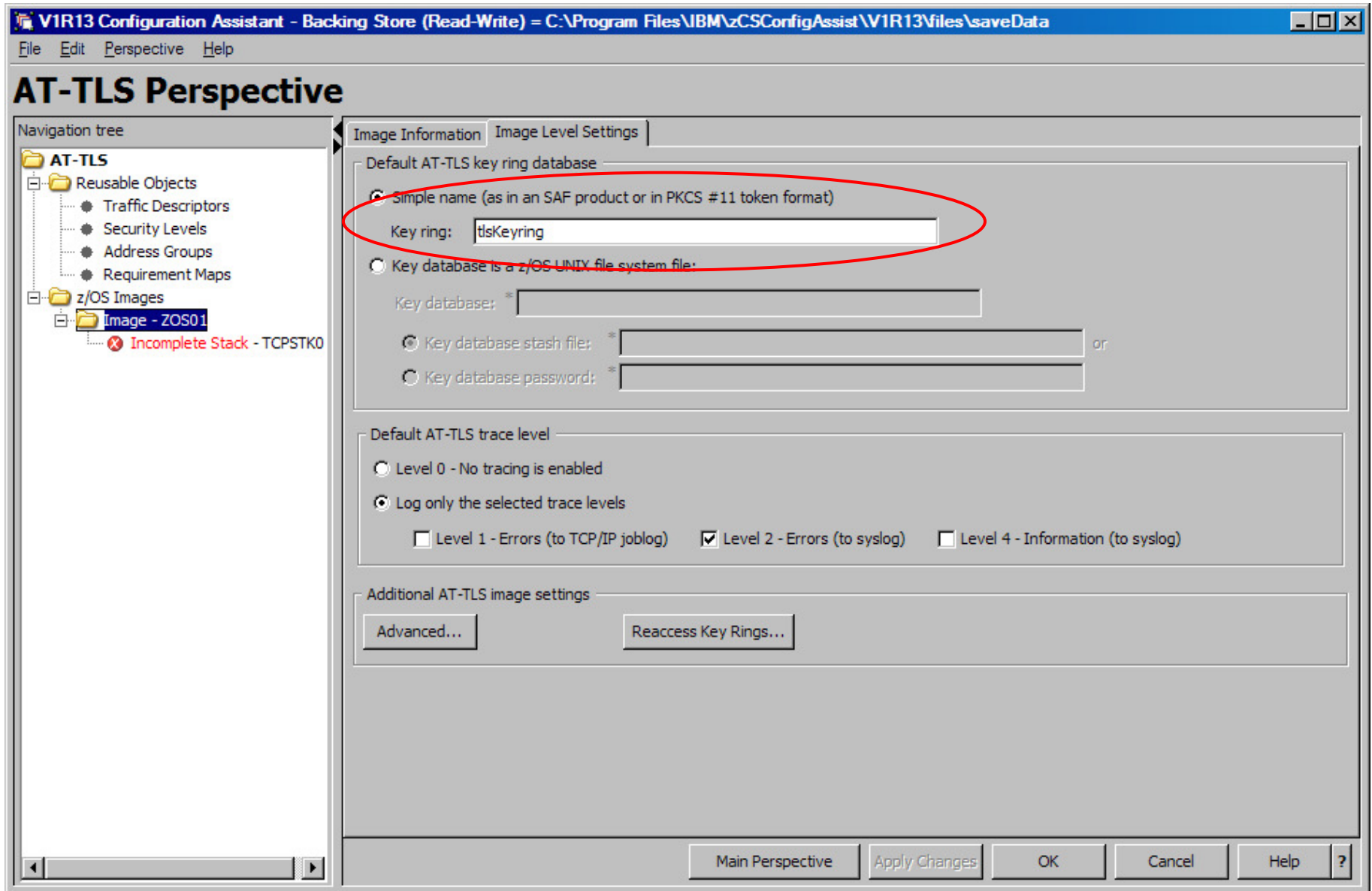
The screenshot shows the V1R13 Configuration Assistant interface. The title bar reads "V1R13 Configuration Assistant - Backing Store (Read-Write) = C:\Program Files\IBM\zCConfigAssist\V1R13\files\saveData". The main window is titled "AT-TLS Perspective". On the left, a "Navigation tree" shows a folder "AT-TLS" containing "Reusable Objects" (Traffic Descriptors, Security Levels, Address Groups, Requirement Maps) and "z/OS Images". In the center, a "Work with reusable objects" section has buttons for "Traffic Descriptors", "Security Levels", "Address Groups", and "Requirement Maps". Below this is a section "Work with settings for z/OS image" with a button "Add a New z/OS Image..." circled in red. A dashed arrow points from this button to a "New z/OS Image" dialog box. The dialog box has the following fields: "z/OS image name:" with value "ZOS01", "Description:" with value "Z/OS System 1", and "z/OS release:" with a dropdown menu set to "V1R13". Under "Default AT-TLS key ring database", the "Simple name (as in an SAF product or in PKCS #11 Token format)" option is selected, with "Key ring:" set to "tlsKeyring". Other options include "Key database is a z/OS UNIX file system file:", "Key database stash file:", and "Key database password:". "OK" and "Cancel" buttons are at the bottom right of the dialog. At the bottom of the main window, there are "Main Perspective" and "Help" buttons.

