IBM Software Group

Security Design Considerations

TXSeries Integrated with CICS Transaction Server

TXSeries V7.1 for Multiplatforms
The Next Generation of Distributed CICS
www.ibm.com/CICS

Contents

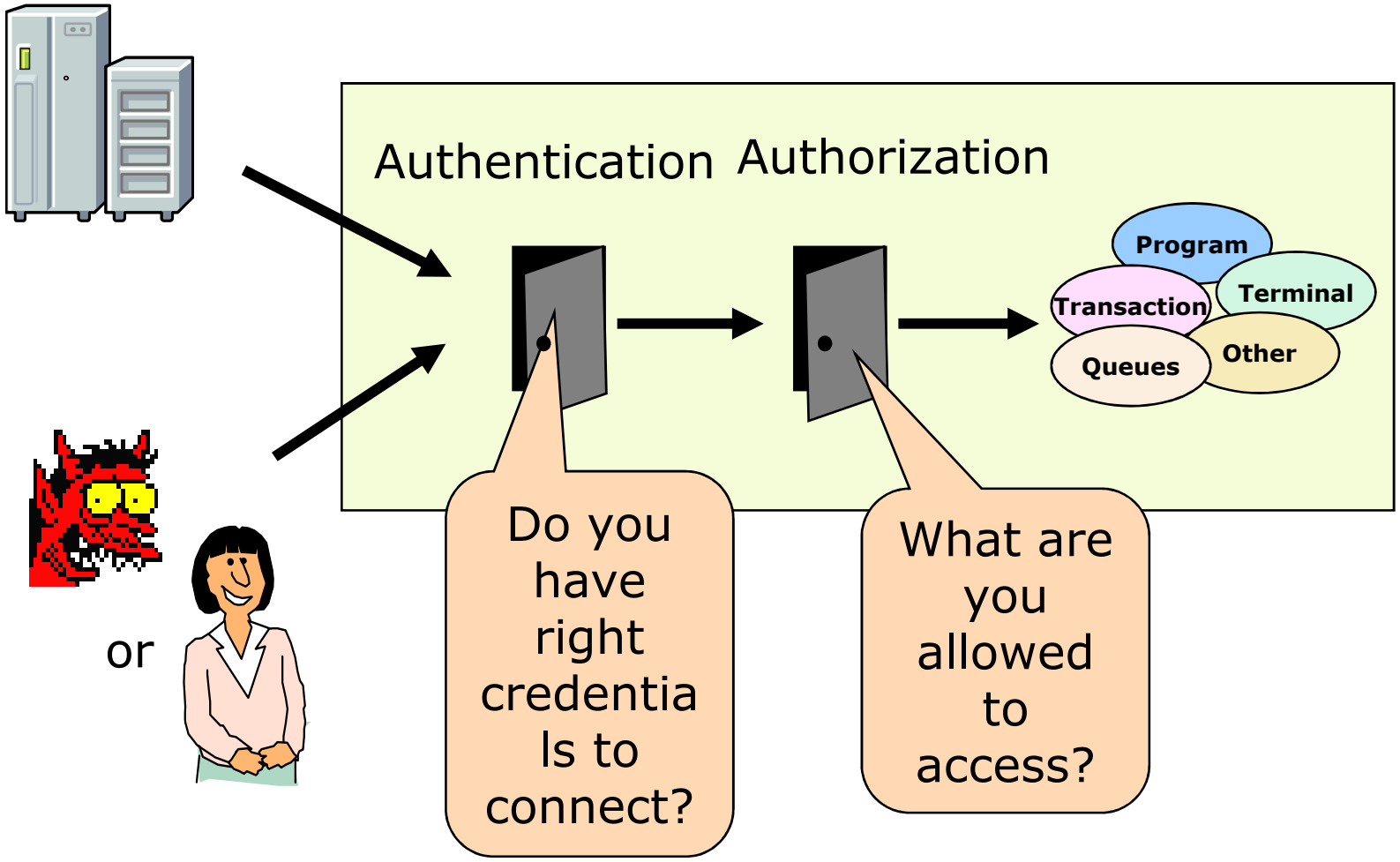
Security

- **Protection of Infrastructure ,System and Data**
- **What users are allowed to access? what they are permitted to?**
- **What other systems are allowed to access?**
- **Is data passed through wire is secure?**

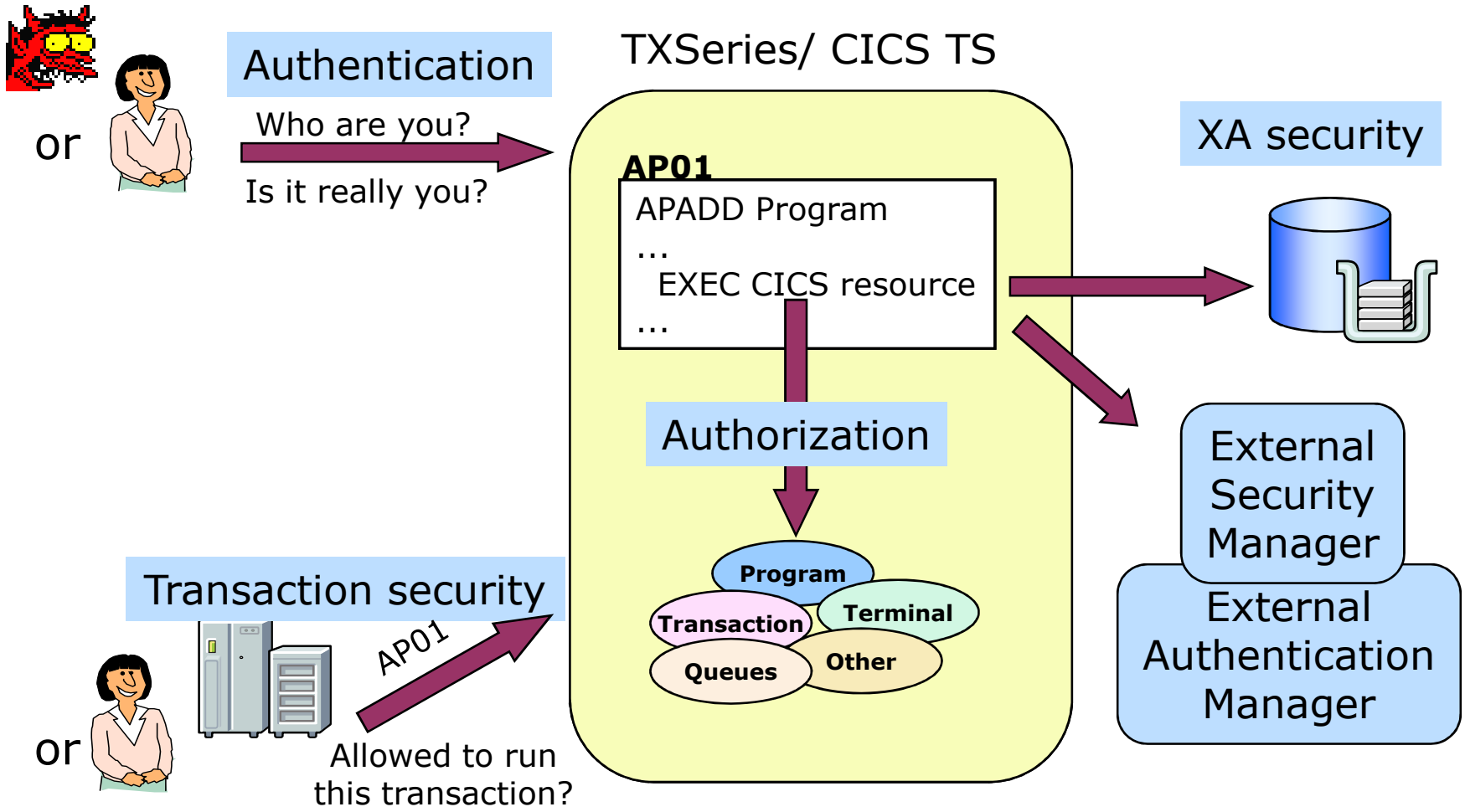
Security Aspects

- **Local Security**
  - **Authentication**
  - **Authorization**
- **Intersystem Security**
  - **Connection Security**
  - **Secure Communications**

