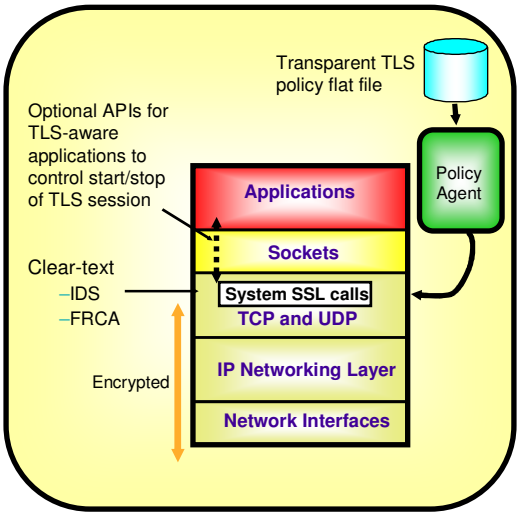
CS z/OS CICS Sockets SSL/TLS enabling

CICS Sockets enhancements in z/OS V1R7

- **Allow IP CICS Sockets to exploit the Application Transparent SSL/TLS functions in CS z/OS V1R7:**
  - SSL/TLS connections supported to CICS Sockets applications
    - Transparent to CICS Sockets server programs - no application code changes needed
    - Remote sockets client need to be able to do SSL also (if not running on z/OS)
    - Controlled via Policy Agent AT-TLS policies
  - If remote client authentication is used, the listener will be able to extract the associated SAF user ID and pass that to the security exit routine
    - New GETTID option on listener definition
  - A configurable listener user ID will also be implemented to allow more control over which user ID the listener task itself executes under
    - New USERID option on listener definition

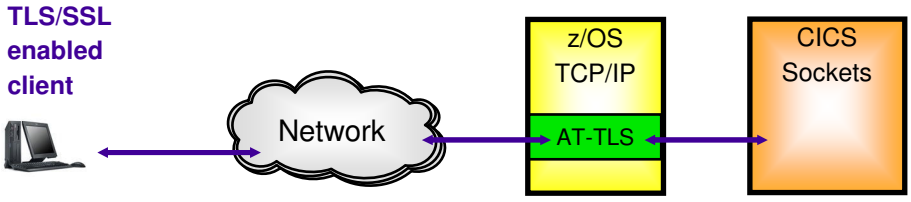
Transparent application security: policy-controlled transparent SSL/TLS support being added in z/OS V1R7



- **Basic TCP/IP stack-based TLS**
  - TLS process performed at TCP layer without requiring any application change (transparent)
  - All connections to specified port are designated as TLS required
    - Can be further qualified by source/destination IP addresses
  - Transparent TLS policies managed via Policy Agent
- **Transparent TLS can be requested by application**
  - Application issues transparent TLS API calls to indicate that connection should start/stop using TLS
- **TCP/IP stack-based TLS with client identification services for application**
  - Application issues TLS API calls to receive user identity information based on X.509 client certificate
- **Available to any TCP application**
  - CICS Sockets is primary focus of this support
    - CICS Sockets listener support for retrieving RACF user ID that is associated with a client digital certificate if client authentication is used
  - All programming languages supported

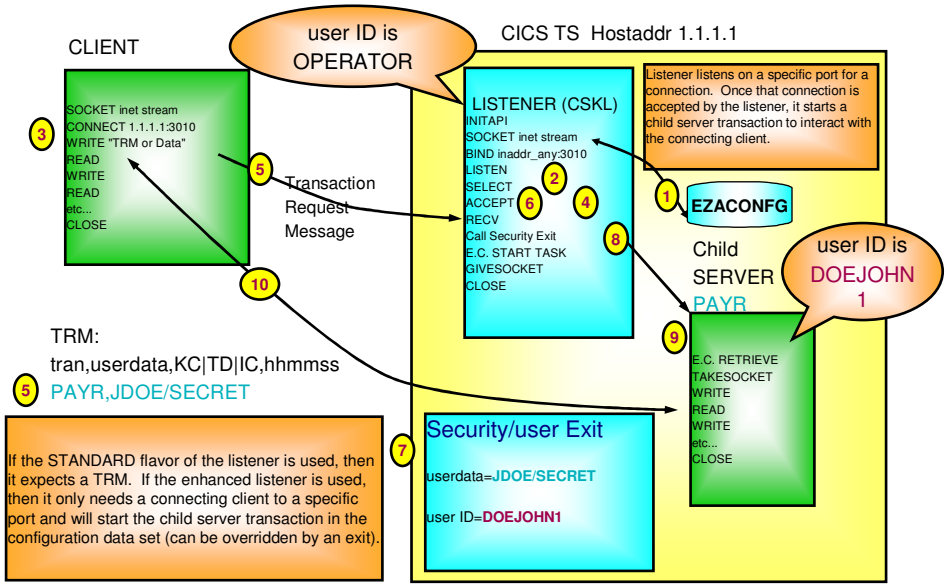
Enable IP CICS Sockets to exploit AT-TLS

