SHARE in Orlando 2015

IMS and Integration Security

Share Session 17759

Suzie Wendler (wendler@us.ibm.com)
Consulting I/T Specialist
IBM

*

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.

The Evolution

- The 4 pillars of the new computing environment

- Benefits
  - Cost savings
  - Rapid procurement and deployment
  - Support for new technologies
  - Scalability, performance, flexibility

Mobile

Cloud

Social

BIG DATA

Embedded Intelligence

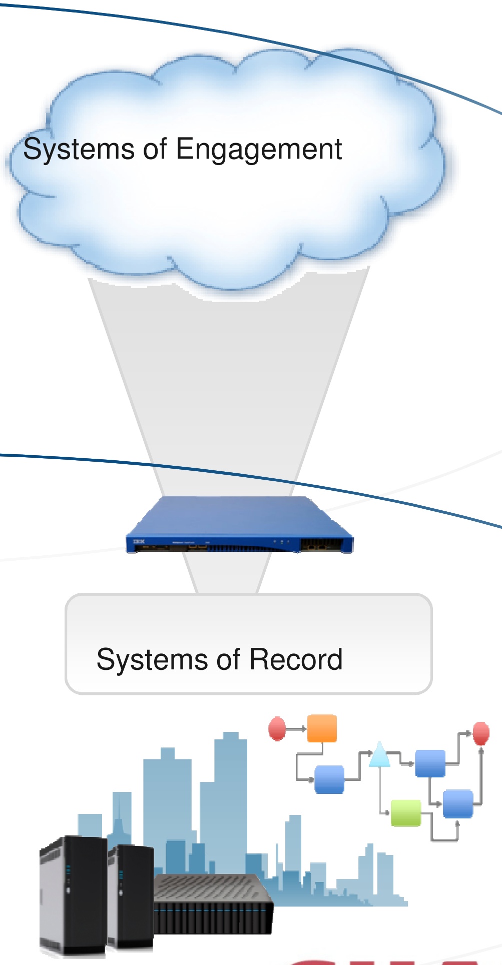
- Challenge
  - Greater need for due diligence, compliance, and sec
    - The “notorious nine” threats: (2013 Cloud Computi
      - Data breaches
      - Data loss
      - Account Hijacking
      - Insecure APIs
      - Denial of Services
      - Malicious insiders
      - Abuse of cloud services
      - Insufficient due diligence
      - Shared technology issue

Security Goal:

To be faster than the speed of threat

So the need includes

- Two levels of protection
  - Defined policies, due diligence
  - Automated monitoring and auditing
  - Software
    - E.g., IBM Qradar, zSecure, Guardium …
  - Appliances, e.g., Datapower
  - User identity mechanisms
    - Userid, certificates, tokens…
  - Protection of resource access
    - RACF, ACF2, Top Secret…