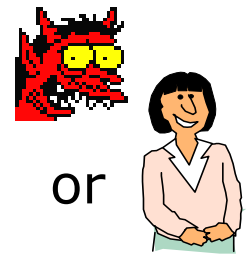
Security in TXSeries CICS Environment



Security in TXSeries CICS Environment



Security in TXSeries CICS Environment



or

Authentication

Who are you?
I am **JANE**

Is it really you?
jane_password

USERID

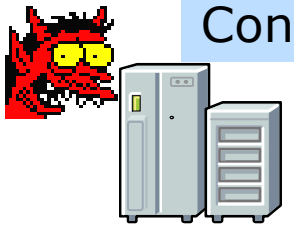
USERID and PASSWORD

TXSeries

NICE can connect as we share the same secret bind key with this server

JANE has authenticated

CICS is ready to accept transactions requests



Connection security

Allowed to connect?

trusted_bind_key

BIND KEY

I am a **NICE** server

User Definition

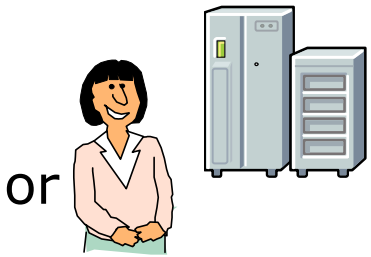
userA	password
userB	password
default	password
JANE	jane_password

Communications Product

Partner	bind_key

Security in TXSeries CICS Environment

Authorization for Transaction



or

Allowed to run this transaction?

AP01

JANE has authenticated

Is **JANE** allowed to run this transaction?