- **Enable the IP CICS Sockets Listener, EZACIC02, to obtain the user ID associated with the TLS enabled client's certificate.**
  - We are solving this requirement by exploiting AT-TLS.
  - Two main benefits are
    - Secure Communications
      - Achieved exclusively via the AT-TLS policy support
    - Ability to perform client authentication using digital certificates
      - This support is not completely transparent, since new CICS Sockets features are needed.

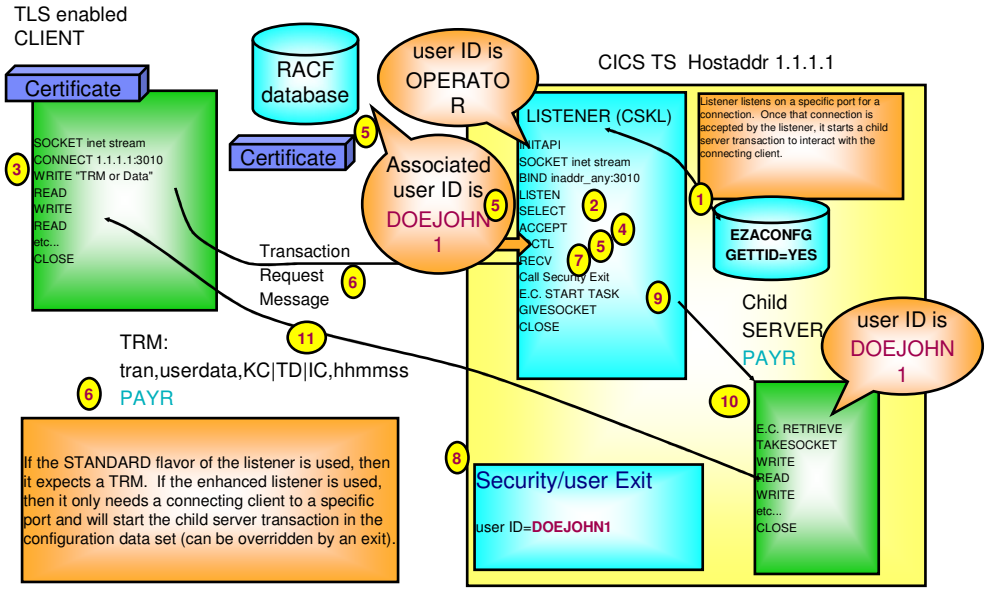


Note: AT-TLS can SSL/TLS-enable your IP CICS Sockets transaction program, it cannot SSL/TLS-enable your remote client (unless the remote client runs on another z/OS V1R7 system)

IP CICS Sockets child server user ID - as it was and still is supported



Associate digital client certificate user ID to CICS Sockets child server in z/OS V1R7 or later



Configure an IP CICS Sockets Listener to get TLS IDs

Part 1 of 2

- **A policy must exist in Policy Agent.**

```
TTLSRule CSKLrule
{
LocalPortRange 3010
Direction Inbound
TTLSGroupActionRef TTLSGRP1
TTLSEnvironmentActionRef TTLSENV1
}
TTLSEnvironmentAction TTLSENV1
{
HandshakeRole ServerWithClientAuth
EnvironmentUserInstance 1
TTLSEnvironmentAdvancedParmsRef
TTLSADV1
}
TTLSEnvironmentAdvancedParms TTLSADV1
{
ClientAuthType SAFcheck
}
TTLSGroupAction TTLSGRP1
{
TTLSEnabled ON
}
```