# Add a TCP/IP stack



The screenshot displays the V1R13 Configuration Assistant interface. The main window is titled "AT-TLS Perspective" and shows a navigation tree on the left with "Image - ZOS01" selected. The main area is divided into "Image Information" and "Image Level Settings" tabs. The "Image Information" tab contains fields for "z/OS image name:" (ZOS01), "Description:" (Z/OS System 1), and "z/OS release:" (V1R13). A red circle highlights the "Add New TCP/IP Stack..." button. A dashed arrow points from this button to a smaller dialog box titled "New TCP/IP Stack: Information". This dialog box has fields for "TCP/IP stack name:" (TCPSTK01) and "Description:" (TCP/IP Stack 1), with "OK", "Cancel", and "Help" buttons at the bottom. The main window also features buttons for "Application Setup Tasks...", "Install Configuration Files...", "Main Perspective", "Apply Changes", "OK", "Cancel", and "Help".

# Set default key ring at the image level



# Predefined connectivity rules are now configured for each stack



V1R13 Configuration Assistant - Backing Store (Read-Write) = C:\Program Files\IBM\zCSConfigAssist\V1R13\files\saveData

File Edit Perspective Help

## AT-TLS Perspective

Navigation tree

- AT-TLS
  - Reusable Objects
    - Traffic Descriptors
    - Security Levels
    - Address Groups
    - Requirement Maps
  - z/OS Images
    - Image - ZOS01
      - Incomplete Stack - TCPSTK0

TCP/IP stack name: \* TCPSTK01

Description: TCP/IP Stack 1

z/OS release: V1R13

Enable the rule you would like to have in your AT-TLS policy.  
To enable a rule, right click on the row and select Enable Rule.

Status	Rule Name	Application / Requirement Map	Key Ring
Disabled	Default_DB2-Requester	DB2-Requester	tsKeyring
Disabled	Default_DB2-Server	DB2-Server	tsKeyring
Disabled	Default_Central_PolicySvr	Centralized_Policy_Server	tsKeyring
Disabled	Default_CICS	CICS	tsKeyring
Disabled	Default_CSSMTP	CSSMTP	tsKeyring
Disabled	Default_FTP-Client	FTP-Client	tsKeyring
Disabled	Default_FTP-Server	FTP-Server	tsKeyring
Disabled	Default_IMS-Connect	IMS-Connect	tsKeyring
Disabled	Default_JES-Client	JES-Client	tsKeyring
Disabled	Default_JES-Server	JES-Server	tsKeyring
Disabled	Default_LBA-Advisor	LBA-Advisor	tsKeyring
Disabled	Default_MSM	MSM	tsKeyring
Disabled	Default_NETCONV	NETCONV	tsKeyring
Disabled	Default_NSS_Client-IKED	NSS_Client-IKED	tsKeyring
Disabled	Default_NSS_Server	NSS_Server	tsKeyring

Modify... Copy... Add... Delete Move Up View Details Health Check

Move Down

Main Perspective Apply Changes OK Cancel Help ?



