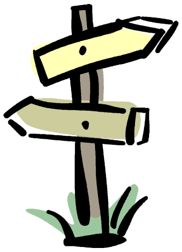
CS z/OS Application Transparent Transport Layer Security (AT-TLS)

AT-TLS agenda

- AT-TLS concepts and modes of operation
- AT-TLS Netstat reports
- Things to think about



AT-TLS concepts and modes of operation

AT-TLS basic principles

➢ **Configured AT-TLS policy for the TCP application to use AT-TLS:**

1 Client connects to server and connection becomes established

2 Server sends data in the clear and TCP layer queues it.

3 TCP layer invokes System SSL to perform SSL handshake under identity of the server.

4 TCP layer invokes System SSL to encrypt queued data and sends it to client.

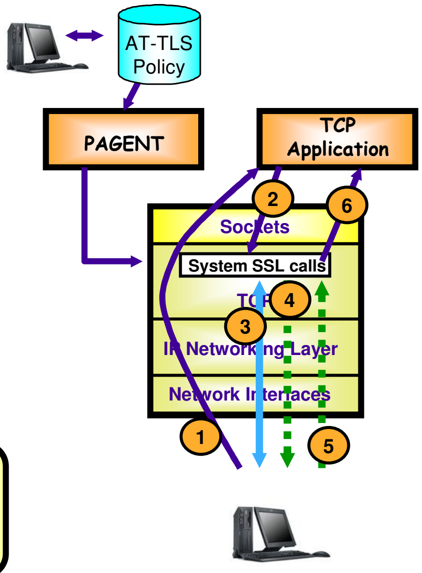
5 Client sends encrypted data, TCP layer invokes System SSL to decrypt.

6 Server receives data in the clear.

⟷ Un-encrypted (clear-text) flows

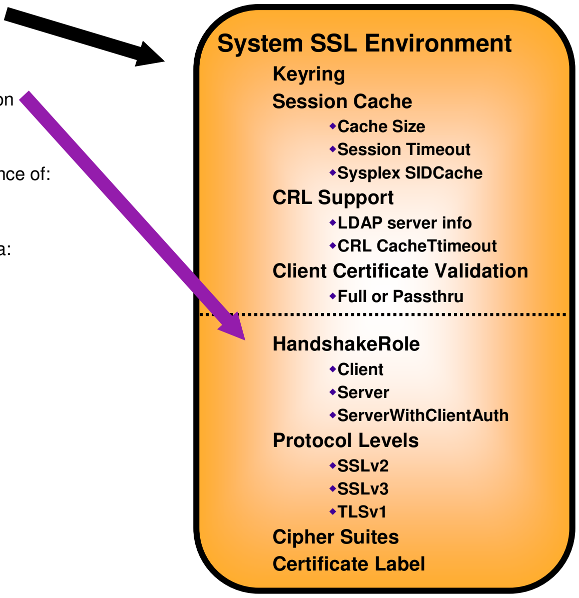
⟷ SSL/TLS handshake flows

▪▪▪▪▶ SSL/TLS-secured (encrypted) flows



AT-TLS environment concepts

- **TTLSEnvironmentAction**
  - Values for System SSL Environment Attributes
- **TTLSConnectionAction**
  - Values for SSL Attributes overridden at Connection
- **System SSL Environment Sharing Rules**
  - Connection policy must reference the same instance of:
    - TTLSGroupAction
    - TTLSEnvironmentAction
  - Connection must meet one of the following criteria:
    - Same process ID and user ID or
    - Same server process family
      - HandShakeRole Server and
      - Passive connection with same parent process and port and same user ID as siblings
- **System SSL Environment Life Cycle**
  - Dynamically created when none found to share
  - Dynamically removed when
    - TTLSEnvironmentAction is active and
      - No connections for 10-20 minutes
    - TTLSEnvironmentAction is stale and
      - No current connections

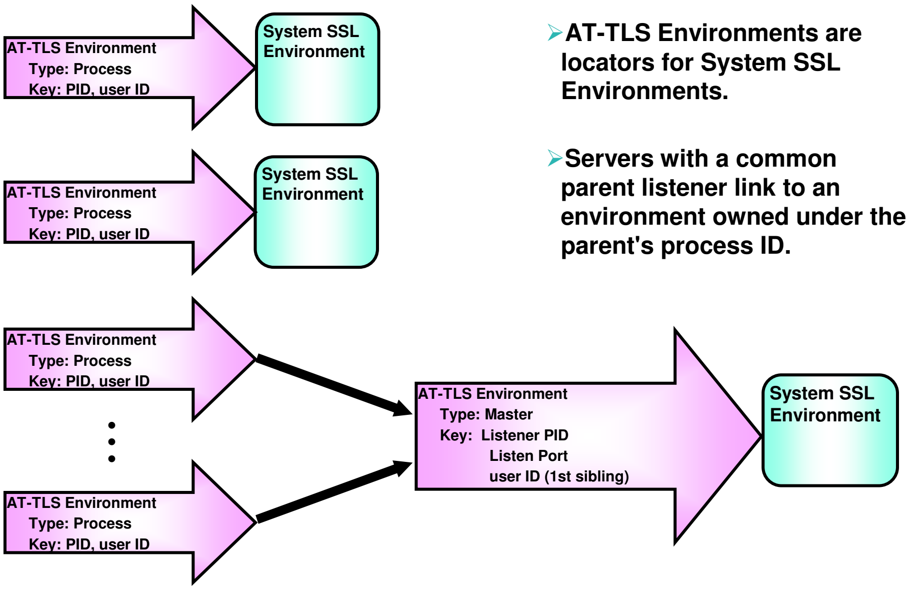


System SSL Environment

- **Keyring**
- **Session Cache**
  - **Cache Size**
  - **Session Timeout**
  - **Sysplex SIDCache**
- **CRL Support**
  - **LDAP server info**
  - **CRL CacheTtimeout**
- **Client Certificate Validation**
  - **Full or Passthru**

