



Software Group | Enterprise Networking and Transformation Solutions (ENTS)

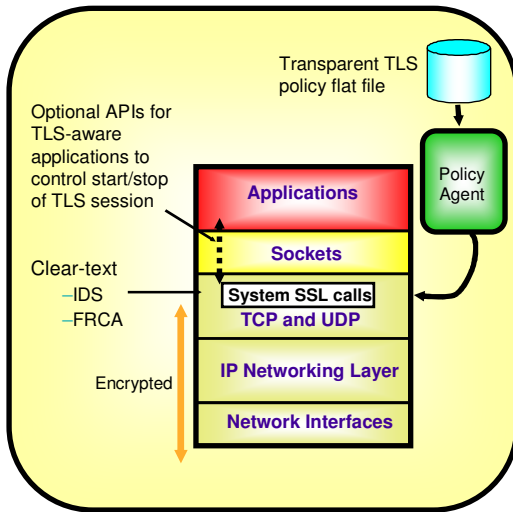
# CS z/OS CICS Sockets SSL/TLS enabling

## 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

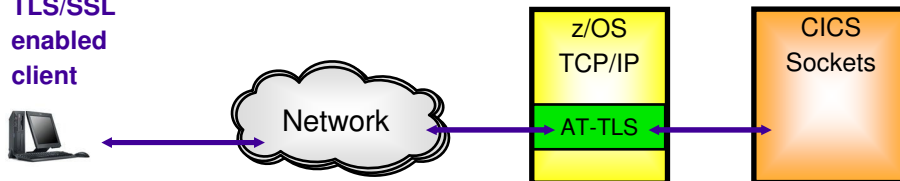
– Secure Communications

• Achieved exclusively via the AT-TLS policy support

– Ability to perform client authentication using digital certificates

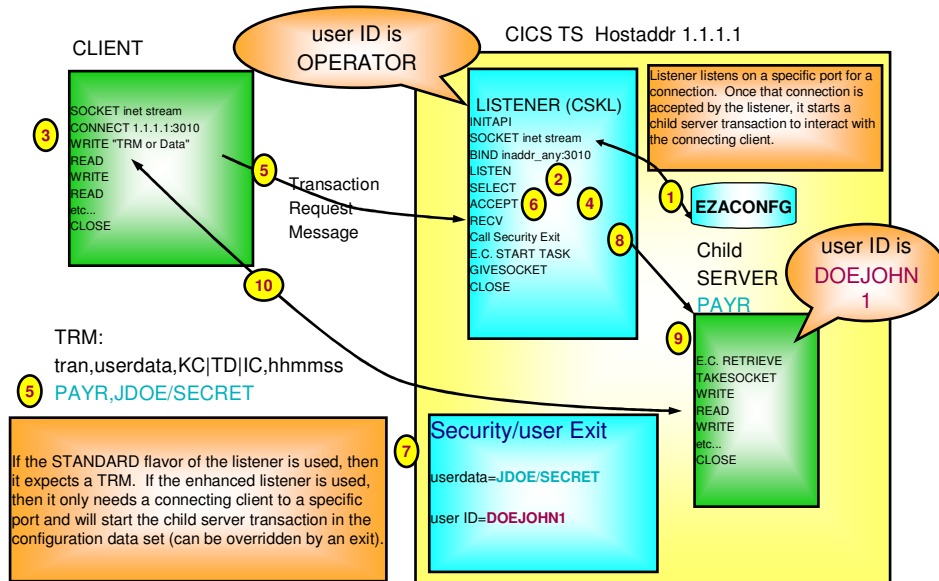
• This support is not completely transparent, since new CICS Sockets features are needed.

**TLS/SSL  
enabled  
client**



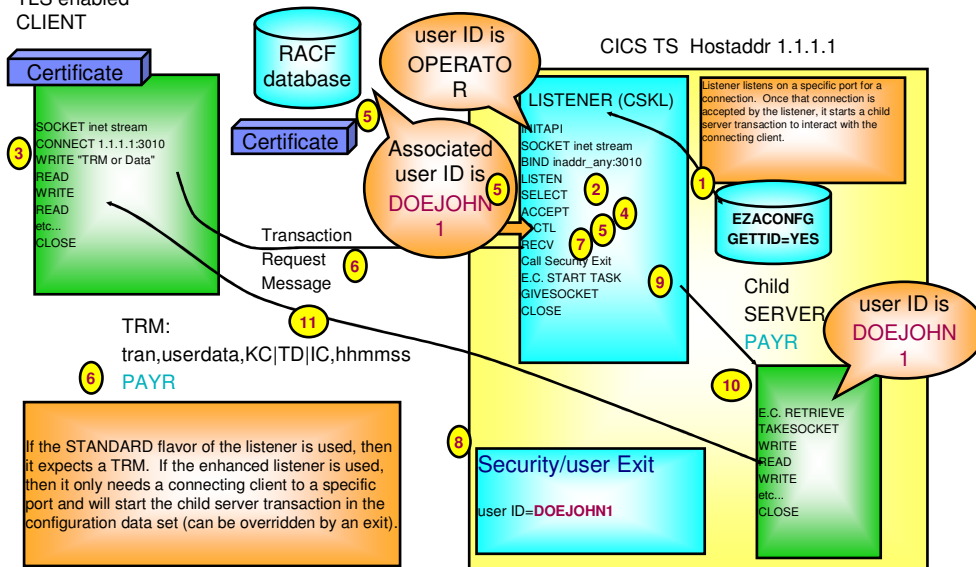
**Note: AT-TLS can SSL/TLS-enable your IP CICS Sockets transaction program, it cannot SSL/TLS-enable your remote client (unless the remote client runs on another z/OS V1R7 system)**