# Preparing the TN3270 pre-defined connectivity rule



V1R13 Configuration Assistant - Backing Store (Read-Write) = C:\Program Files\IBM\zCSConfigAssist\V1R13\files\saveData

File Edit Perspective Help

## AT-TLS Perspective

Navigation tree

- AT-TLS
  - Reusable Objects
    - Traffic Descriptors
    - Security Levels
    - Address Groups
    - Requirement Maps
  - z/OS Images
    - Image - ZOS01
      - Incomplete Stack - TCPSTK0

TCP/IP stack name: \* TCPSTK01

Description: TCP/IP Stack 1

z/OS release: V1R.13

Enable the rule you would like to have in your AT-TLS policy.  
To enable a rule, right click on the row and select Enable Rule.

Status	Rule Name	Application / Requirement Map	Key Ring
Disabled	Default_CSSMTP	CSSMTP	tlsKeyring
Disabled	Default_FTP-Client	FTP-Client	tlsKeyring
Disabled	Default_FTP-Server	FTP-Server	tlsKeyring
Disabled	Default_IMS-Connect	IMS-Connect	tlsKeyring
Disabled	Default_JES-Client	JES-Client	tlsKeyring
Disabled	Default_JES-Server	JES-Server	tlsKeyring
Disabled	Default_LBA-Advisor	LBA-Advisor	tlsKeyring
Disabled	Default_MSM	MSM	tlsKeyring
Disabled	Default_NETCONV	NETCONV	tlsKeyring
Disabled	Default_NSS_Client-IKED	NSS_Client-IKED	tlsKeyring
Disabled	Default_NSS_Server	NSS_Server	tlsKeyring
Disabled	Default_PolicyAgentImport	PolicyAgentImport	tlsKeyring
Disabled	Default_RRSF-Client	RRSF-Client	tlsKeyring
Disabled	Default_RRSF-Server	RRSF-Server	tlsKeyring
Disabled	Default_TN3270-Server	TN3270-Server	tlsKeyring

Modify... Copy.. Add... Delete Move Up View Details Health Check

Move Down

See next page

Main Perspective Apply Changes OK Cancel Help ?

# Describe traffic



**Modify Rule**

AT-TLS rule name

Rule name: \*   Enable rule Restore Defaults

Specify settings

Traffic | Role | Key Ring | Data Endpoints | Security Level | Advanced

Use this panel to specify the traffic settings.

Application name: \*

Local port

All ports  
 All ephemeral ports  
 Ports: \*   
Separate multiple ports with a comma

Remote port

All ports  
 All ephemeral ports  
 Ports: \*   
Separate multiple ports with a comma

Indicate the TCP connect direction

Either  Inbound only  Outbound only

Specify jobname and user ID

Jobname:  User ID:

OK Cancel Help ?



## Describe role – Not changeable

**Modify Rule**

AT-TLS rule name

Rule name: \*Default\_TN3270-Server  Enable rule Restore Defaults

Specify settings

Traffic **Role** Key Ring Data Endpoints Security Level Advanced

The following fields are disabled for this application. The policy rule will fail if the settings were changed.  
Use this panel to specify the AT-TLS roles.

AT-TLS handshake role

Server  Client

Application controlled

On  Off

Secondary map

On  Off

OK Cancel Help ?