- **HandshakeRole**
  - **Client**
  - **Server**
  - **ServerWithClientAuth**
- **Protocol Levels**
  - **SSLv2**
  - **SSLv3**
  - **TLSv1**
- **Cipher Suites**
- **Certificate Label**

AT-TLS environments



- **AT-TLS Environments are locators for System SSL Environments.**

- **Servers with a common parent listener link to an environment owned under the parent's process ID.**

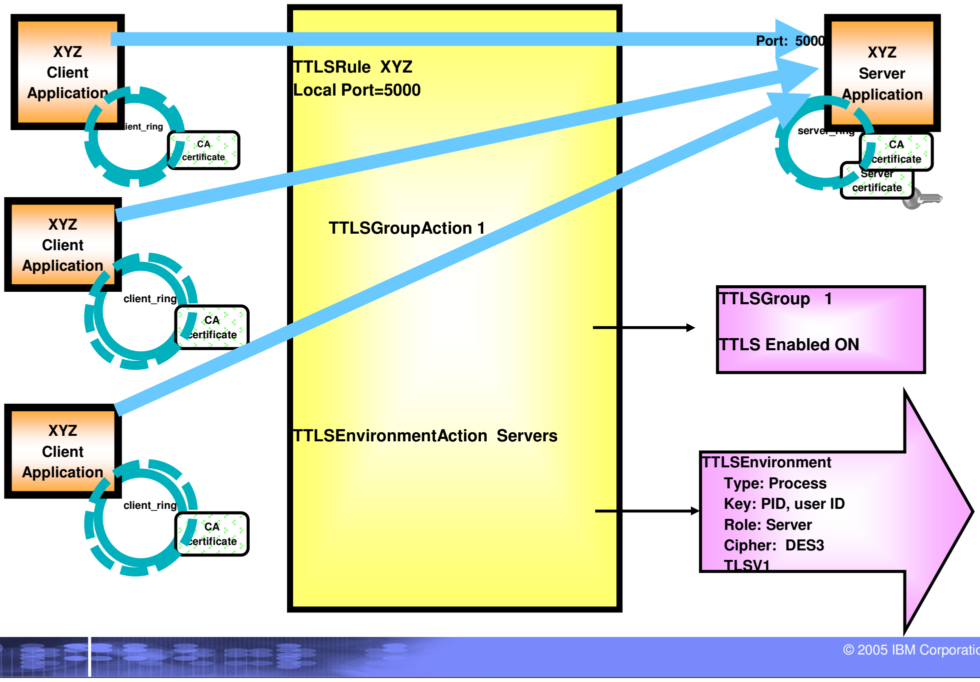
AT-TLS policy preview

PolicyAgent main configuration file

- CommonTTLSConfig statement names a file containing AT-TLS objects shared across TCP/IP stacks
    - TTLSRule statements
    - TTLSGroupAction statements
    - TTLSEnvironmentAction statements
    - TTLSConnectionAction statements

- PEPInstance statement names a file containing policy for one TCP/IP stack
    - TTLSConfig statement names a file containing AT-TLS objects for this stack
        - TTLSRule statements
        - TTLSGroupAction statements
        - TTLSEnvironmentAction statements
        - TTLSConnectionAction statements