Security manager say YES

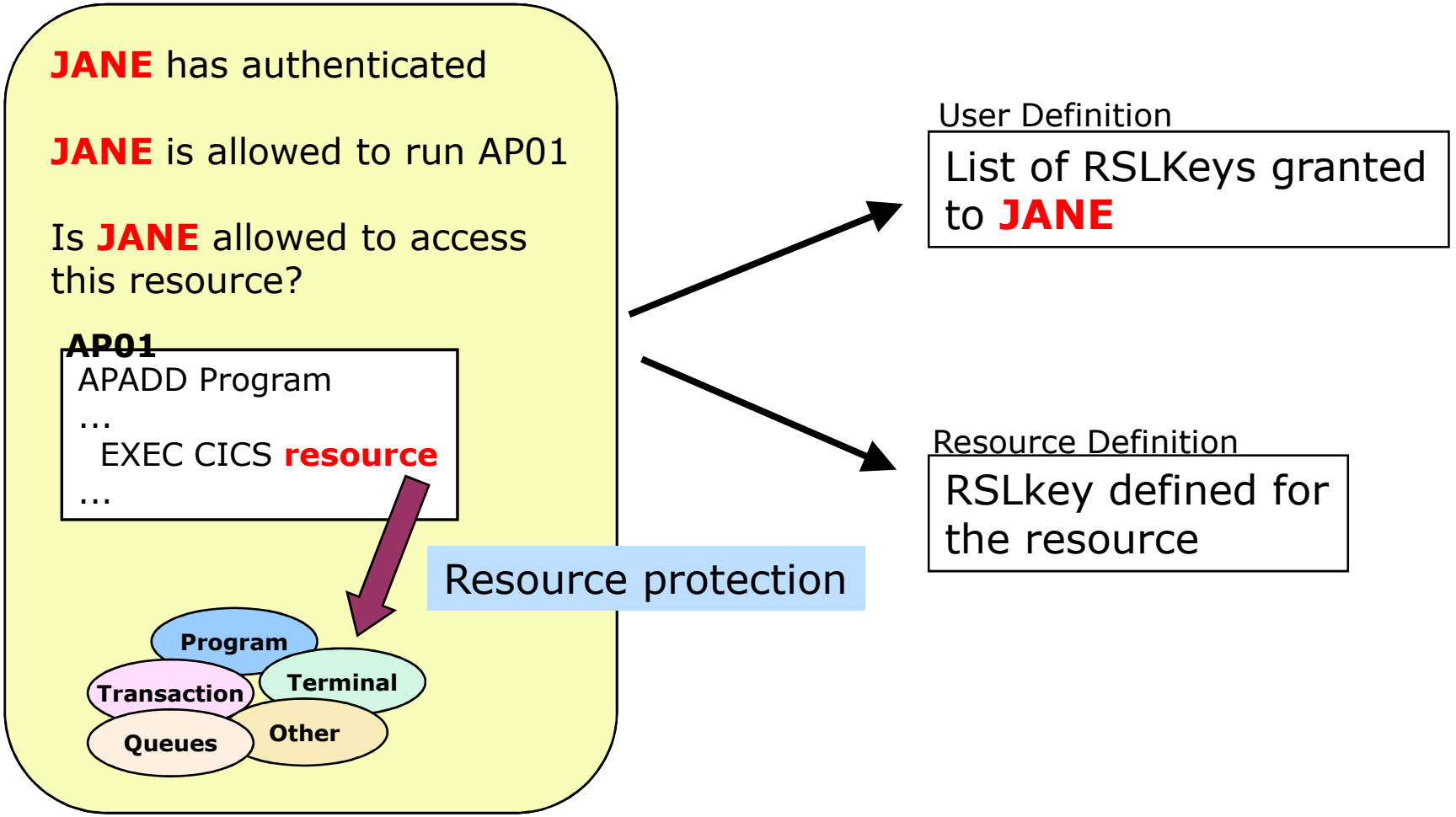
Transaction Definition

TSLkey defined for the **AP01** transaction

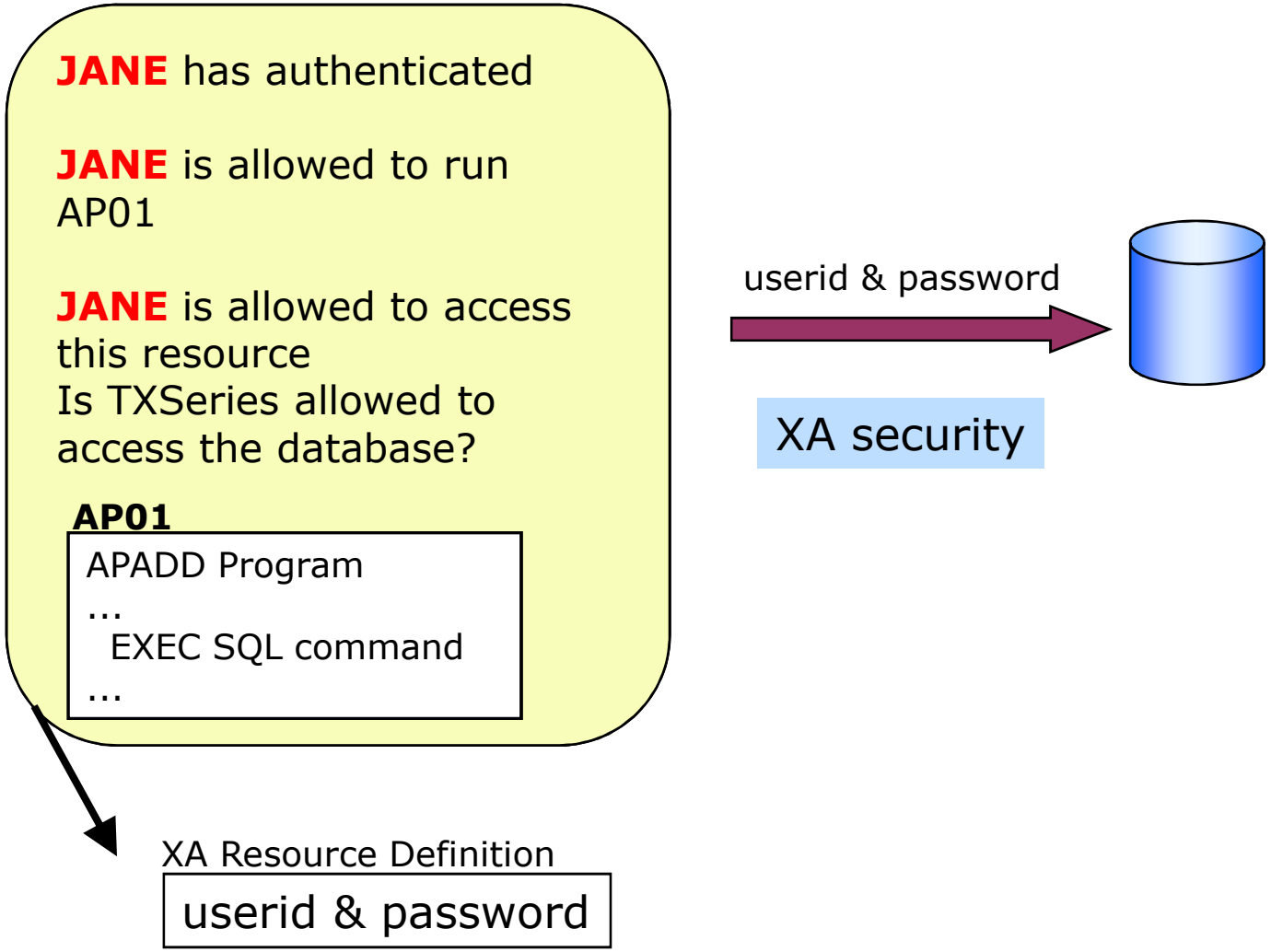
User Definition

List of TSLKeys granted to **JANE**

Security in TXSeries CICS Environment

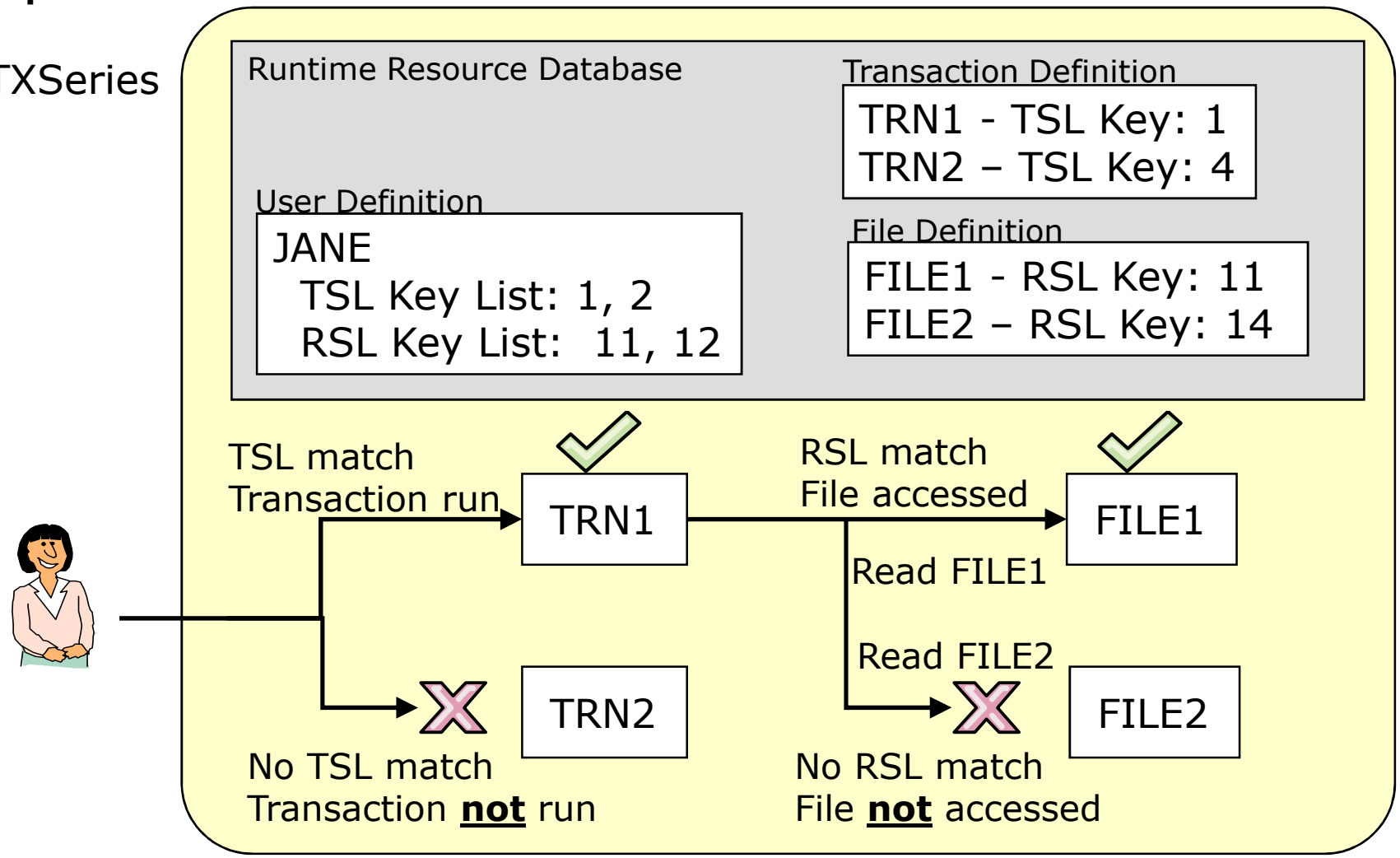


Security in TXSeries CICS Environment



Security in TXSeries CICS Environment

Example



Security in TXSeries CICS Environment

Security with CICS Clients

CICS Transaction Gateway
and CICS Universal Client

USERID
and
PASSWORD

Client system not trusted

JANE must authenticated

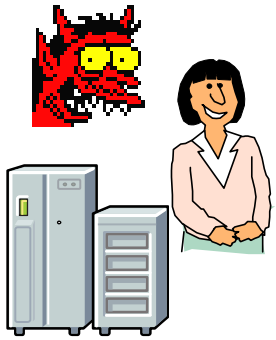
CICS is ready to accept transactions requests