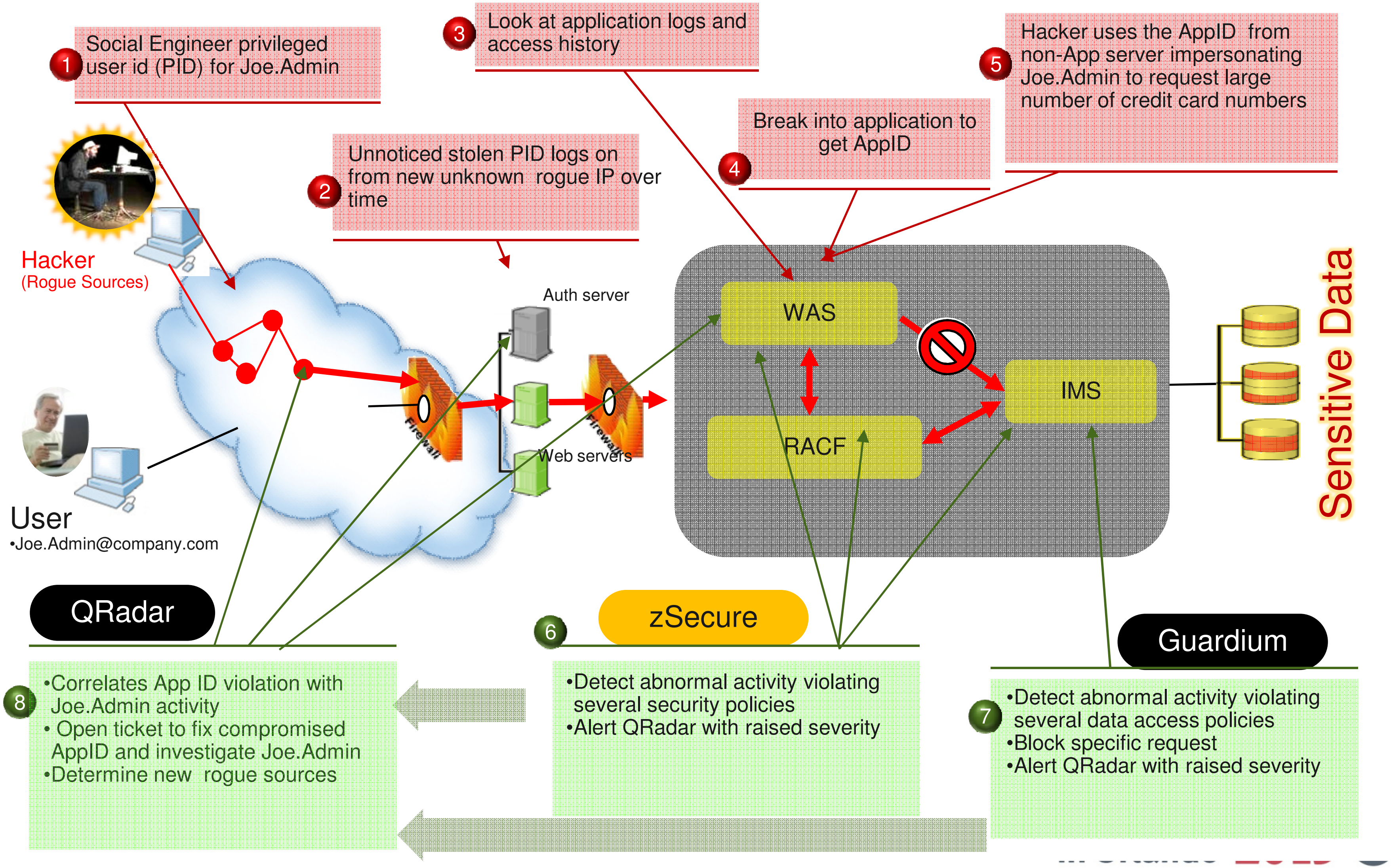
Systems of Engagement

Systems of Record

Solutions

- IBM **Qradar** Security Intelligence Platform products
  - Provide a unified architecture for integrating security information and event management (SIEM), log management, anomaly detection, incident forensics and configuration and vulnerability management
    - And for system z:
      - Extends Enterprise security monitoring to System z to provide a single view into the security posture of the **total environment**
    - http://tinyurl.com/pq57kex **(Integrating IMS with Qradar)**
      - The IMS DSM (device support module) for QRadar allows event collection and auditing of IMS database transactions .
      - To integrate IBM IMS events with QRadar, you must download scripts that allow IBM IMS events to be written to a log file.
- IBM Security **zSecure** solutions
  - Provide comprehensive, end-to-end security across System z platforms that can also interoperate with distributed security solutions to:
    - Automate the time consuming and complex tasks of creating and maintaining User **Accounts and Access Permissions within RACF for System z**
    - Provide real-time and point-in-time monitoring of **security events in z/OS** and major **sub-systems**
    - Create pre-configured and customizable compliance reports to address external regulatory requirements and internal management controls
    - http://tinyurl.com/p72kutg **(zSecure 2.1 support for IMS 13)**
- InfoSphere **Guardium**
  - Provides a simple, robust solution for data security and data privacy
    - Assures the integrity of trusted information in the data center and reduces costs by automating the entire compliance auditing process across heterogeneous environments.