AT-TLS basic policy overview



TTLSRule XYZ
Local Port=5000

TTLSGroupAction 1

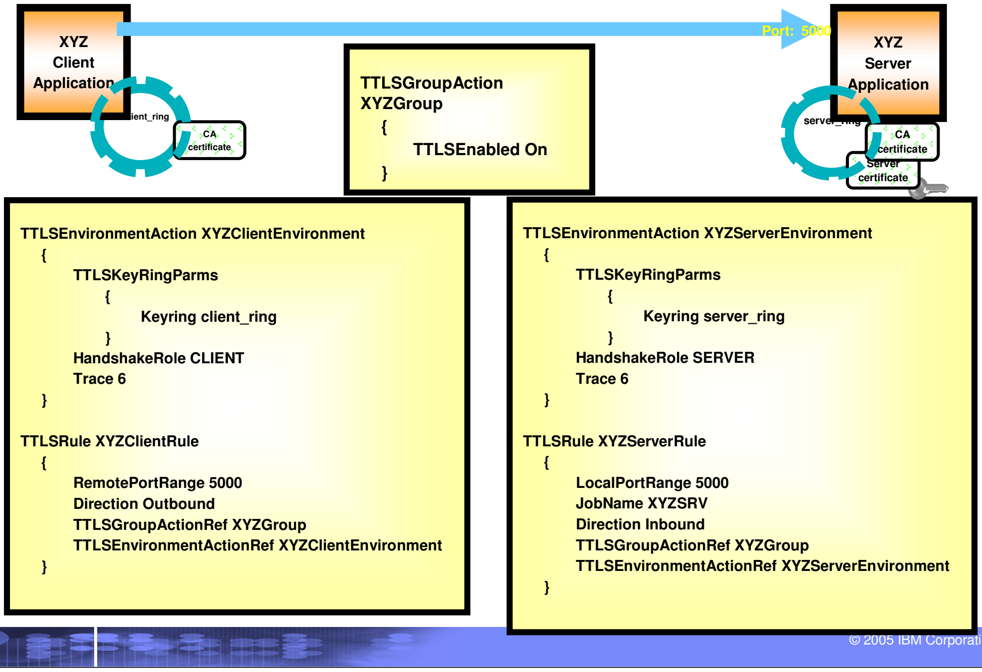
TTLSEnvironmentAction Servers

TTLSGroup 1

TTLS Enabled ON

TTLSEnvironment
Type: Process
Key: PID, user ID
Role: Server
Cipher: DES3
TLSV1

AT-TLS basic policy examples



```
TTLSGroupAction
XYZGroup
   {
         TTLSEnabled On
   }
```

```
TTLSEnvironmentAction XYZClientEnvironment
   {
        TTLSKeyRingParms
             {
                  Keyring client_ring
             }
        HandshakeRole CLIENT
        Trace 6
   }

TTLSRule XYZClientRule
   {
        RemotePortRange 5000
        Direction Outbound
        TTLSGroupActionRef XYZGroup
        TTLSEnvironmentActionRef XYZClientEnvironment
   }
```

```
TTLSEnvironmentAction XYZServerEnvironment
   {
        TTLSKeyRingParms
             {
                  Keyring server_ring
             }
        HandshakeRole SERVER
        Trace 6
   }

TTLSRule XYZServerRule
   {
        LocalPortRange 5000
        JobName XYZSRV
        Direction Inbound
        TTLSGroupActionRef XYZGroup
        TTLSEnvironmentActionRef XYZServerEnvironment
   }
```

AT-TLS policy mapping

- **Rule search**
  - One-time event for each connection
  - Result persists for life of connection
  - Search order is Rule Name (alphanumeric) within Priority (high to low)
  - Conditions:
    - Connection direction, Local / remote IP address and port, Jobname, User ID

- **Security context**
  - Caller's security context is "cloned" into stack at time of mapping
    - Includes: User ID, Group ID, UID and GID
  - This security context is used to access keyring and certificate keys

- **Mapping events**
  - Outbound
    - Connect
  - Inbound
    - Select or poll for readable or writable
    - Any form of read or write
  - SIOCTTLSCTL ioctl

- **Secure session auto start**
  - If ApplicationControlled Off, Secure connection is AutoStarted when mapped except
    - On connect, AutoStart is deferred until connection is established
    - SIOCTTLSCTL ioctl never AutoStarts

AT-TLS policy mapping rationale

NOTES

- A critical aspect of AT-TLS operation is the security context cloning required to access keyrings and certificates on behalf of an owning application. Analysis of several common application models indicated the need to defer security context cloning on inbound connections to sometime after accept().

- This is most apparent in the family of servers invoked by inetd. The passive socket is created by inetd {socket(), bind(), listen()}. New connections are recognized by inetd {accept()}. Based on the port connected to, inetd creates a new server process {fork()}, optionally changes the security context in the new process {setuid()}, and then turns control over to the server program {exec()}. In many cases, the application protocol includes some form of login negotiation. The server program then changes its security context to one supplied by the client over the new connection.

- The optimal security context to clone is the one initially used by the server process. The inetd security context does not allow enough granularity and protection of server certificates - any server invoked by inetd could be configured to use any server certificate that inetd had access to. The client security context would require all clients to have access to the server's private keys - this would be a serious breach of security.

- In all analyzed application models, the server security context is the one presented to the stack on the first data oriented service requested over the socket.

AT-TLS application types

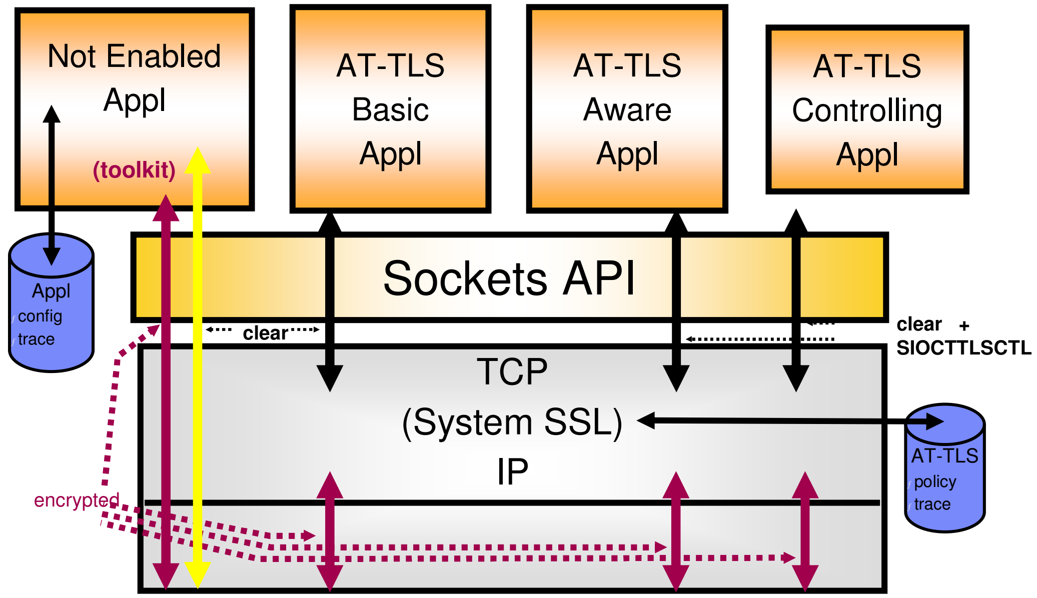
- **Not enabled**
  - Pascal API and Web Fast Response Cache Accelerator (FRCA) not supported
  - No policy or policy explicitly says Enabled OFF
    - Includes those permitted to start during InitStack window
  - Application may optionally use SSL or TLS toolkit directly