User Definition

userA	password
userB	password
default	password
JANE	jane_password

Security in TXSeries CICS Environment

External security managers

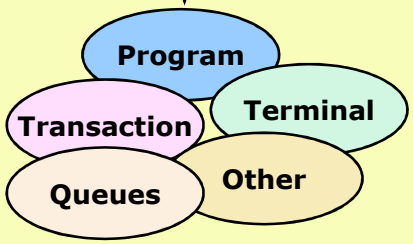


TXSeries

Authentication

Transaction security

Resource protection



External Authentication Manager

External Security Manager

Region Definition

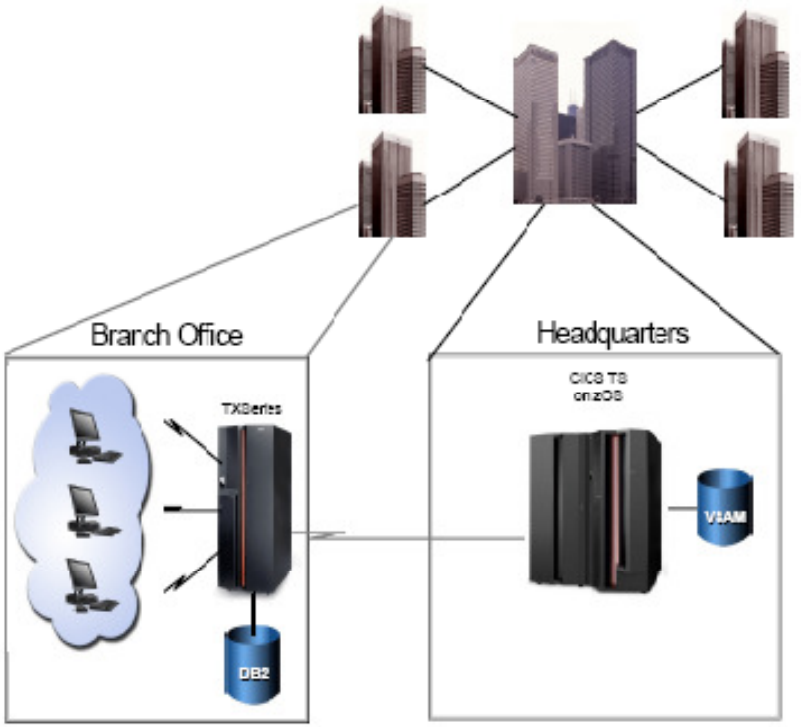
```
EAMLoad=yes
EAMModule

ESMLoad=no
ESMModule
RSLCheck=external
```

Transaction Definition

```
TSLCheck=external
RSLCheck=external
```

What is Inter System Communication ?

- **In a heterogeneous environment , TXSeries CICS (CICS on Open Systems and CICS for Windows NT) region can communicate with other systems to**
  - Provide users of the local region with services that are held on remote system
  - Provide users on remote system with the services that are held on the local region
- **The communication between the interconnected**
- **systems is referred to as *inter system communication*.**



Supported Network communication Protocols

NETWORK PROTOCOLS

SNA Network protocol

TCP/IP Network protocol

SNA Network

TXSeries CICS supports intercommunication across an SNA network between a local region and the

- Other TXSeries CICS regions
- Other CICS products such as CICS/ESA, CICS/MVS, CICS/VSE, CICS OS/2, and CICS/400 regions
- CICS on Open Systems clients and IBM CICS Universal Clients
- Applications on systems that support the SNA LU 6.2 protocol

Communication Methods

- Local SNA
  - Communication between TXSeries Systems and CICS TS on Z/OS
- PPC GATEWAY
  - Communication between TXSeries Systems and other TXSeries Systems over SNA with Synclevel 2

Supported Network communication Protocols

TCP/IP Network

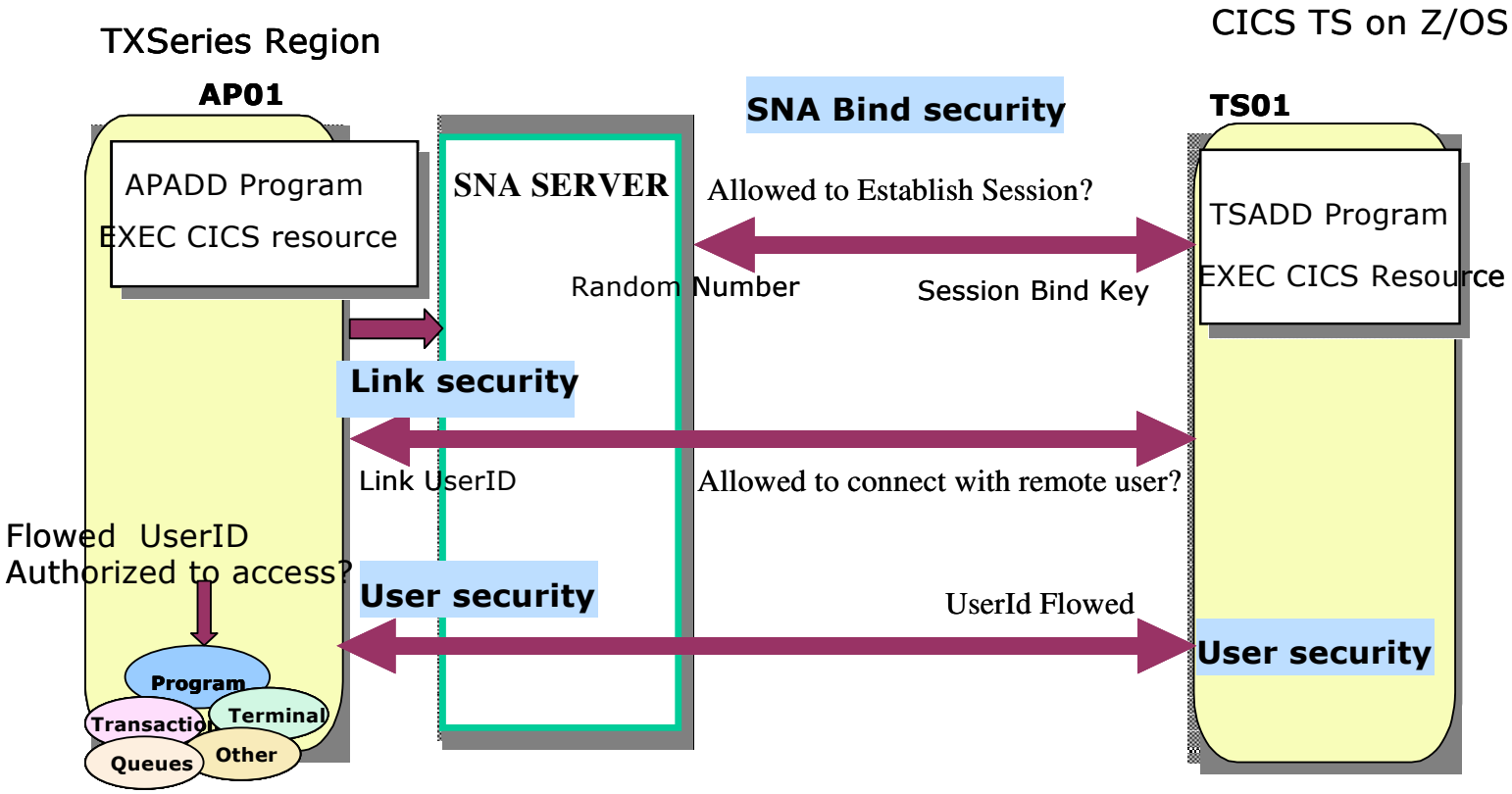
This allows a local region to communicate with

- Other TXSeries CICS regions using IP.
- CICS OS/2 regions
- IBM CICS Universal Clients
- CICS/Encina Peer-to-Peer Communications (PPC/TCP)-based applications

Communication Methods

- CICS TCP
  - Communication between TXSeries Systems and other TXSeries Systems over IP
- IPIC (IP InterConnectivity)
  - Communication between TXSeries Systems and CICS TS on Z/OS over IP
  - Communication between TXSeries Systems and other TXSeries Systems over IP
- PPC TCP
  - Communication between TXSeries Systems and other TXSeries Systems over IP with Synclevel 2