# Define key ring – in this case use the z/OS image level key ring

**Modify Rule**

AT-TLS rule name

Rule name: \*   Enable rule Restore Defaults

Specify settings

Traffic | **Role** | **Key Ring** | Data Endpoints | Security Level | Advanced

Use this panel to specify the key ring database and certificate label to use for this rule.

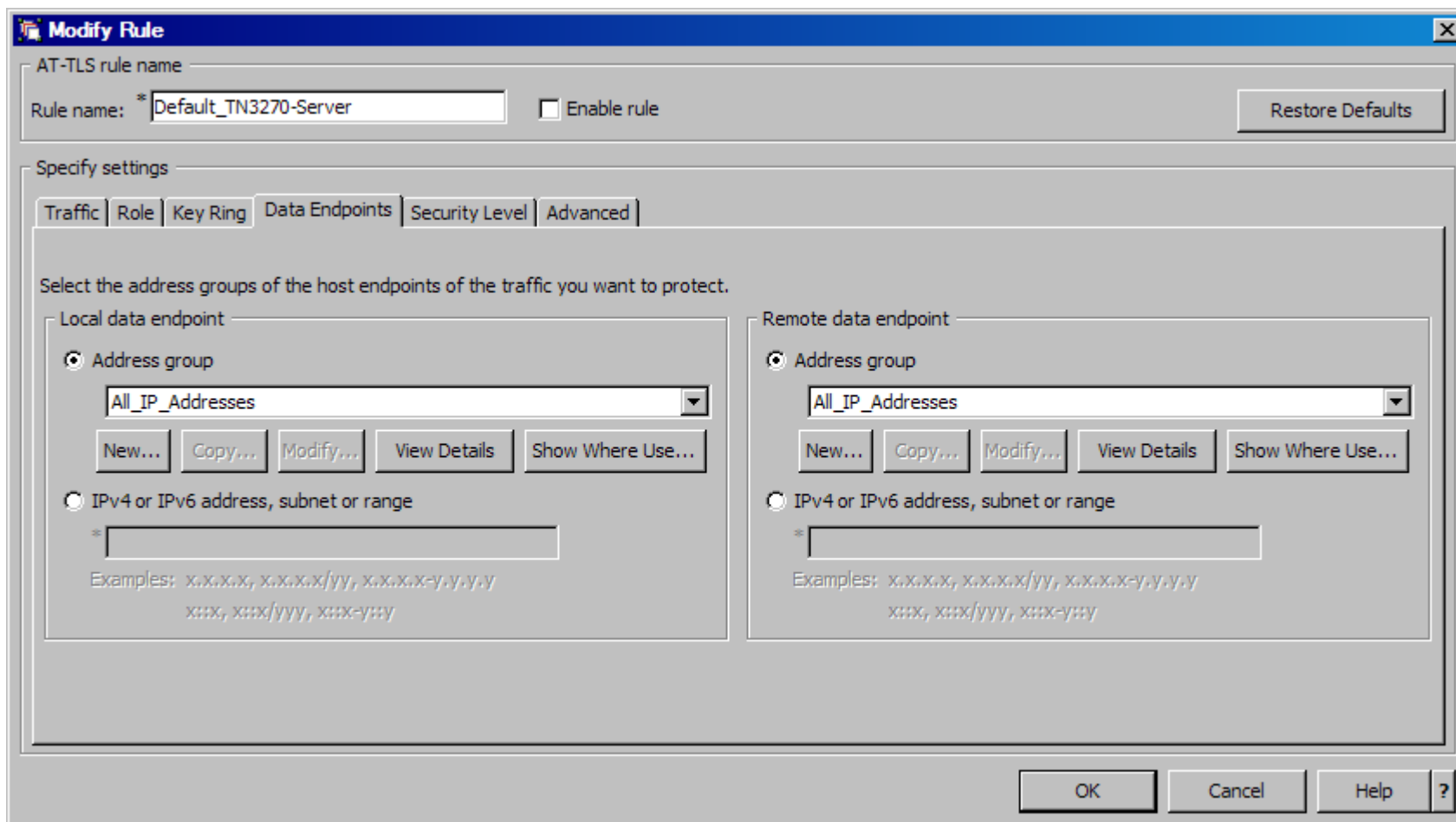
Key ring database

- Use the key ring database defined for the z/OS image
- Use a Simple name (as in an SAF product or in PKCS #11 Token format):
  - Key ring: \*
- Use this z/OS UNIX file system key database:
  - Key database: \*
  - Key database stash file: \*  or
  - Key database password: \*

Certificate label:

OK Cancel Help ?