- **Basic**
  - Policy says Enabled ON
  - Application unchanged and unaware of AT-TLS
  - Application protocol unaffected by use of AT-TLS (consider http: versus https:)

- **Aware**
  - Policy says Enabled ON
  - Application changed to use SIOCTTLSCTL ioctl to extract AT-TLS information:
    - Policy status, negotiated version and cipher, partner certificate, associated user ID

- **Controlling**
  - Application protocol may negotiate use of TLS in cleartext prior to starting secure session
  - Policy says Enabled ON and ApplicationControlled ON
  - Application changed to use SIOCTTLSCTL ioctl to extract and control AT-TLS
    - Policy status, negotiated version and cipher, partner certificate, associated user ID
    - Start secure session, reset session, reset cipher

AT-TLS structure



AT-TLS SIOCTTLSCTL IOCTL - Aware

- **Aware application wants to examine partner's certificate or associated user ID ...**
  - Establish new connection
  - Wait for handshake to complete on new connection (select for writable)
  - Ioctl SIOCTTLSCTL TTLSi_Req_Type = TTLS_QUERY_ONLY
  - On successful return
    - TTLSi_Stat_Policy = TTLS_POL_ENABLED
    - TTLSi_Stat_Conn = TTLS_CONN_SECURE
    - TTLSi_Sec_Type = certificate processing option defined in policy
    - TTLSi_Cert_Len = size of certificate buffer required
    - TTLSi_UserID = user ID associated with client certificate (Null terminated)
    - TTLSi_UserID_Len = number of characters before the first Null
  - Allocate storage for certificate
  - Ioctl SIOCTTLSCTL TTLSi_Req_Type = TTLS_RETURN_CERTIFICATE
    - TTLSi_BufferPtr = address of certificate buffer provided by application
    - TTLSi_BufferLen = size of certificate buffer provided by application
  - On successful return, certificate buffer contains System SSL certificate structure

- **Application can request certificate on first call if typical certificate size is known**
  - Failure with errno ENOBUFS
    - TTLSi_Cert_Len = size of certificate buffer required

AT-TLS SIOCTTLSCTL IOCTL - Aware

N O T E S

- TTLSi_Sec_Type =
  - TTLS_SEC_CLIENT
    - valid server certificate required
    - no associated user ID support
  - TTLS_SEC_SERVER
    - no client certificate available
  - TTLS_SEC_SRV_CA_PASS
    - client certificate optional
    - not validated by System SSL if presented
  - TTLS_SEC_SRV_CA_FULL
    - client certificate optional
    - validated by System SSL if presented
  - TTLS_SEC_SRV_CA_REQD
    - client certificate required
    - client certificate validated by System SSL
    - associated user ID optional
  - TTLS_SEC_SRV_CA_SAFCHK
    - client certificate required
    - client certificate validated by System SSL
    - associated user ID required

AT-TLS SIOCTTLSCTL IOCTL - Controlling

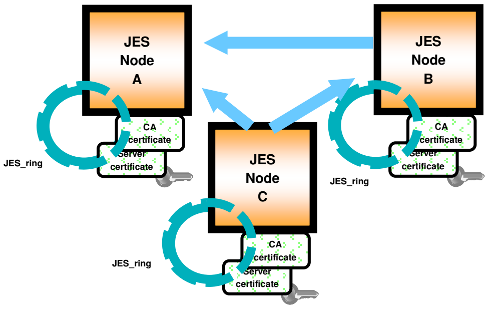
- **Controlling application wants to negotiate use of TLS ...**
  - Establish new connection
  - Ioctl SIOCTTLSCTL TTLSi_Req_Type = TTLS_QUERY_ONLY
    - TTLSi_Stat_Policy = TTLS_POL_APPLCNTRL
      - Enabled ON, ApplicationControlled ON
    - TTLSi_Stat_Conn = TTLS_CONN_NOTSECURE
      - ApplicationControlled ON and application has not yet started secure session
  - Send and receive cleartext application protocol records to negotiate connection security
    - Close connection or
    - Continue in cleartext or
    - Start handshake (ApplicationControlled ON)
      - Do not leave unread application record data
      - Do not read past application record data
      - Ioctl SIOCTTLSCTL TTLSi_Req_Type = TTLS_INIT_CONNECTION
      - Optionally wait for handshake to complete on connection (select for writable)
      - Optionally use SIOCTTLSCTL to query, reset session or reset cipher at any time
  - Send and receive cleartext application protocol data (AT-TLS handles ciphertext on wire)

AT-TLS SIOCTTLSCTL IOCTL - Controlling

NOTES

- TTLSi_Stat_Policy =
  - TTLS_POL_OFF
    - TCPCONFIG NOTTLS
    - AT-TLS not enabled in this stack
  - TTLS_POL_NO_POLICY
    - Connection didn't map
    - This connection did not match any AT-TLS rule
  - TTLS_POL_NOT_ENABLED
    - Enabled OFF
    - The policy for this connection prevents use of AT-TLS
  - TTLS_POL_ENABLED
    - Enabled ON, ApplicationControlled OFF
    - Stack will autostart handshake
  - TTLS_POL_APPLCNTRL
    - Enabled ON, ApplicationControlled ON
    - Connection is cleartext until application starts secured session
- TTLSi_Stat_Conn =
  - TTLS_CONN_NOTSECURE
    - AT-TLS not possible or
    - ApplicationControlled OFF and application has not caused AutoStart (connect, read, write, select)
    - ApplicationControlled ON and application has not issued SIOCTTLSCTL TTLS_INIT_CONNECTION
  - TTLS_CONN_HS_INPROGRESS
    - AT-TLS already started handshake
  - TTLS_CONN_SECURE
    - AT-TLS already completed handshake