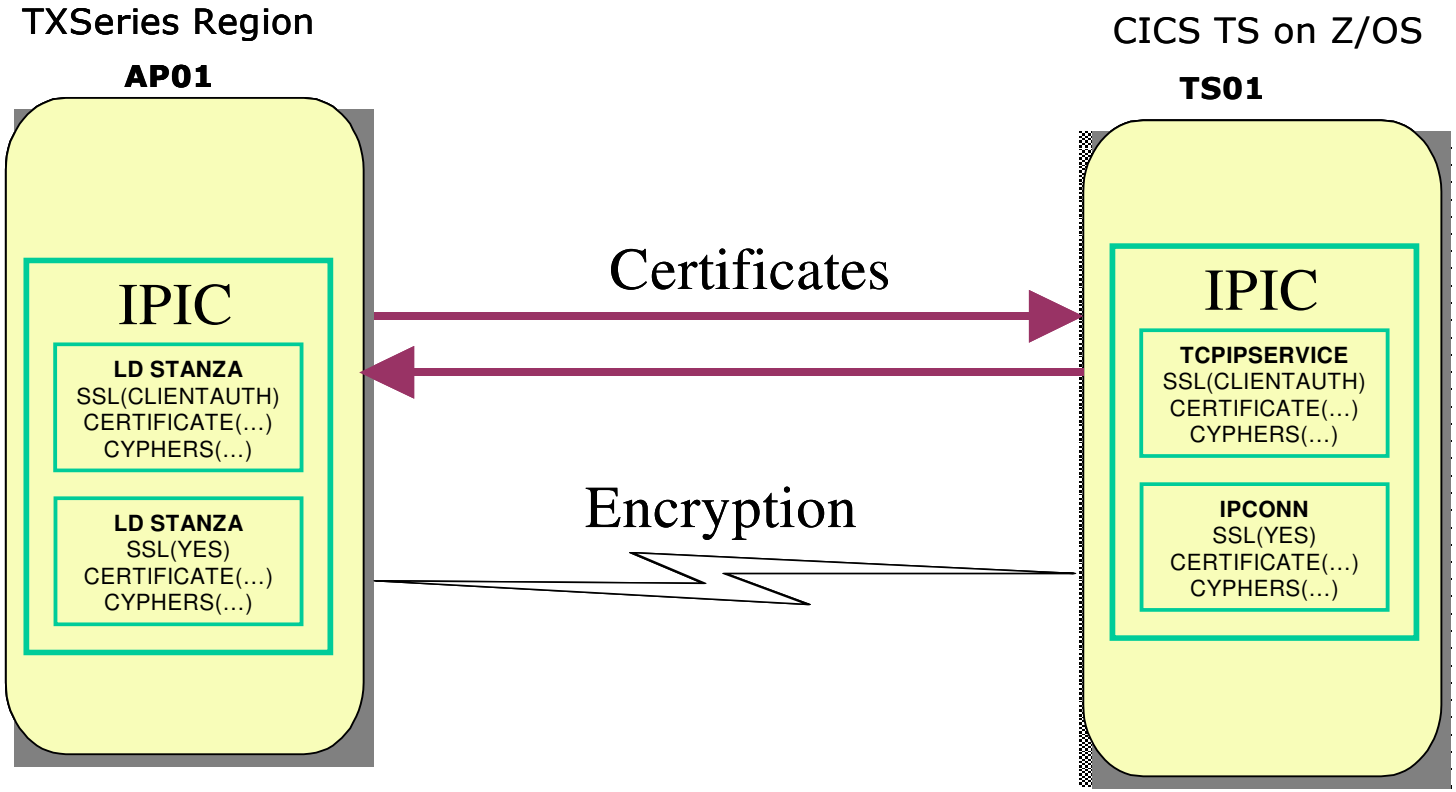
Intersystem/Connection Security



- **For Bind Security ,Bind passwords are set up in the SNA productthat is managing SNA connectivity.**

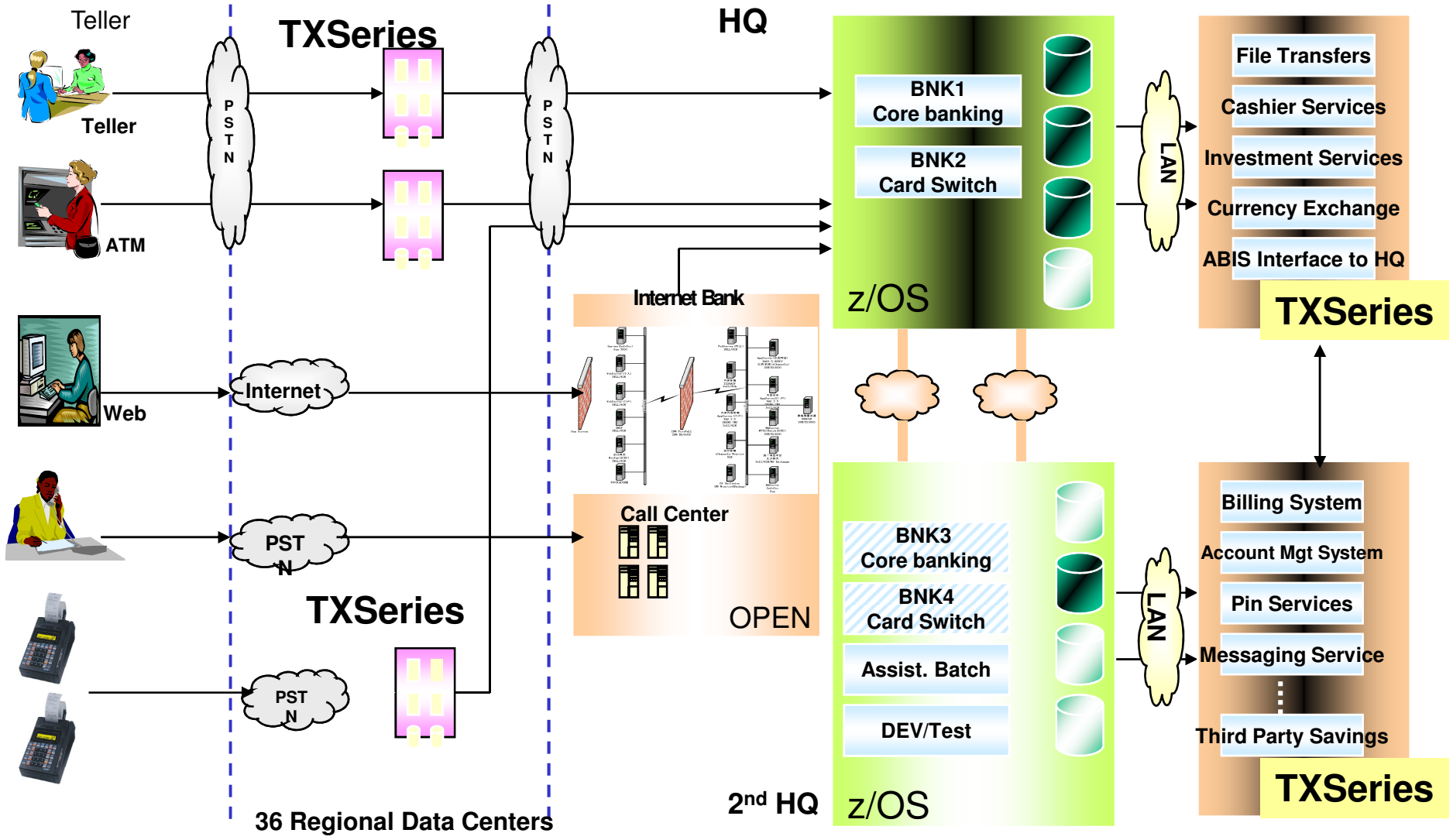
- **For Link Security ,Link UserID are set up in the respective regions authenticate and authorize for the inbound requests.**