First Level



1 Social Engineer privileged user id (PID) for Joe.Admin

2 Unnoticed stolen PID logs on from new unknown rogue IP over time

3 Look at application logs and access history

4 Break into application to get AppID

5 Hacker uses the AppID from non-App server impersonating Joe.Admin to request large number of credit card numbers

User
•Joe.Admin@company.com

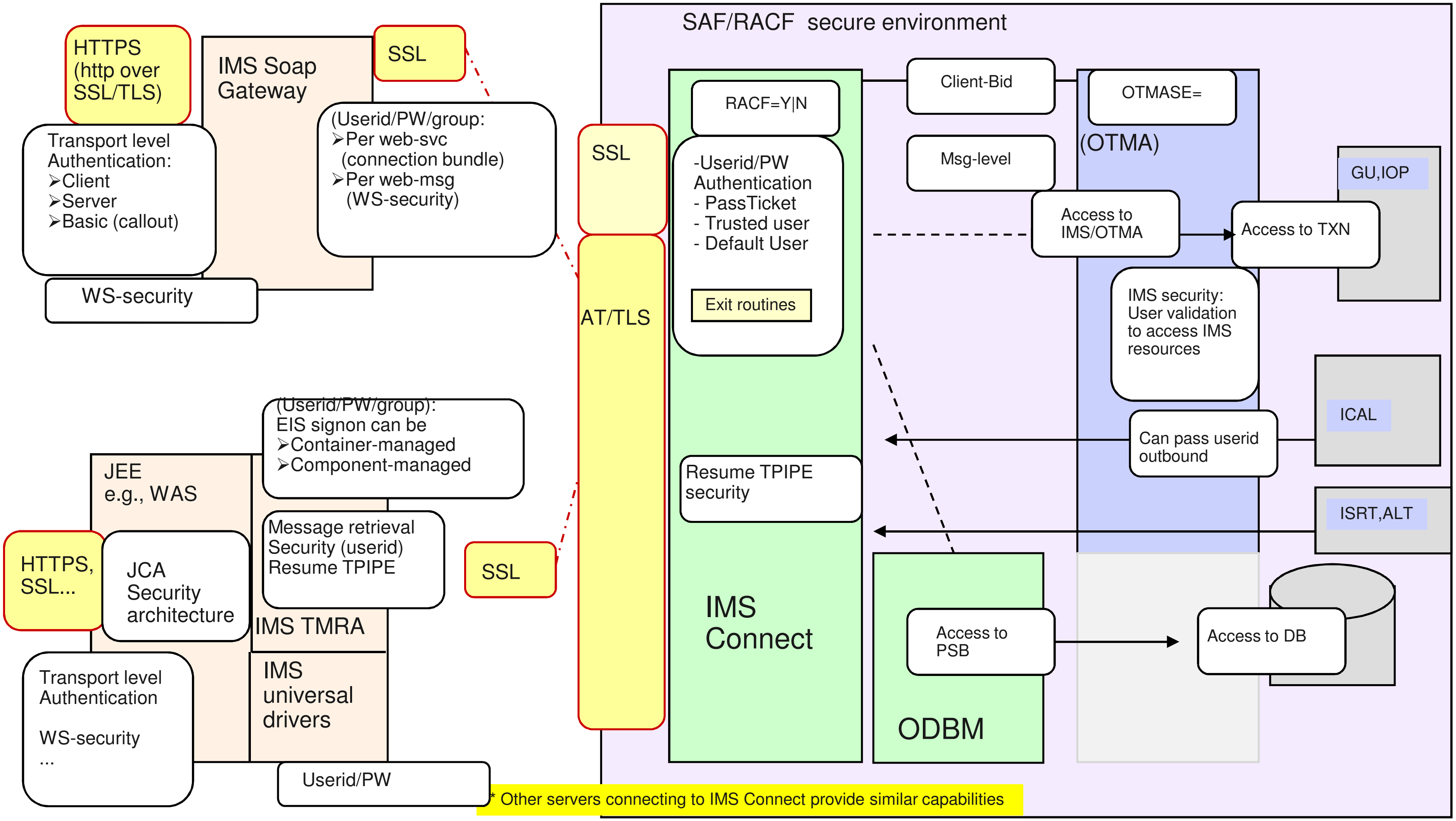
6 zSecure
- •Detect abnormal activity violating several security policies
- •Alert QRadar with raised severity

7 Guardium
- •Detect abnormal activity violating several data access policies
- •Block specific request
- •Alert QRadar with raised severity

8 QRadar
- •Correlates App ID violation with Joe.Admin activity
- • Open ticket to fix compromised AppID and investigate Joe.Admin
- •Determine new rogue sources

Second level: Security Points for an Enterprise Server

- Connectivity Options with IMS Connect



HTTPS (http over SSL/TLS)

IMS Soap Gateway

SSL

Transport level Authentication:
- Client
- Server
- Basic (callout)

(Userid/PW/group:
- Per web-svc (connection bundle)
- Per web-msg (WS-security)

WS-security

SSL

AT/TLS

SAF/RACF secure environment

RACF=Y|N

-Userid/PW Authentication
- PassTicket
- Trusted user
- Default User

Exit routines

Client-Bid

Msg-level

OTMASE=

(OTMA)