# Describe data endpoints – in this case apply rule to all endpoints

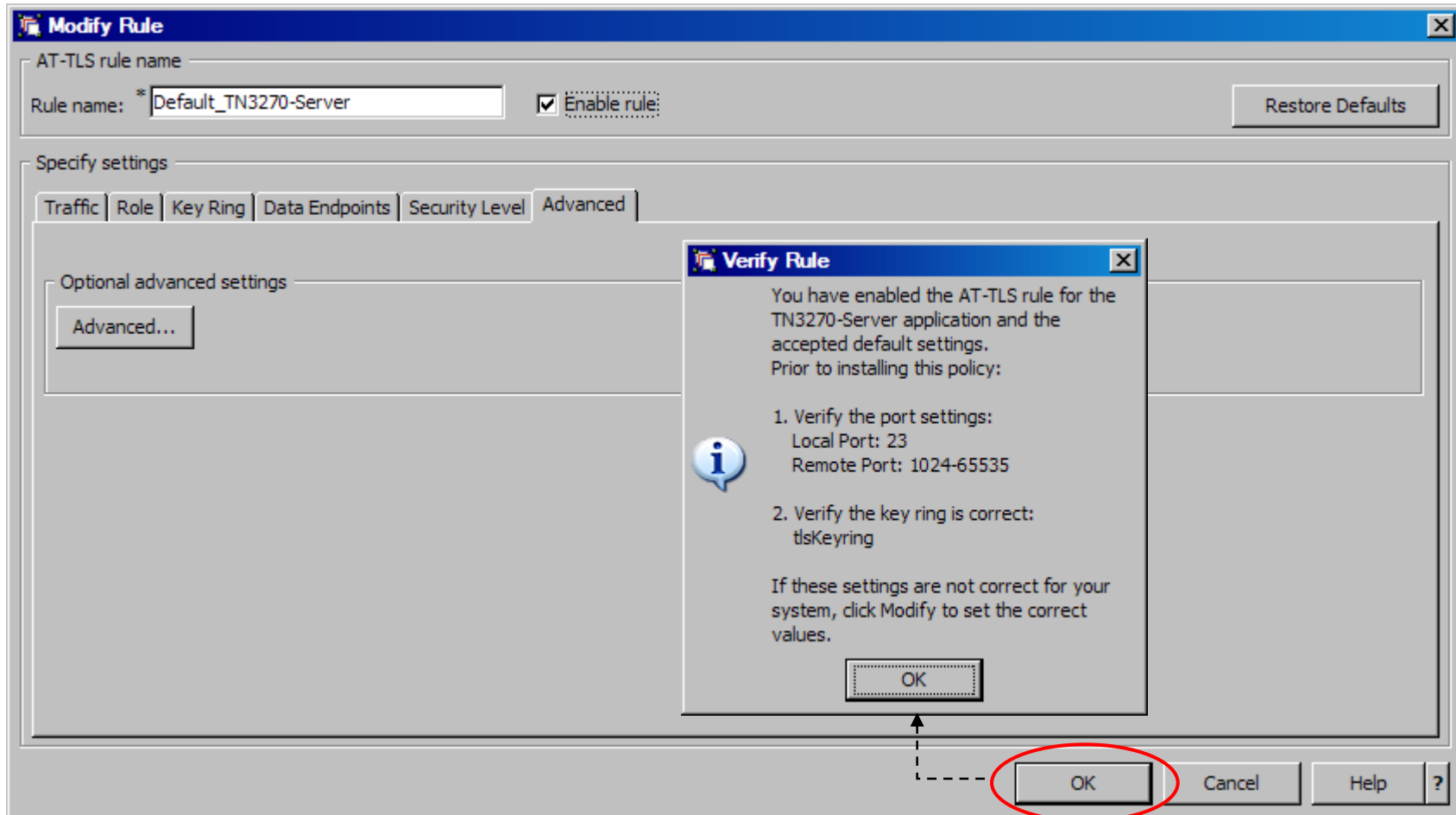


## Specify details of TLS protection

The screenshot shows a 'Modify Rule' dialog box with the following elements:

- AT-TLS rule name:** A text field containing 'Default\_TN3270-Server' and an 'Enable rule' checkbox.
- Specify settings:** A section with tabs for 'Traffic', 'Role', 'Key Ring', 'Data Endpoints', 'Security Level', and 'Advanced'. The 'Security Level' tab is active.
- Select the security level that will protect this traffic descriptor:** A dropdown menu showing 'Default\_Ciphers - IBM supplied: 3DES, AES-256 bit, AES-128 bit encryption'.
- Buttons:** 'New...', 'Copy...', 'Modify...', 'View Details', and 'Show Where Used' are located below the dropdown.
- Footer:** 'OK', 'Cancel', 'Help', and '?' buttons are at the bottom right.

# Enable rule



# Pre-defined TN3270 server rule is now enabled



V1R13 Configuration Assistant - Backing Store (Read-Write) = C:\Program Files\IBM\zCSConfigAssist\V1R13\files\saveData

File Edit Perspective Help

## AT-TLS Perspective

Navigation tree

- AT-TLS
  - Reusable Objects
    - Traffic Descriptors