Secure Communications

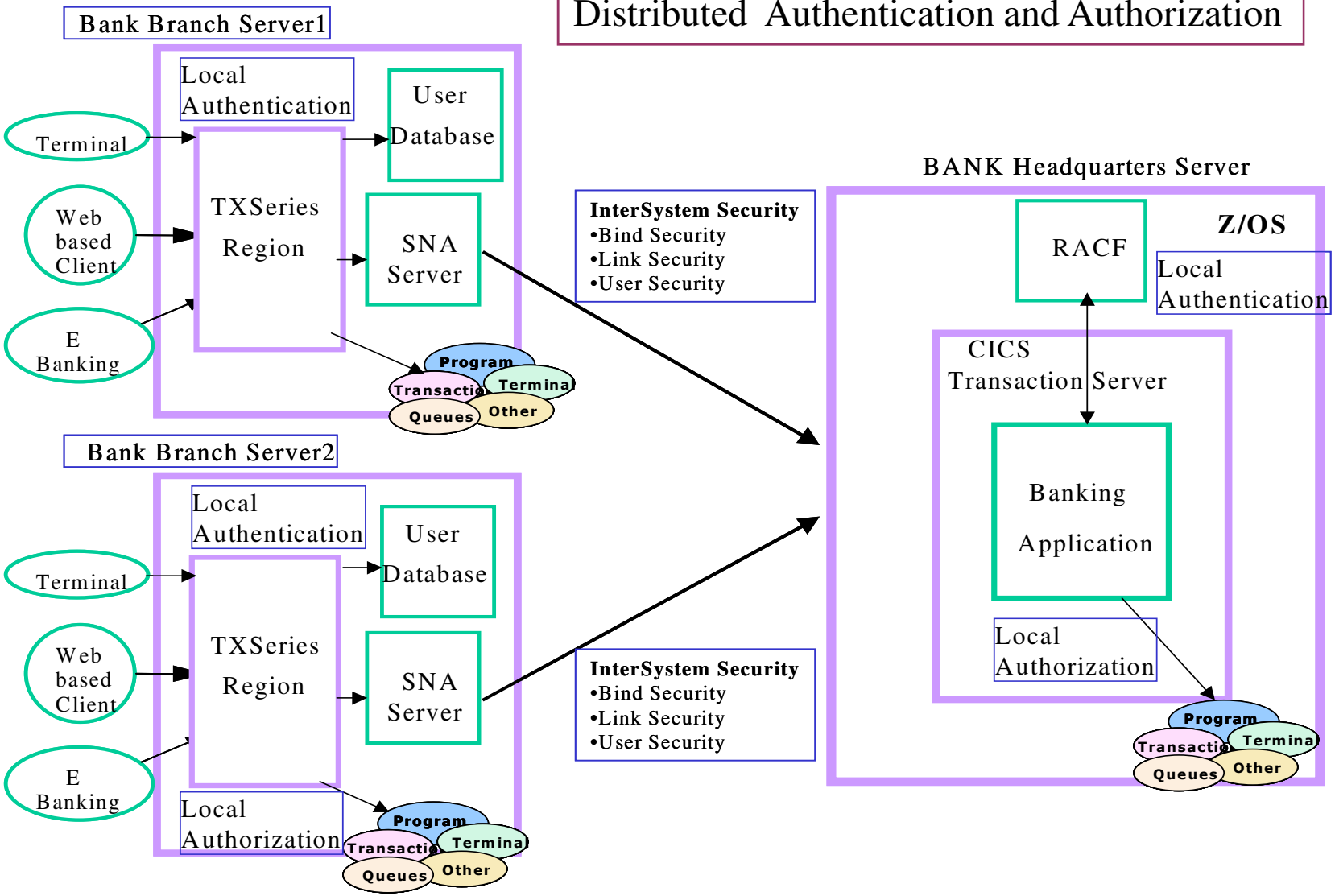


IPIC – IP InterConnectivity

Typical ISC Business Scenario



Distributed Authentication and Authorization



Distributed Authentication and Authorization

Security features

User credentials are managed locally by the respective branch and headquarter server.

security aspects Provided between TXSeries and CICS TS

Authentication

Authorization

Link security,

SNA bind security

User security

Distributed Authentication and Authorization

Pros

- Security checks provide minimal overhead on the overall performance of the transaction

  Authentication and Authorization are performed locally on the branches

Branches had flexibility to define security for their own applications

Distirbuted Authentication and Authorization

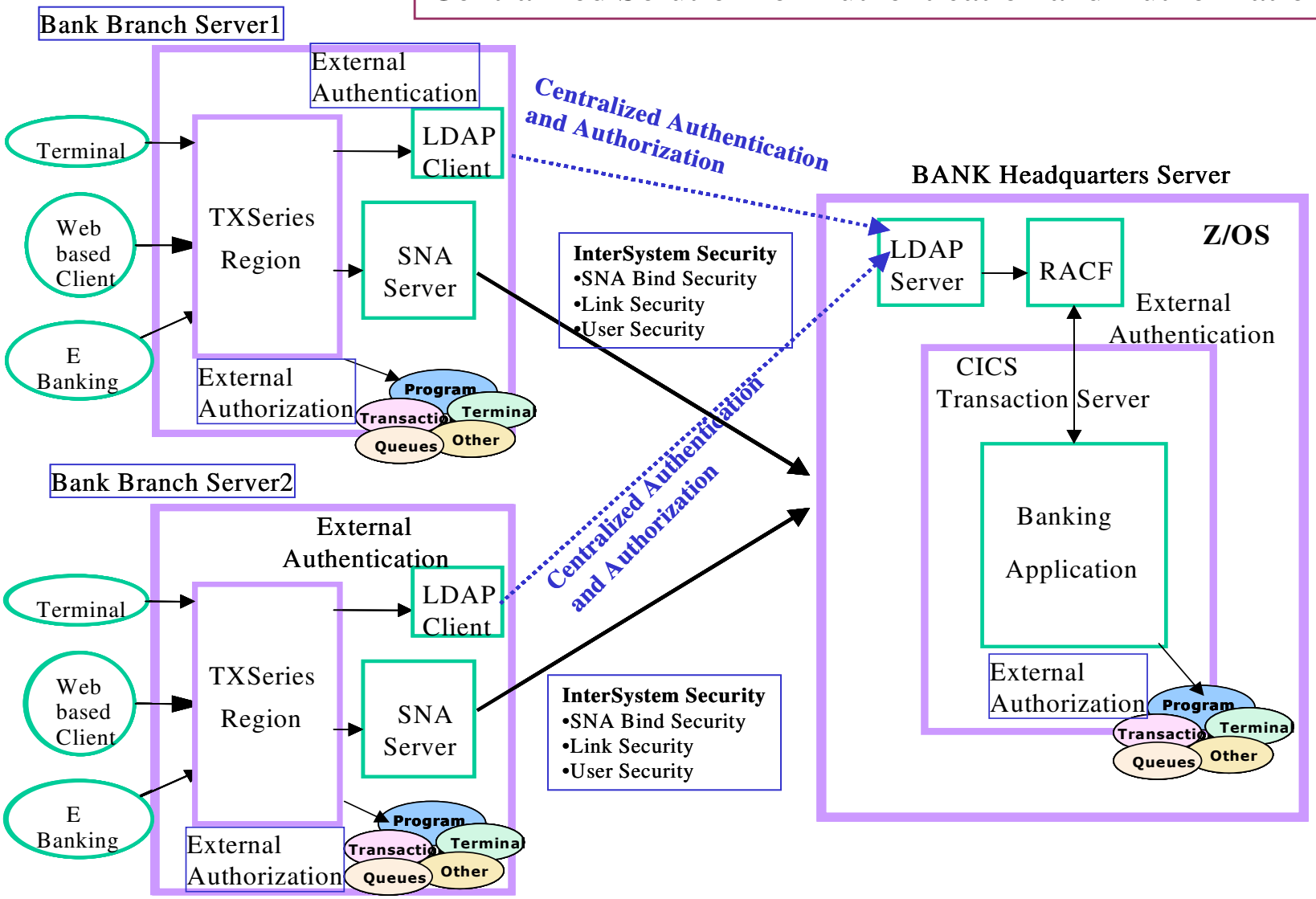
Cons

- User security is distributed and not consolidated

  leads to multiple user checks across systems for the same user application requests.