GU,IOP

Access to IMS/OTMA

Access to TXN

IMS security: User validation to access IMS resources

ICAL

Can pass userid outbound

ISRT,ALT

(Userid/PW/group):
EIS signon can be
- Container-managed
- Component-managed

JEE
e.g., WAS

Message retrieval Security (userid) Resume TPIPE

Resume TPIPE security

HTTPS, SSL…

JCA Security architecture

SSL

IMS TMRA

IMS Connect

Access to PSB

Access to DB

IMS universal drivers

ODBM

Transport level Authentication

WS-security
…

Userid/PW

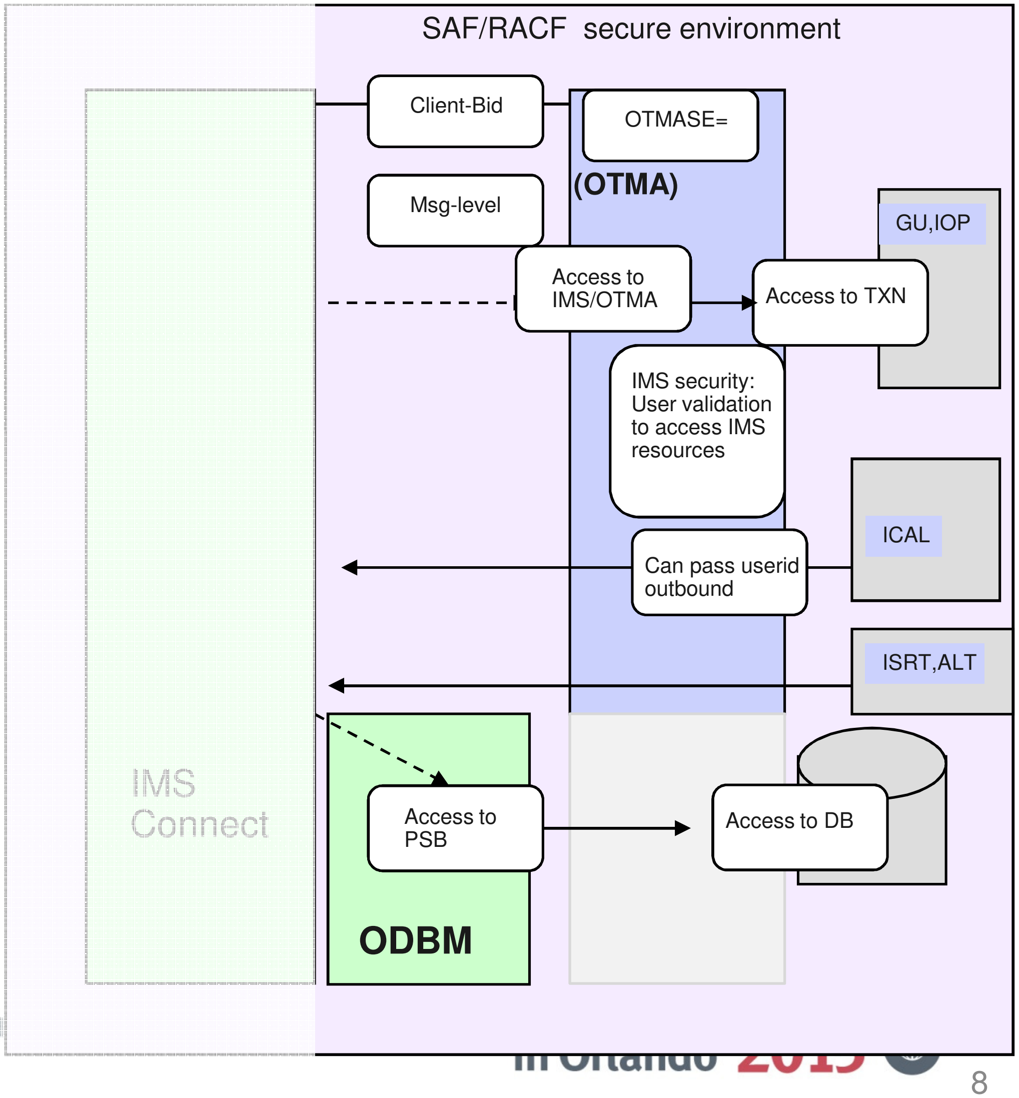
* Other servers connecting to IMS Connect provide similar capabilities

Security scenarios

- IMS as a provider
  - Transactions
    - Synchronous and asynchronous
  - Commands
  - Database
    - Open DB support and the universal drivers
- IMS as a consumer
  - Synchronous callout
  - Asynchronous callout
    - Including Business Event processing

IMS Security

- *Continues to be based on userid access to the IMS resource*
  - Transaction, command, PSB, DB, etc..
- **OTMA** - *for transaction and command access*
  - Client Bid security
    - Determines whether an OTMA client, e.g., IMS Connect, can connect to IMS
  - Message security
    - OTMA setting to determine the level of checking for each message
- **ODBM** - *for database access*
  - APSB security and/or IMS RAS (ISIS=) security



Userid

- **Control blocks** that represent the secured user
  - **ACEE** – Accessor Environment Element
    - z/OS control block which represents a user's identity
    - Created by the SAF security manager, e.g., RACF
    - IMS security validation uses ACEEs
  - **User Token**
    - z/OS control block that can be passed and used by IMS to build an ACEE
      - an 80-byte value which can be used to represent a user
        - Contains a user ID, default group ID, and some credential information
  - **RACO** – RACF Environment Object
    - A "flattened" ACEE which can be transported from one address space to another address space and reconstituted into an ACEE
    - Can be used across MVS images

Created by components, e.g., IMS Connect, where authentication takes place

OTMA Security

- Two Types of OTMA security
  - OTMA Client Bid security
    - Determines whether an OTMA client, e.g., IMS Connect, MQ, etc., can connect to OTMA
      - When IMS Connect initializes
        - » A "Client-bid" message is sent to IMS
        - » Uses userid associated with IMS Connect
      - If OTMA security is enabled (something other than NONE)
        - » IMS Connect userid must have READ access to the RACF facility classes:
        - » IMSXCF.xcfgrp.ims connect-member-name
  - OTMA Message security
      - OTMA setting to determine the level of checking for each message
- OTMA clients, e.g., IMS Connect, also have their own connection security