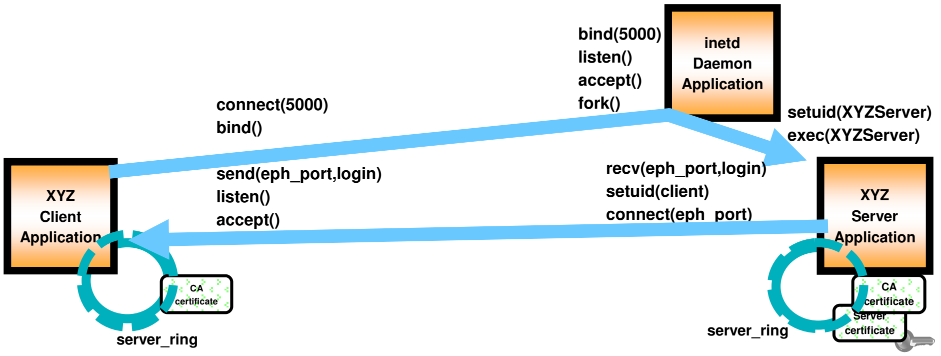
AT-TLS common policy examples (peer)



- **JES peer network**
  - Each node tries all known nodes, then listens for others.
  - Use of TLS negotiated in the clear.
  - HandshakeRole follows connect direction.

```
TTLSEnvironmentAction JESEnvironment
{
          HandshakeRole Server
          TTLSKeyRingParms
          {
                    Keyring JES_ring
          }
          Trace 6
          TTLSEnvironmentAdvancedParms
          {
                    ApplicationControlled             ON
          }
}
TTLSConnectionAction            ClientConnection
{
          HandshakeRole Client
}
TTLSRule JESInbound
{
          JobName         JES
          Direction       Inbound
          TTLSGroupActionRef
          EnabledGroup
          TTLSEnvironmentActionRef          JESEnvironment
}
TTLSRule JESOutbound
{
          JobName         JES
          Direction       Outbound
          TTLSGroupActionRef
          EnabledGroup
          TTLSEnvironmentActionRef          JESEnvironment
          TTLSConnectionActionRef
          ClientConnection
}
```

Applications with secondary connections



bind(5000)
listen()
accept()
fork()

inetd
Daemon
Application

connect(5000)
bind()

setuid(XYZServer)
exec(XYZServer)

XYZ
Client
Application

send(eph_port,login)
listen()
accept()

recv(eph_port,login)
setuid(client)
connect(eph_port)

XYZ
Server
Application

- Some applications create a second connection between the client and the forked server instance. This second connection can be established in either direction.

- Some applications use two dynamically assigned ports (for example, rexec or rsh stderr connection). It can be difficult to define an effective rule for these connections.

- In other applications the server changes to a client login identity before the second connection is mapped (for example, FTP data connection). The server's security context is no longer available for accessing the server's keyring and certificate keys.

AT-TLS SecondaryMap

- **AT-TLS policy for primary connection**
  - TTLSxxxActionAdvancedParms
    - SecondaryMap ON
  - Primary connection is recorded in internal table
    - Entry created when primary connection is mapped
    - Indexed by process ID, local IP, and remote IP
    - Entry removed when primary connection closes

- **When future connections are mapped**
  - Normal policy lookup
  - Check internal table for primary connection with
    - Same process ID and same IP endpoints
  - New connection is a secondary connection if match found in internal table and
    - No policy found for new connection or
    - Found policy is lower priority than primary connection policy
  - Secondary connections
    - Share SSL Environment with primary connection
    - Use security context from primary connection

- **Application model requirements**
  - One primary connection (serially reused client, forking server)
  - May have multiple secondary connections

AT-TLS common policy parameters

NOTES

- TTLSEnabled
  - Controls whether AT-TLS should be used on connections mapping to this policy. Provided so that AT-TLS can be disabled for a subset of connections that would otherwise map to a broader policy with AT-TLS enabled.

- Trace
  - Controls the level of AT-TLS tracing. Defined values correspond to bit flags and are additive.

–1	error	joblog
–2	error	syslogd
–4	info	
–8	event	
–16 flow		
–32 data		

  - Default is 2, errors to syslogd. Recommended value for new policies is 6 (2 + 4), errors, map and start messages to syslogd. Values above 7 (1 + 2 + 4) may result in large numbers of messages to syslogd and are intended for problem diagnosis not production.

- HandShakeRole
  - Defines the role to be played by this end of the connection in the SSL Handshake Protocol. This is typically consistent with the direction of the connection: outbound is client and inbound is server, but is not required to be. Server side must always have a server or site certificate. Client only needs a user certificate if server side requires client authentication.