Configure an IP CICS Sockets Listener to get TLS IDs

Part 2 of 2

- **Enable an IP CICS Sockets Listener to get a user ID from AT-TLS by adding GETTID=YES to the EZACICD TYPE=LISTENER macro. GETTID is supported by both the standard and enhanced flavors of the Listener.**
  - The values for GETTID are NO and YES (NO being the default).
- **If GETTID is YES, the Listener attempts to obtain that user ID.**
- **If the start type is task control (KC) or interval control (IC) and a user ID is successfully obtained, the Listener will use that to initialize the user ID of the child server, unless a security exit overrides it.**
- **If the start type is transient data (TD), any user ID obtained will not be associated with the child server.**
  - Note:
    - The user ID under which the Listener executes must have CICS RACF surrogate authority to any user ID that it uses to initialize the child server.

```
EDIT ---- CFGTLS JCL A1 ------------------------------------------- COLUMNS 001 080
COMMAND ===>                                                      SCROLL ===> CSR
000085 CSKL     EZACICD TYPE=LISTENER,   Create Listener Record              X
000086                  APPLID=CICS1A,     APPLID of CICS                    X
000087                  TRANID=CSKL,       Use standard transaction ID       X
000088                  PORT=3010,         Use port number 3010              X
000089                  AF=INET,           Listener Address Family           X
000090                  GETTID=YES,        Get AT-TLS ID                     X
000091                  BACKLOG=40,        Set backlog value to 40           X
000092                  ACCTIME=999,       Set timeout value to 30 seconds   X
000093                  GIVTIME=999,       Set givesocket timeout to 10 seconds X
000094                  REATIME=999,       Set read timeout to 5 minutes     X
000095                  NUMSOCK=100,       Support 99 concurrent connections X
000096                  MINMSGL=11,        Minimum input message is 4 bytes  X
000097                  IMMED=YES,         Start listener immediately        X
000098                  TRANTRN=YES,      Is TRANUSR=YES conditional?        X
000099                  TRANUSR=YES,      Translate user data?               X
000100                  SECEXIT=CISTSE    Name of security exit program
```

Policy Agent definitions for the Listener

- **A policy must exist in Policy Agent for Listeners specifying GETTID=YES**

AT-TLS definitions:

```
TTLSRule CSKLrule
{
LocalPortRange 3010
Direction Inbound
TTLSGroupActionRef NOTTLSGR
}
TTLSGroupAction NOTTLSGR
{
TTLSEnabled OFF
}

TTLSRule CSKMrule
{
LocalPortRange 3011
Direction Inbound
TTLSGroupActionRef TTLSGRP1
TTLSEnvironmentActionRef TTLSENV1
}
TTLSEnvironmentAction TTLSENV1
{
HandshakeRole ServerWithClientAuth
EnvironmentUserInstance 1
TTLSEnvironmentAdvancedParmsRef TTLSADV1
}
TTLSEnvironmentAdvancedParms TTLSADV1
{
ClientAuthType SAFcheck
}
TTLSGroupAction TTLSGRP1
{
TTLSEnabled ON
}
```

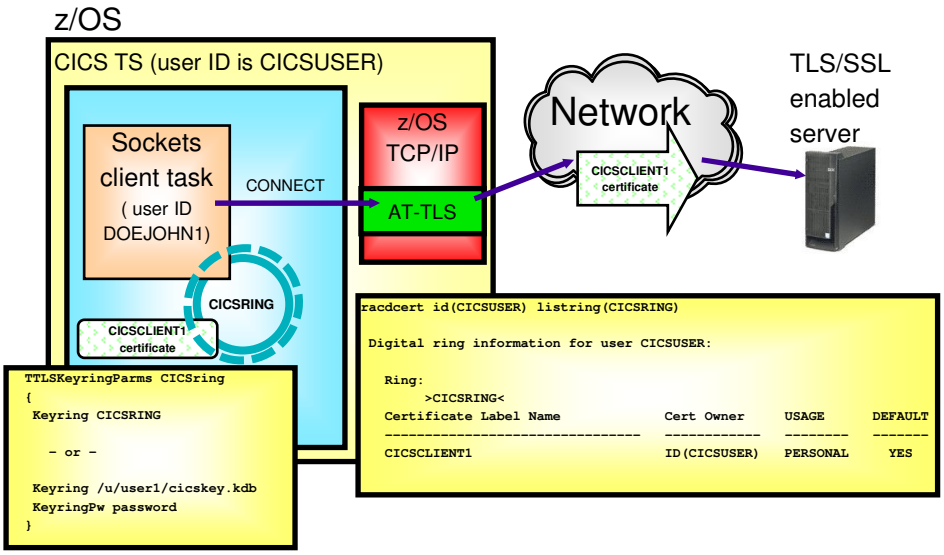
IP CICS Listener configuration:

```
TRANID ===> CSKL
PORT   ===> 03010
GETTID ===> NO

TRANID ===> CSKM
PORT   ===> 03011
GETTID ===> YES
```

Outbound CICS Sockets clients

- **A CICS transaction that is processing as a client must associate its client certificate with the user ID of the CICS region.**



Things to think about

- **The client application must be enabled for TLS or SSL processing.**
- **There are no programming changes for applications wishing to exploit AT-TLS.**
- **Before changing GETTID to YES, you should do the following:**
  - Set the TTLS parameter in TCPCONFIG.
  - Work with the security administrator to ensure RACF contains the elements needed to support AT-TLS.
  - Ensure the required POLICY exists in Policy Agent to support the Listener and any outbound clients.

Trademarks, Copyrights and Disclaimers