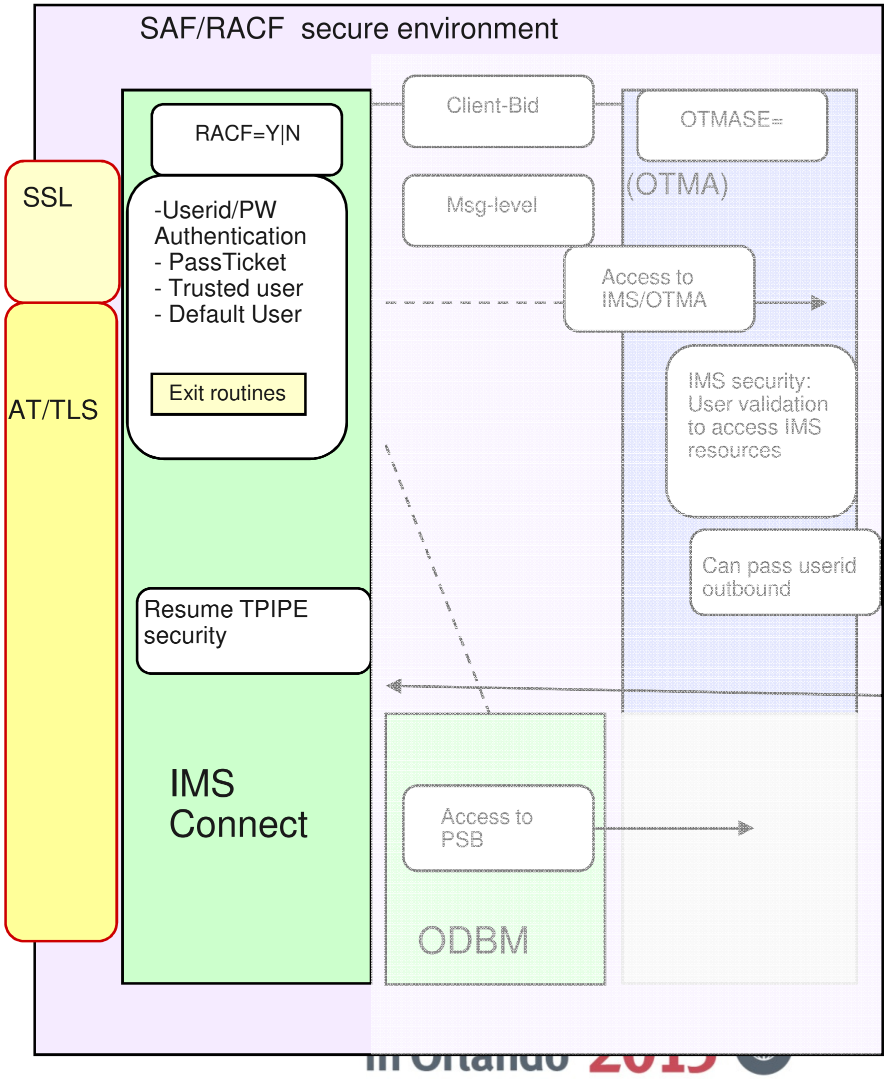
OTMA Message Security …

- **IMS Security**
  - Validates userid access to transaction or command
  - Userid: from message header or RACFID (see IMS Connect security)
  - /SECURE OTMA None | Check | Full | Profile or OTMASE=
    - Anything other than NONE – the userid is used to access IMS resources
    - Access to DB2 resources (use Full to propagate the userid)

- **Resume TPIPE Security (associated with IMS Connect)**
  - RIMS SAF/RACF security resource class
    - Security definition association between TPIPE name and Userid/Group that can access the TPIPE
  - OTMA security exit DFSYRTUX
    - Always invoked after the call to SAF/RACF
    - Can override the decision of SAF/RACF
    - Invoked even if new RIMS security resource class is not defined
  - Supports both the asynchronous callout and synchronous (ICAL) callout
  - Authorization is performed by IMS OTMA when the message is retrieved from the hold queue

IMS Connect Security

- Accessing IMS transactions from a remote client
  - Remote TCP/IP Client
    - Provides Userid, Password, Groupid in message header
  - IMS Connect authenticates the userid/password
    - Configuration values for IMS Connect (HWSCFGxx)
      - RACF = Y | N and RACFID = userid (default)
      - Issues RACROUTE calls to authenticate user if RACF=Y
    - Message exits can also call a user-written routine which are called before any SAF/RACF calls:
      - IMSLSECX –security exit routine for transactions and commands
      - HWSAUTH0 – security exit routine for DB requests
    - Default RACFID
      - Useful if the inbound request does not carry a userid value and a value needs to be passed into IMS for authorizing access to resource
        - » Does not provide an override for requests that carry a blank userid from the IMS TM resource adapter (e.g., WAS environment)