- Administration of user credentials are performed at each and every bank branch. It adds to overall administrative overhead on the system security

Centralized Solution for Authentication and Authorization



Centralized Authentication and Authorization

Security features

- Provides centralized authentication and authorization through LDAP and RACF.
  - ❖ To store user credentials for authentication and authorization in a centralized RACF (Remote Access Control Facility)
- User credentials are kept in RACF,
  - ❖ Branch-based TXSeries servers and the Headquarters server can access same database to fetch the user credentials.

Centralized Authentication and Authorization

Pros

- Ensures that transactions (business applications) spawned across Regions(CICS TS and TXSeries) are accessed with the same user credentials.

- Administration of security credentials are performed at single place, hence maintenance overhead is reduced drastically with this architecture

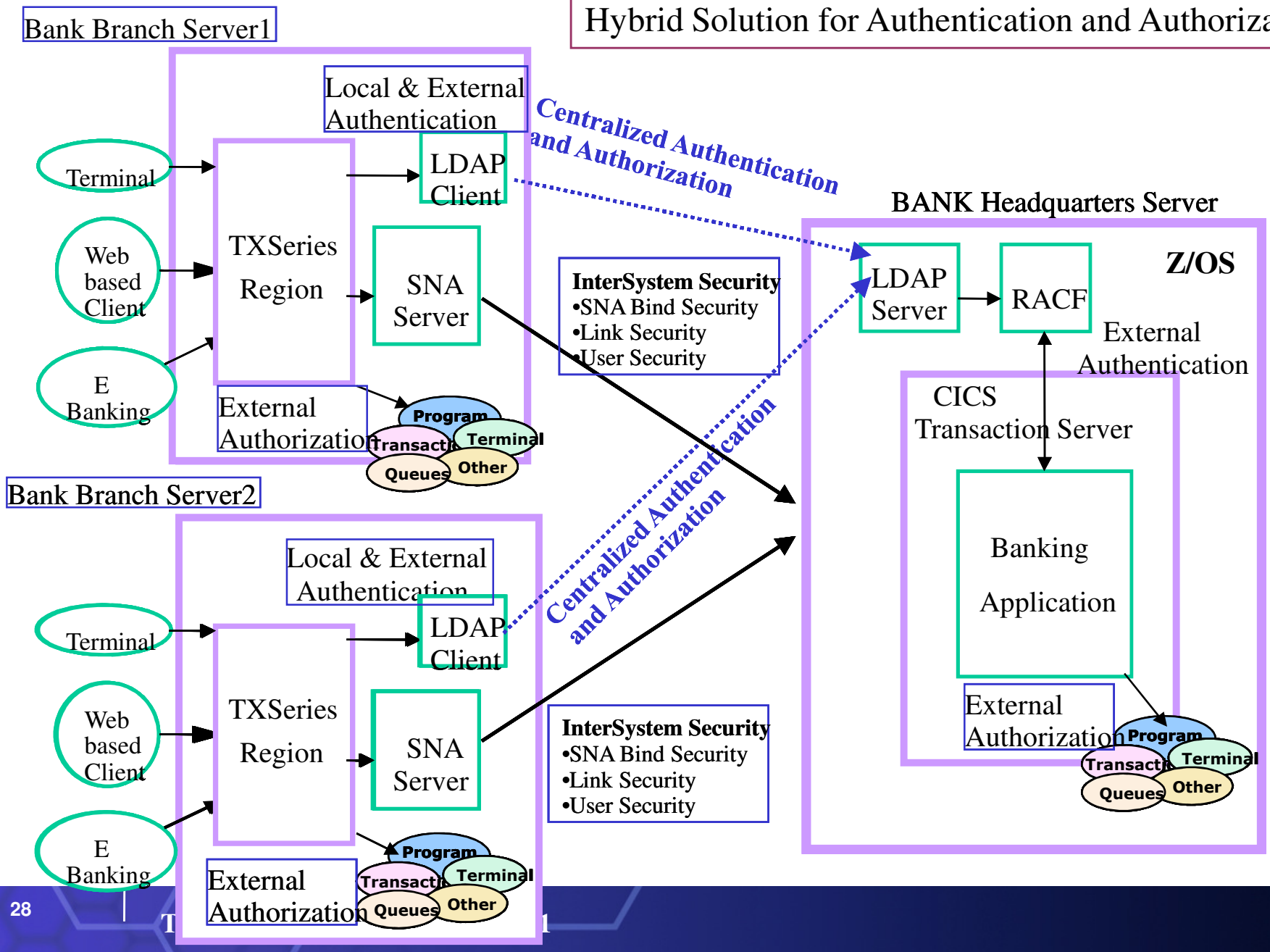
- Provides a clear view of security credentials across branch servers

Centralized Authentication and Authorization

Cons

- Adds a little security check overhead in the transaction performance, as each time the user credential check has to reach headquarters centralized server for validation.
- Faster and Reliable network between the systems can reduce the overhead.
- Even for Branch based Local applications, the security check is sent to centralized RACF server.

Hybrid Solution for Authentication and Authorization



Hybrid Solution for Authentication and Authorization

Security Features

- This architecture uses same security features as previous
- Hybrid solution makes the authentication manager requests to be intelligently routed to local and external authentication manager based on requests