    - Security Levels
    - Address Groups
    - Requirement Maps
  - z/OS Images
    - Image - ZOS01
      - Stack - TCPSTK01

TCP/IP stack name: \* TCPSTK01

Description: TCP/IP Stack 1

z/OS release: V1R13

Enable the rule you would like to have in your AT-TLS policy.  
To enable a rule, right click on the row and select Enable Rule.

Status	Rule Name	Application / Requirement Map	Key Ring
Disabled	Default_CSSMTP	CSSMTP	tlsKeyring
Disabled	Default_FTP-Client	FTP-Client	tlsKeyring
Disabled	Default_FTP-Server	FTP-Server	tlsKeyring
Disabled	Default_IMS-Connect	IMS-Connect	tlsKeyring
Disabled	Default_JES-Client	JES-Client	tlsKeyring
Disabled	Default_JES-Server	JES-Server	tlsKeyring
Disabled	Default_LBA-Advisor	LBA-Advisor	tlsKeyring
Disabled	Default_MSM	MSM	tlsKeyring
Disabled	Default_NETCONV	NETCONV	tlsKeyring
Disabled	Default_NSS_Client-IKED	NSS_Client-IKED	tlsKeyring
Disabled	Default_NSS_Server	NSS_Server	tlsKeyring
Disabled	Default_PolicyAgentImport	PolicyAgentImport	tlsKeyring
Disabled	Default_RRSF-Client	RRSF-Client	tlsKeyring
Disabled	Default_RRSF-Server	RRSF-Server	tlsKeyring
Enabled	Default_TN3270-Server	TN3270-Server	tlsKeyring