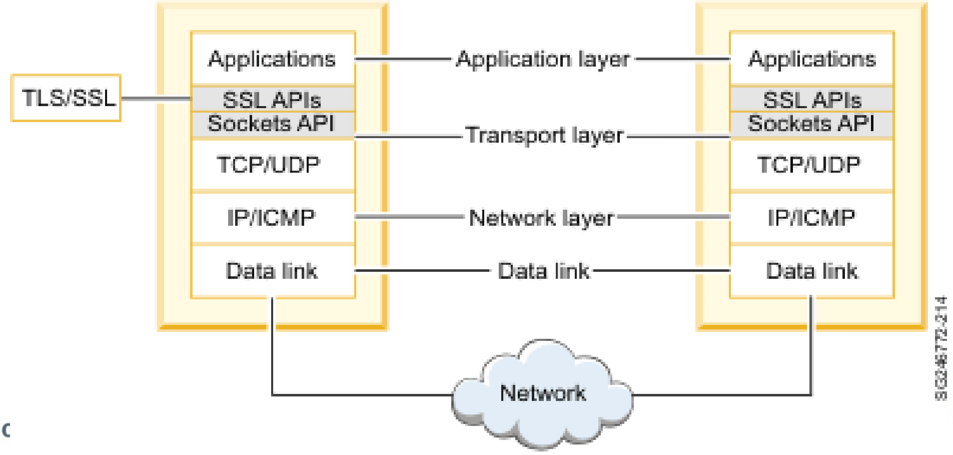
Securing Access to IMS Connect …

- Accessing IMS transactions from a remote client …
  - IMS Connect authenticates the userid/password (cont'd)
    - Support for RACF mixed case passwords and passphrases
    - Support for RACF ENF (event notification) which signals a change in the userid
      - Recycles any ACEES that are cached
  - Transport level:
    - Basic security …
      - Considerations
        - Security requests flow in the clear
        - No encryption
    - Alternatives:
      - IMS Connect Security
        - Passtickets
        - Trusted User Support
        - SSL
      - AT-TLS

SSL → TLS

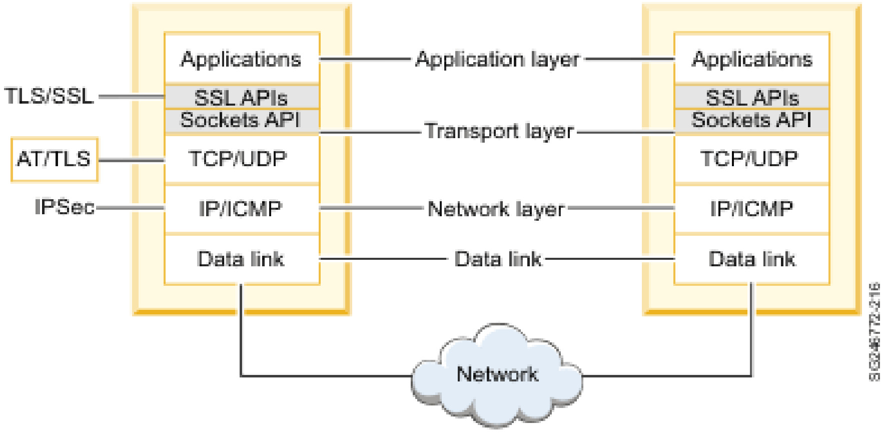
- Secure Sockets Layer - TCP/IP encryption and authentication protocol
  - Secure transfer of sensitive information which uses encryption to provide confidentiality and authentication between two TCP/IP applications

- Transport Layer Security – an evolution from SSL
  - As SSL gained in popularity, the IETF formally standardized SSL, made a few improvements and changed the name to Transport Layer Security (TLS)
  - TLS is defined in Request for Comments (RFC) 2246
    - Authentication of the server
    - A decision about how the data is to be encrypted
    - Optionally, the authentication of the client



TLS -> Application Transparent TLS (AT-TLS)

- Application Transparent TLS (AT-TLS) is a unique usage of TLS on z/OS
  - Instead of having the application itself (IMS Connect) be aware of TLS
    - Establishing the TLS connection is pushed down the stack into the TCP layer
  - Remote clients cannot distinguish between "normal" TLS (where the z/OS server application does the socket calls necessary for TLS) and AT-TLS (where the TCP layer handles the connection)
    - Application on z/OS can run without even being aware that the underlying connection to the remote client is using TLS



- AT-TLS is activated by specifying the TTLS option in the TCPCONFIG statement block in the TCP/IP profile data

And … Why choose to use AT-TLS?