AT-TLS common policy parameters (continued)

NOTES

- Keyring
  - Defines the name of the keyring. To minimize administration, RACF keyrings with a common name are recommended. The user ID will be automatically prepended when the System SSL Environment is initialized. Gskkyman keyring names are UNIX path names.
- KeyringPw, KeyringStashFile
  - GSKKman keyrings require a password. You can provide the password or the pathname of the stashfile that contains the password. Do not specify either parameter with RACF keyrings.
- V2CipherSuites, V3CipherSuites
  - List of cipher suites you are willing to use. Server side determines order of preference. Values entered as string of hex characters. Policy Agent calls System SSL to validate values. AT-TLS has no default. If parameter is not specified, System SSL uses its default.
- GroupUserInstance, EnvironmentUserInstance, ConnectionUserInstance
  - These fields are reserved for customer use. They can be used for change management.
  - They can also be used to force reinitialization of an AT-TLS Group or System SSL Environment when no other parameters have changed in an action. If the contents of a keyring have changed, the EnvironmentUserInstance field may be used to cause new connections to use the new certificates without affecting the application or current connections.

AT-TLS advanced policy parameters

NOTES

- SSLv2, SSLv3 and TLSv1
  - The SSLv2 protocol is supported but is not as secure as the SSLv3 or TLSv1 protocols. The AT-TLS default is to enable the SSLv3 and TLSv1 protocols but to disable the SSLv2 protocol. You should only turn SSLv2 on if you must support connections with older applications that do not support the more secure protocols.
- HandshakeTimeout
  - This parameter controls the amount of time AT-TLS will wait during the SSL handshake. Timeouts can be caused by configuration mismatches or long delays in initial connection processing by applications.
- ResetCipherTimer
  - The SSLv3 and TLSv1 protocols allow the encryption key to be renegotiated during a secure connection. This can provide a higher level of security for long-running connections. The AT-TLS default is to not reset the cipher. You may specify a time interval to cause AT-TLS to request a reset of the cipher in the range of 1 to 1440 seconds. The cipher reset will be requested when the timer expires and the next application read or write completes. The time interval is restarted when the cipher has been changed.
- CertificateLabel
  - If you need to use a certificate other than the keyring's default one, you should specify the other certificate's name.
- ClientAuthType
  - For policies that specify HandshakeRole ServerWithClientAuth, this parameter specifies what actions AT-TLS should take to authenticate the client certificate.

AT-TLS advanced policy parameters **(continued)**

NOTES

- CtraceClearText
  - Applications that implement SSL or TLS can control whether unencrypted application data is included in diagnostic traces. Lower layers only have access to encrypted data. When using AT-TLS, the TCP, PFS and SOCKAPI layers have access to unencrypted data. The AT-TLS default is to suppress this data in CTRACE records generated by these layers to protect the application's users. If you need to see this data in these records to diagnose a problem, you can set CtraceClearText ON.
- ApplicationControlled
  - Application needs to control secure session.
- SecondaryMap
  - Application creates second connection that needs to use primary connection policy and System SSL environment.
- EnvFile
  - This parameter specifies the name of a file containing environment variable assignments that modify the behavior of z/OS Language Environment or System SSL. This parameter should normally only be used under the direction of IBM service.
- SyslogFacility
  - This parameter controls whether AT-TLS trace messages written to syslogd by this group use the syslog facility name Daemon or Auth. The default is Daemon. It can be set only in TTLSGroupAdvancedParms.
  - You can use this parameter to isolate messages written by some AT-TLS groups from messages written by the other groups. You can also use it to isolate AT-TLS messages from those written by the stack's SNMPsub-agent.

AT-TLS advanced policy parameters (continued)

NOTES

- GSK_LDAP_SERVER, GSK_LDAP_SERVER_PORT, GSK_LDAP_USER, GSK_LDAP_USER_PW, GSK_CRL_CACHE_TIMEOUT
  - Applications using HandshakeRole ServerWithClientAuth may optionally use a Certificate Revocation List (CRL) service. This service is provided by an LDAP server. This set of parameters is used to configure System SSL so that it can contact the CRL service. Connections used by System SSL to contact the CRL service should not fall under an Enabled AT-TLS policy because these connections may be made before AT-TLS policy has been installed.

- GSK_V2_SIDCACHE_SIZE, GSK_V2_SESSION_TIMEOUT, GSK_V3_SIDCACHE_SIZE, GSK_V3_SESSION_TIMEOUT
  - These parameters allow you to configure the System SSL SID cache in your application environment. The size parameters control how many different partners session information is cached for. The timeout parameters control how long the session information should be kept in the cache. When session information is found in the cache, connections may use the SSL short handshake, which requires less processing.

- GSK_SYSPLEX_SIDCACHE
  - Applications may use AT-TLS with Sysplex Distributor. Setting this parameter on instructs System SSL to make the SID cache available across the Sysplex.

SAF InitStack SERVAUTH profile

- **Exposure: The stack is not secure until Policy Agent installs policy**
  - Connections established before policy installation never use AT-TLS
  - Causes application failures or unprotected network traffic

- **AT-TLS stack initialization window**
  - From completion of initial TCPIP.PROFILE processing with AT-TLS enabled
  - MSG: EZZ4248E tcpname WAITING FOR PAGENT TTLS POLICY
  - Until either
    - Policy Agent installs AT-TLS policy or
    - Vary Obeyfile command disables AT-TLS

- **SAF profile limits access to stack during window**
  - Only permit required network infrastructure applications such as:
    - Policy Agent, Name Server, OMPROUTE, LDAP, Firewall
    - Connections mapped during the window will not have AT-TLS policy available
  - Non-permitted applications are told stack is not yet up
    - errno: EAGAIN errno2: JrTcpNotActive

- **Common INET new stack notification is deferred until window closes**
  - setibmsockopt SO_EioIfNewTP

TCPCONFIG ... TTLS/NOTTLS ....