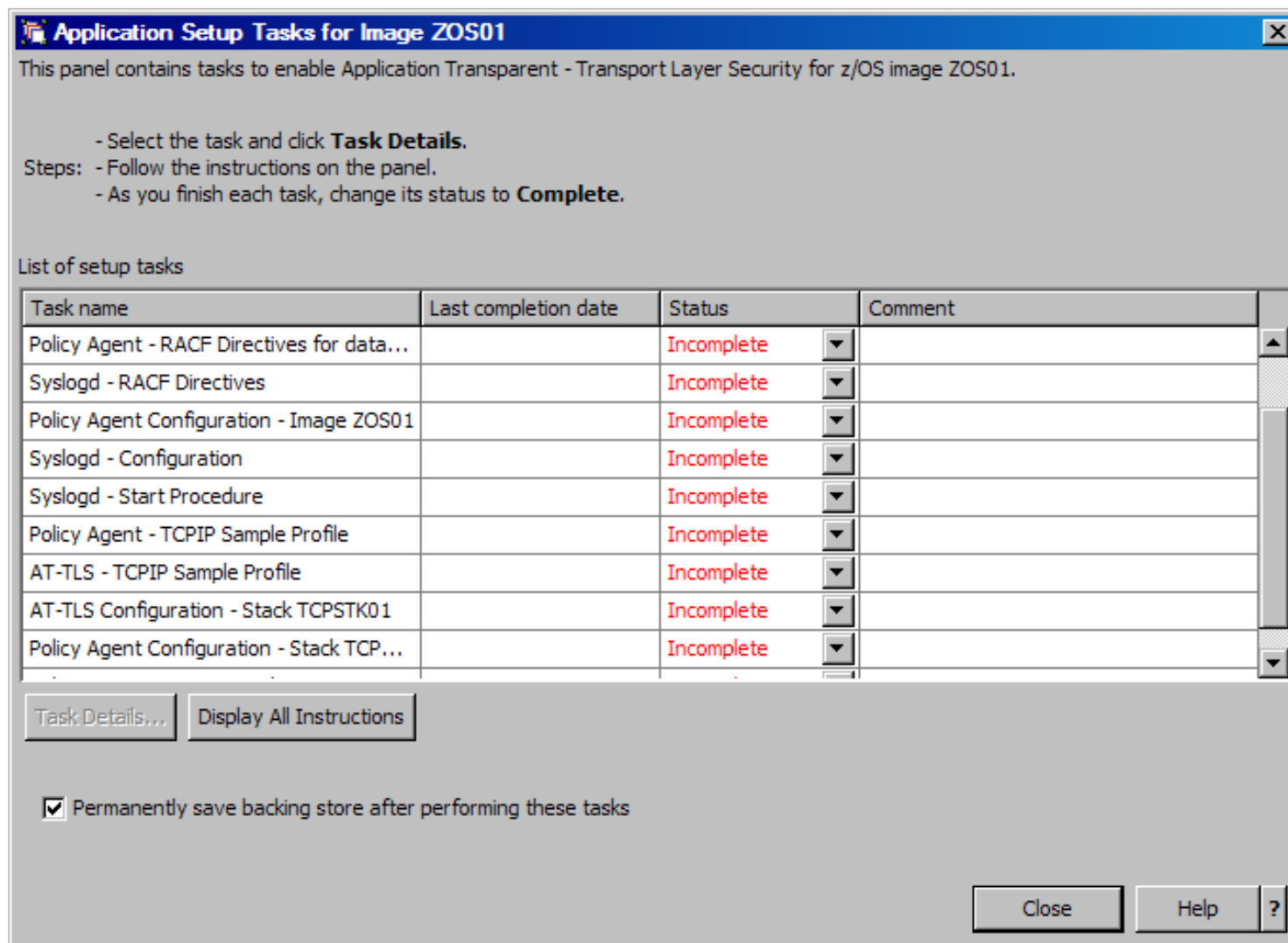
Modify... Copy... Add... Delete Move Up View Details Health Check

Move Down

Main Perspective Apply Changes OK Cancel Help ?

# Application setup task checklist guide to setting up policy infrastructure

## Assistance with the z/OS System Preparation Tasks – Use the Application Setup Task Checklist



**Application Setup Tasks for Image ZOS01**

This panel contains tasks to enable Application Transparent - Transport Layer Security for z/OS image ZOS01.

- Select the task and click **Task Details**.