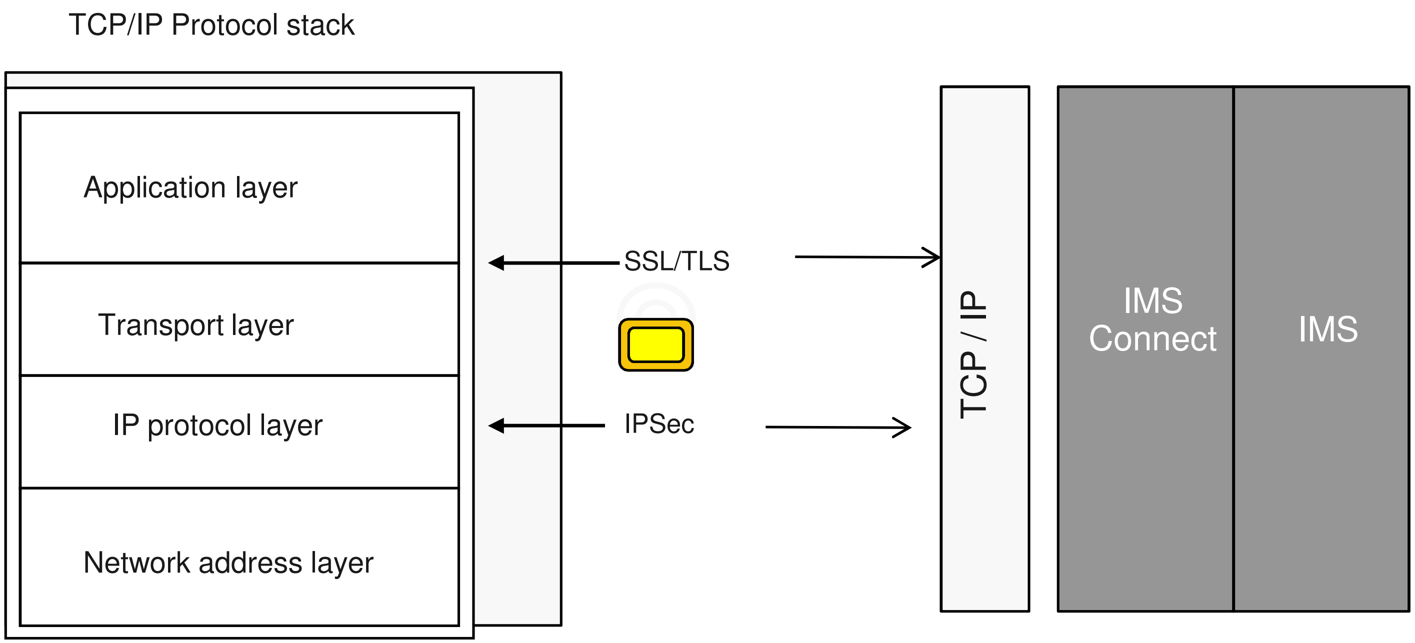
- Participation in AT-TLS is transparent to IMS Connect
  - IMS Connect can therefore be invoked by a remote client using TLS

    and
  - Rely on the z/OS TCPIP stack to perform the handshaking protocol to negotiate as well as perform all the require authentications and encryption

- Supports multiple ports
  - SSL support in IMS Connect is limited to a single port for the IMS Connect instance
  - IMS Connect-specific support for SSL is being withdrawn