AT-TLS Netstat reports

AT-TLS information added to Netstat all report

```
D TCPIP,TCPCS3,N,ALL
EZD0101I NETSTAT CS V1R7 TCPCS3 304
CLIENT NAME: FTPD1                    CLIENT ID: 00000031
LOCAL SOCKET: 9.42.104.156..21        FOREIGN SOCKET: 9.27.154.137..1638
  LAST TOUCHED:       16:46:15          STATE:              ESTABLISH
  BYTESIN:            0000001062        BYTESOUT:           0000000480
  SEGMENTSIN:         0000000019        SEGMENTSOUT:        0000000019
  RCVNXT:             3296375906        SNDNXT:             3296308452
  CLIENTRCVNXT:       3296375906        CLIENTSNDNXT:       3296308452
  INITRCVSEQNUM:      3296374843        INITSNDSEQNUM:      3296307971
  CONGESTIONWINDOW:   0000340353        SLOWSTARTTHRESHOLD: 0000016384
  INCOMINGWINDOWNUM:  3296408638        OUTGOINGWINDOWNUM:  3296341180
  SNDWL1:             3296375906        SNDWL2:             3296308452
  SNDWND:             0000032728        MAXSNDWND:          0000032768
  SNDUNA:             3296308452        RTT_SEQ:            3296308412
  MAXIMUMSEGMENTSIZE: 0000065483        DSFIELD:            00
  ROUND-TRIP INFORMATION:
    SMOOTH TRIP TIME: 37.000            SMOOTHTRIPVARIANCE: 101.000
  REXMT:              0000000000        REXMTCOUNT:         0000000000
  DUPACKS:            0000000000
  SOCKOPT:            00                TCPTIMER:           00
  TCPSIG:             00                TCPSEL:             C0
  TCPDET:             F0                TCPPOL:             00
  QOSPOLICYRULENAME:
  TTLSPOLICY:         YES
    TTLSRULE:         FTP_SERV_21
    TTLSGRPACTION:    GRP_ACT1
    TTLSENVACTION:    ENV_ACT_SERV
  RECEIVEBUFFERSIZE:  0000016384        SENDBUFFERSIZE:     0000016384
```

New Netstat filter to limit connection reports to AT-TLS connections

- **Netstat filter (CONNType/-X) added to limit ALLConn/-a and COnn/-c responses by connection type**

- **Subfilters allow for specification of connection type:**

  - NOTTLSPolicy
    - Connections not mapped to AT-TLS policy
  - TTLSPolicy
    - Connections mapped to AT-TLS policy
  - TTLSPolicy,CURRent
    - Connections mapped to AT-TLS policy - rule and actions still available for use with new connections
  - TTLSPolicy,GRoup=groupid
    - Connections using the specified AT-TLS group
  - TTLSPolicy,STALE
    - Connections mapped to AT-TLS policy - rule or at least one action no longer available for use with new connections

```
--CONNType-+-NOTTLSPolicy-----------------+------>
           '-TTLSPolicy-+---------------+-'
                        +-CURRent-------+
                        +-GRoup-groupid-+
                        '-STALE---------'
```

New Netstat TTLS report added

- **Netstat option (TTLS/-x) added to display AT-TLS data**
  - Suboptions allow for display of specific AT-TLS data:
    - GRoup
      - Summary information for AT-TLS groups.
    - GRoup,DETAIL
      - Detailed information for AT-TLS groups.
    - COnn=connid
      - Name of AT-TLS policy rule and names of associated actions for specified connection.
    - COnn=connid,DETAIL
      - Details of AT-TLS policy rule and associated actions for specified connection.

```
          .-GRoup-----------------------.
   --TTLS-+-----------------------------+--------
>
          +-COnn-connid--+--------+-----+
          |              '-DETAIL-'     |
          '-GRoup--+--------+-----------'
                   '-DETAIL-’
```

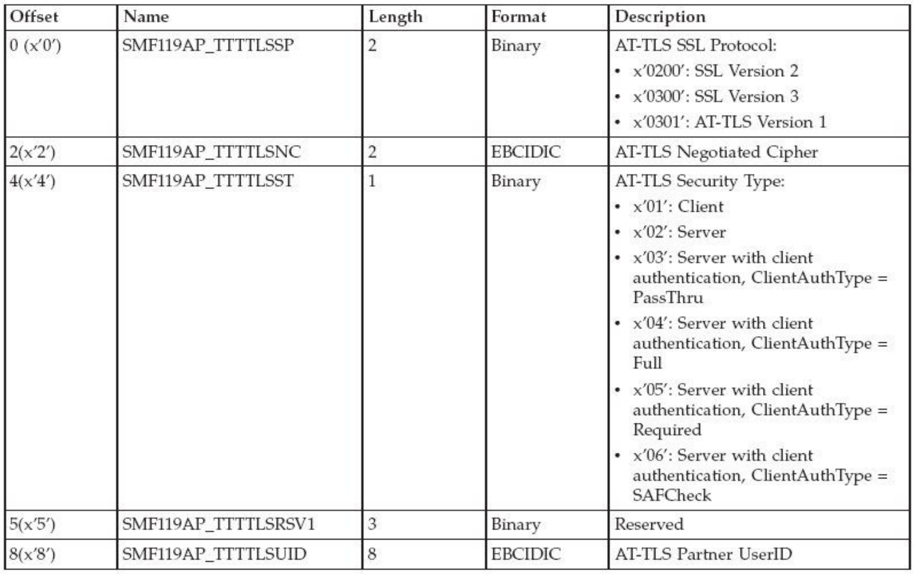
Netstat TTLS,CONN=connid report sample

```
D TCPIP,TCPCS3,TTLS,COnn=connid report:

D TCPIP,TCPCS3,N,TTLS,CONN=31
EZD0101I NETSTAT CS V1R7 TCPCS3 393
CONNID: 00000031
  JOBNAME:      FTPD1
  LOCALSOCKET:  ::FFFF:9.42.104.156..21
  REMOTESOCKET: ::FFFF:9.27.154.137..1638
  SECLEVEL:     TLS VERSION 1
  CIPHER:       05 TLS_RSA_WITH_RC4_128_SHA
  CERTUSERID:   N/A
  MAPTYPE:      PRIMARY
TTLSRULE: FTP_SERV_21
  TTLSGRPACTION:  GRP_ACT1
  TTLSENVACTION:  ENV_ACT_SERV
1 OF 1 RECORDS DISPLAYED
END OF THE REPORT
```