## 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

TLS enabled CLIENT



## Configure an IP CICS Sockets Listener to get TLS IDs

### Part 1 of 2

➤ A policy must exist in Policy Agent.

```
TTLSRule CSKRule
{
  LocalPortRange 3010
  Direction Inbound
  TLSGroupActionRef 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          MINMSG=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
  
```



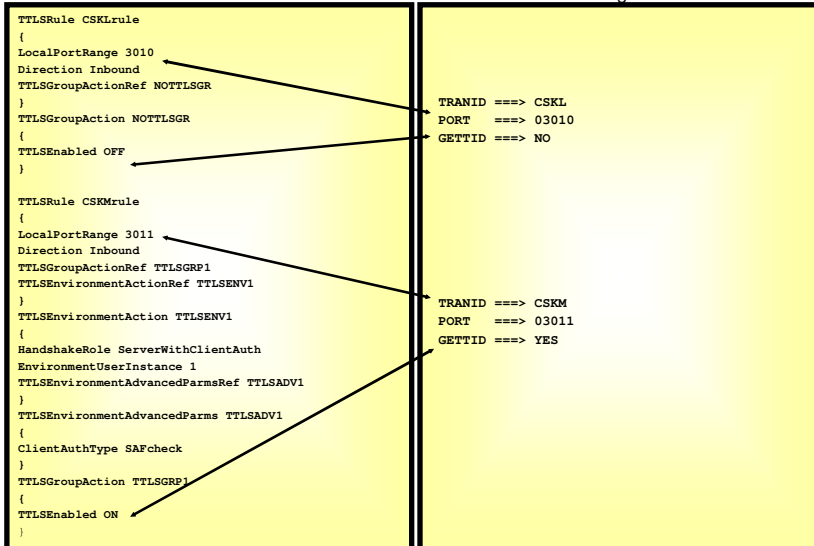


## Policy Agent definitions for the Listener

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

AT-TLS definitions:

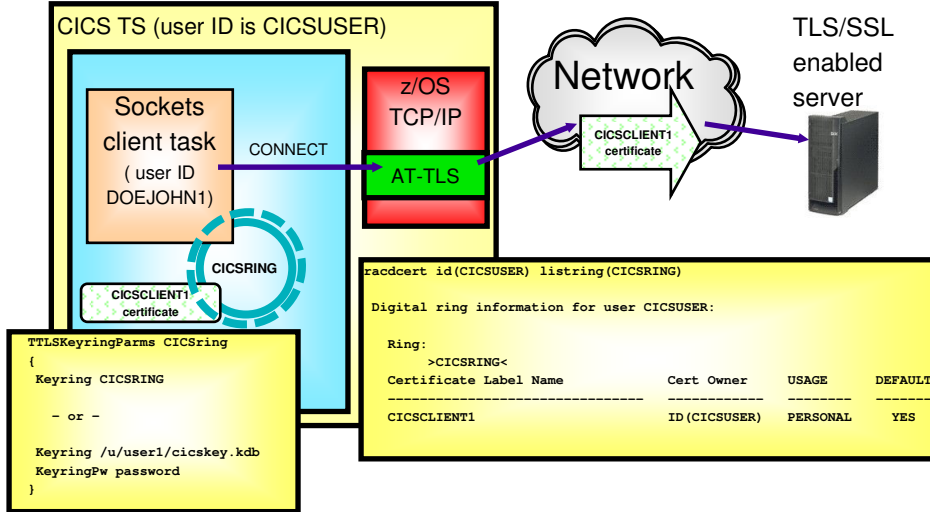
IP CICS Listener configuration:



## 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.

z/OS



## 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

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

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

© Copyright International Business Machines Corporation 2005. All rights reserved.

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.