Hybrid Solution for Authentication and Authorization

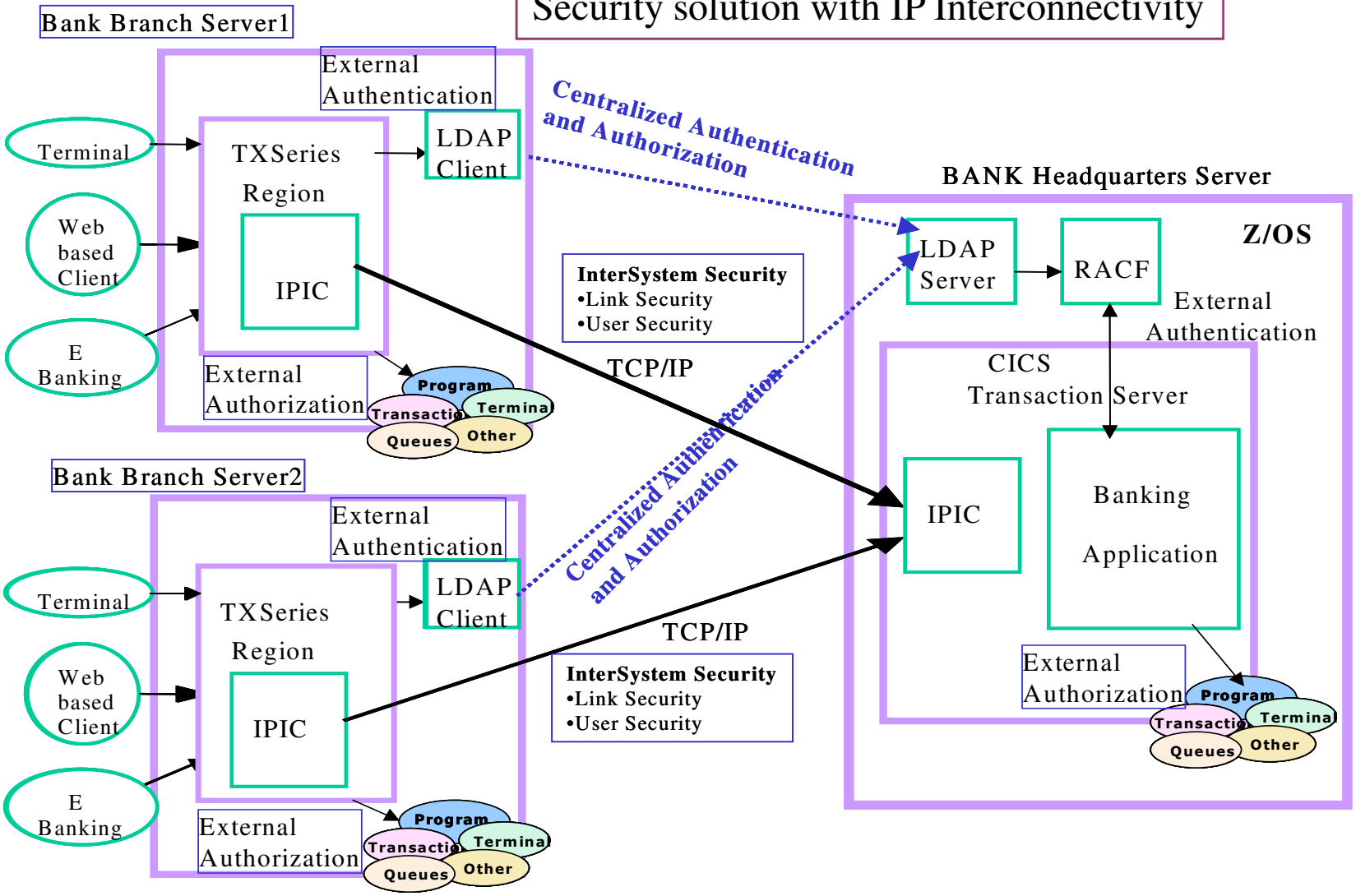
Pros

- Specific Bank Branch applications gets authenticated locally

- Reduces the performance overhead on the local branch requests security checks.

- Application requests spawning across branch and headquarter will be authenticated still using centralized solution.

Security solution with IP Interconnectivity



Centralized Security Solution with IP Interconnectivity

Security Features

- This architecture uses IP interconnectivity protocol, which gives flexibility to use the IP-based security mechanism.

- SNA-equivalent bind security is not provided in this architecture.

- Other than bind security, this architecture provides all the other needed security aspects.

Centralized Security Solution with IP Interconnectivity

Pros

- SNA server is not required in this configuration, because the communications happen through IP.

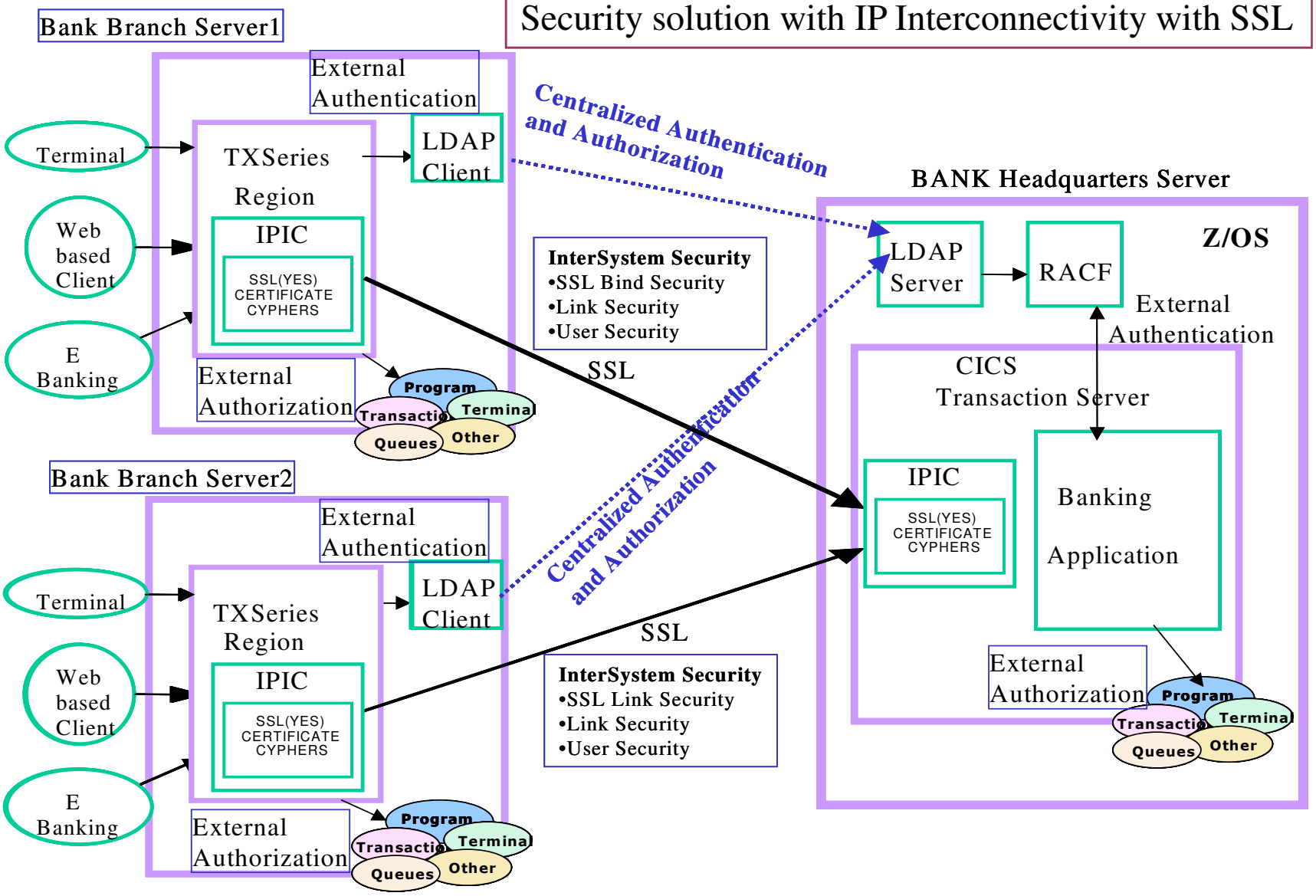
- Securities provided by TCP/IP networks can be used.

Centralized Security Solution with IP Interconnectivity

Cons

- IP based connectivity without SSL has more security threat ,since connection is not secure across regions

Security solution with IP Interconnectivity with SSL



Centralized Security Solution using IP Interconnectivity with SSL

Security Features

- To configure branch and headquarter systems to use SSL for communication, you set the IPCONN and TCPIPSERVICE SSL attributes.

- Uses digital certificates for key exchange, server authentication, and optionally, client authentication.

- Provides bind Security

- During session establishment, the SSL handshake is performed, which produces the cryptographic attributes to be used for data encryption between the partner systems.

- When the session is established between partner systems, all the data that flows over the wire is first encrypted using cryptographic attributes, and then sent. The other end decrypts the received data before use.

Centralized Security Solution using IP Interconnectivity with SSL

Pros

- Data passed across network is secured with data encryption and ssl authentication mechanism

Cons

- Every communication between partner region systems is encrypted and decrypted(SSL) over the network, adds little performance overhead to the business transaction.

Summary

- Security is a very important aspect to understand when designing business-critical applications.
- importance of security and different security aspects provided by CICS TS and TXSeries.
- Also discussed the security considerations when designing the business applications that integrate CICS TS and TXSeries.
- Seen real-world bank business application architecture scenarios.
- Can Take it as guidance on providing security consideration for designing business architecture for real-world, enterprise business applications.

References

- CICS Transaction Server 4.1 Information Center

- TXSeries 7.1 Information Center

THANK YOU