AT-TLS SMF records and network management interface changes

- **New SMF 119 TCP connection termination subsection if AT-TLS was used for the connection:**



Offset	Name	Length	Format	Description
0 (x'0')	SMF119AP_TTTTLSSP	2	Binary	AT-TLS SSL Protocol: • x'0200': SSL Version 2 • x'0300': SSL Version 3 • x'0301': AT-TLS Version 1
2(x'2')	SMF119AP_TTTTLSNC	2	EBCIDIC	AT-TLS Negotiated Cipher
4(x'4')	SMF119AP_TTTTLSST	1	Binary	AT-TLS Security Type: • x'01': Client • x'02': Server • x'03': Server with client authentication, ClientAuthType = PassThru • x'04': Server with client authentication, ClientAuthType = Full • x'05': Server with client authentication, ClientAuthType = Required • x'06': Server with client authentication, ClientAuthType = SAFCheck
5(x'5')	SMF119AP_TTTTLSRSV1	3	Binary	Reserved
8(x'8')	SMF119AP_TTTTLSUID	8	EBCIDIC	AT-TLS Partner UserID

Things to think about

Dependencies and restrictions - AT-TLS

- **z/OS Cryptographic Services System Secure Sockets Layer (System SSL)**
  - The PDS pdsename.SIEALNKE contains the System SSL DLLs.
  - It must be in the program search order for TCPIP and Policy Agent.
  - If it’s not in the linklist or LPA,
    - use the STEPLIB DD statement in your TCPIP JCL
    - use the STEPLIB environment variable in the shell:
      export STEPLIB=$STEPLIB:pdsename.SIEALNKE

- **z/OS UNIX APAR OA11339 is required.**
  - If it is not installed, all AT-TLS connections will fail with the message
    - syslogd: EZD1286I ... RC: 5019 Initial Handshake
    - console: EZD1287I ... RC: 5019 Initial Handshake

- **AT-TLS does not support the following applications.**
  - These connections will not map to AT-TLS policy.
  - They will be permitted to proceed in clear text.

    - Applications using the Pascal API to access TCP/IP
      - Line Print daemon and commands
      - LPD, LPQ, LPRM
      - Simple Mail Transfer Protocol (JES Spool Server)
      - TSO Telnet client
    - Web servers using Fast Response Cache Accelerator
    - Network administration applications permitted to EZB.INITSTACK profile
      - Connections established and mapped prior to installation of AT-TLS policy will proceed in clear text.
      - Connections established and mapped after installation of AT-TLS policy are subject to policy installed.

Migration considerations - AT-TLS

- **z/OS CS ships some applications with native SSL/TLS support.**
  - Some may use either the native support or AT-TLS.
  - Don't configure both for the same application!

- **Digital Certificate Access Server (DCAS)**
  - Not currently an AT-TLS Aware application
  - Do not use with AT-TLS

- **FTP client and FTPD server**
  - Must specify SecondaryMap in AT-TLS policy
  - If using implicit secure socket 990, see policy sample for guidance
    - /usr/lpp/tcpip/samples/pagent_TTLS.conf (/usr/lpp/tcpip/samples/IBM/EZAPAGFT)

- **TN3270E server**
  - Must specify Basic Port (no security information in TN displays)
  - No security parameters accepted
    - (Keyring/LDAP/Encryption/ConnType/SAFCert/ExpressLogon)

- **Sendmail**

IPSec and AT-TLS comparison - a few selected characteristics

	IPSec	AT-TLS
Traffic protected with data authentication and encryption	All protocols	TCP
End-to-end protection	Yes	Yes
Network segment protection	Yes	No
Scope of protection	Security association 1)all traffic 2)protocol 3)single connection	TLS session 1)single connection
How controlled	IPSec policy 1)z/OS responds to IKE peer 2)z/OS initiates to IKE peer based on outbound packet, IPSec command, or policy autoactivation	AT-TLS policy 1)For handshake role of server, responds to TLS client based on policy 2)For handshake role of client, initializes TLS based on policy 3)Advanced function applications
Requires application modifications	No	No, unless advanced function needed 1)Obtain client cert/userid 2)Start TLS
Type of security	Device to device	Application to application
Type of authentication	Peer-to-peer	1)Server to client 2)Client to server (opt)
Authentication credentials	1)Preshared keys 2)X.509 certificates	X.509 certificates
Authentication principals	Represents host	Represents user
Session key generation/refresh	Yes with IKE No with manual IPSec	TLS handshake

Trademarks, Copyrights, and Disclaimers

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

IBM
IBM(logo)
e(logo)business
AIX
CICS
Cloudscape
DB2
DB2 Universal Database
IMS
Informix
iSeries
Lotus
MQSeries
OS/390
OS/400
pSeries
Tivoli
WebSphere
xSeries
zSeries

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 registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

Other company, product and service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance 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 or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.