Steps:

- Follow the instructions on the panel.
- As you finish each task, change its status to **Complete**.

List of setup tasks

Task name	Last completion date	Status	Comment
Policy Agent - RACF Directives for data...		Incomplete	
Syslogd - RACF Directives		Incomplete	
Policy Agent Configuration - Image ZOS01		Incomplete	
Syslogd - Configuration		Incomplete	
Syslogd - Start Procedure		Incomplete	
Policy Agent - TCPIP Sample Profile		Incomplete	
AT-TLS - TCPIP Sample Profile		Incomplete	
AT-TLS Configuration - Stack TCPSTK01		Incomplete	
Policy Agent Configuration - Stack TCP...		Incomplete	

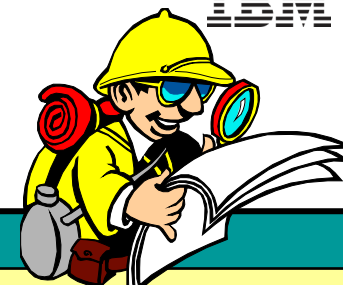
Permanently save backing store after performing these tasks

## For more information...

- IBM Configuration Assistant for z/OS Communications Server V1R12 download at <http://www.ibm.com/support/docview.wss?uid=swg24013160>
- *IBM z/OS V1R12 Communications Server TCP/IP Implementation Volume 4: Security and Policy-Based Networking (SG24-7899)*
- *z/OS Communications Server V1R12 IP Configuration Guide (SC31-8775 )*
- *z/OS Communications Server V1R12 IP Configuration Reference (SC31-8776)*
- *z/OS V1R12 Cryptographic Services System SSL Programming (SC24-5901-09)*







For more information...

URL		Content
<a href="http://www.twitter.com/IBM_Commserver">http://www.twitter.com/IBM_Commserver</a>		IBM Communications Server Twitter Feed
<a href="http://www.facebook.com/IBMCommserver">http://www.facebook.com/IBMCommserver</a>		IBM Communications Server Facebook Fan Page
<a href="http://www.ibm.com/systems/z/">http://www.ibm.com/systems/z/</a>		IBM System z in general
<a href="http://www.ibm.com/systems/z/hardware/networking/">http://www.ibm.com/systems/z/hardware/networking/</a>		IBM Mainframe System z networking
<a href="http://www.ibm.com/software/network/commserver/">http://www.ibm.com/software/network/commserver/</a>		IBM Software Communications Server products
<a href="http://www.ibm.com/software/network/commserver/zos/">http://www.ibm.com/software/network/commserver/zos/</a>		IBM z/OS Communications Server
<a href="http://www.ibm.com/software/network/commserver/z_lin/">http://www.ibm.com/software/network/commserver/z_lin/</a>		IBM Communications Server for Linux on System z
<a href="http://www.ibm.com/software/network/ccl/">http://www.ibm.com/software/network/ccl/</a>		IBM Communication Controller for Linux on System z
<a href="http://www.ibm.com/software/network/commserver/library/">http://www.ibm.com/software/network/commserver/library/</a>		IBM Communications Server library
<a href="http://www.redbooks.ibm.com">http://www.redbooks.ibm.com</a>		ITSO Redbooks
<a href="http://www.ibm.com/software/network/commserver/zos/support/">http://www.ibm.com/software/network/commserver/zos/support/</a>		IBM z/OS Communications Server technical Support – including TechNotes from service
<a href="http://www.ibm.com/support/techdocs/atmastr.nsf/Web/TechDocs">http://www.ibm.com/support/techdocs/atmastr.nsf/Web/TechDocs</a>		Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
<a href="http://www.rfc-editor.org/rfcsearch.html">http://www.rfc-editor.org/rfcsearch.html</a>		Request For Comments (RFC)
<a href="http://www.ibm.com/systems/z/os/zos/bkserv/">http://www.ibm.com/systems/z/os/zos/bkserv/</a>		IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server