- No additional configuration specifications in IMS Connect

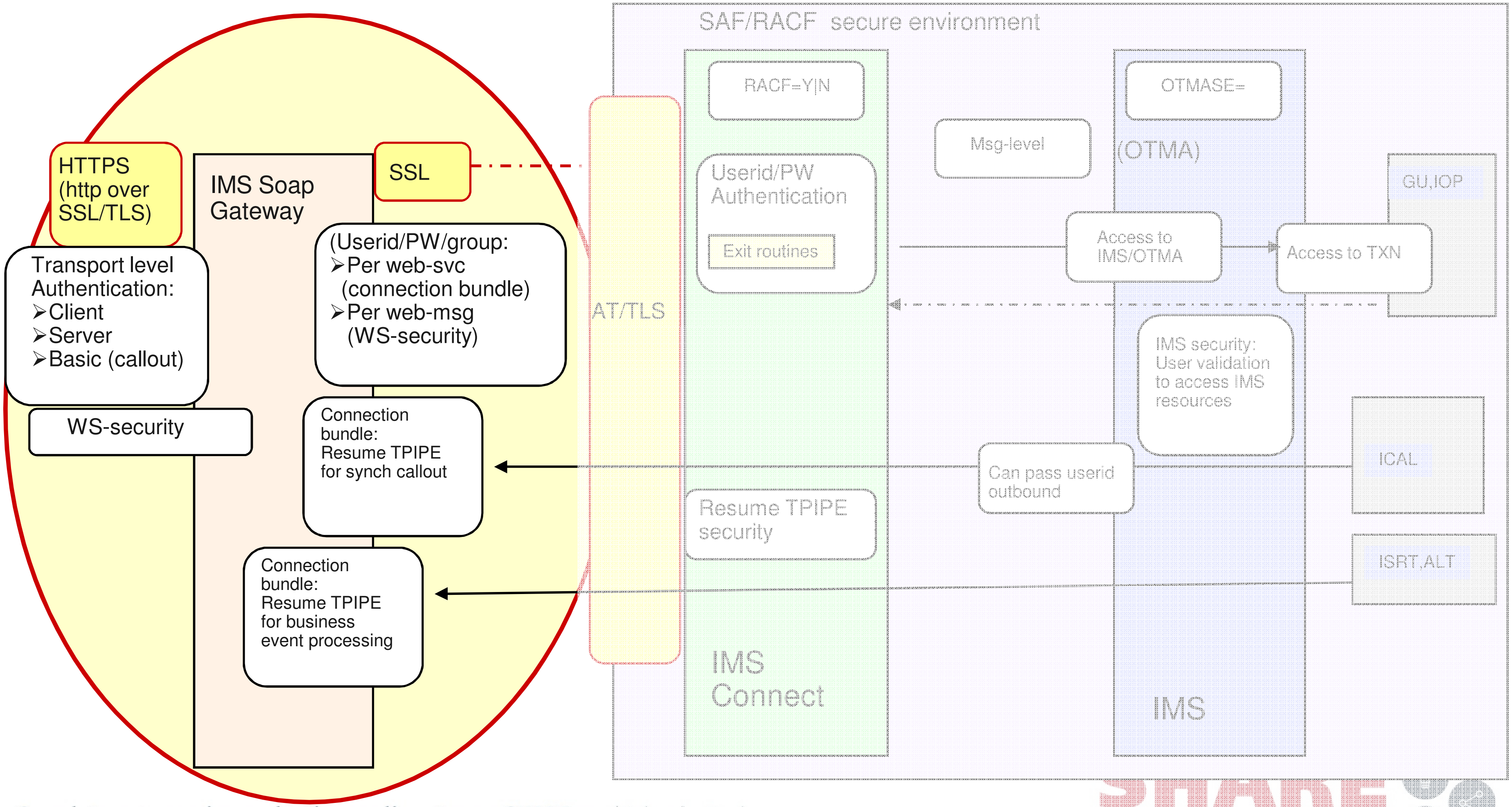
How About IPSec



- IPSec is intended to protect traffic between two TCP/IP stacks, absolutely transparently to the applications, and can potentially protect any TCP/IP protocol that TCP/IP datagrams are carrying
  - It is an industry-wide adapted protocol, and you can expect interoperability between different platforms
  - It provides device-to-device type of security with peer-to-peer authentication and supports all protocols

- AT-TLS is intended to protect traffic between specific client and server applications, as well as between the TCP/IP stacks to which these applications are bound
  - It provides application-to-application security (protects specific applications/ports) with server-to-client or client-to-server types of authentication

IMS Soap Gateway Security



HTTPS (http over SSL/TLS)

IMS Soap Gateway

SSL

Transport level Authentication:
- Client
- Server
- Basic (callout)

(Userid/PW/group:
- Per web-svc (connection bundle)
- Per web-msg (WS-security)

WS-security

Connection bundle: Resume TPIPE for synch callout

Connection bundle: Resume TPIPE for business event processing

AT/TLS

SAF/RACF secure environment

RACF=Y|N

Userid/PW Authentication

Exit routines

Resume TPIPE security

IMS Connect

Msg-level

Can pass userid outbound

OTMASE=

(OTMA)

Access to IMS/OTMA

IMS security: User validation to access IMS resources

IMS

Access to TXN

GU,IOP

ICAL

ISRT,ALT

IMS Soap Gateway

- Supports HTTPS connections with clients and SSL/AT-TLS with IMS Connect

- Transport-level (connection) security between remote client and IMS SG
  - Server authentication
    - During the SSL handshake, the server sends a certificate to the client to authenticate itself
      - Client authenticates the identity the certificate represents
        - Certificate contains a public key and the cryptographic algorithms used in SSL
  - Client (Mutual) authentication
    - Server authentication (making it mutual) plus the requirement for the client to send its certificate to the server for authentication
  - * Certificates come from a trusted CA (Certification Authority)
    - They are exchanged at the transport level to establish trust before the connection can be established or a web service invoked

IMS Soap Gateway...

- Basic authentication (for IMS as a web service consumer, e.g. IMS callout)
  - When IMS Soap Gateway is the client, the server that hosts the web service may require basic authentication credentials in order to call the remote service
  - Connection bundle optional properties (IMS SG configuration)
    - Basic authentication user ID: Specifies the user ID to send to the server that hosts the web service for basic authentication
      - basic authentication password
    - Callout truststore name: Specifies the fully qualified path name of the truststore on SOAP Gateway that stores the certificates of trusted external web service servers(required for client or server authentication)
      - Trustore password
    - Callout keystore name: Specifies the fully qualified path name of the keystore on SOAP Gateway that stores the trusted client certificates for a callout application to authenticate with a target web service (Required for client authentication)
      - Keystore password
  - Security certificates can be sent at the transport level for server authentication or client authentication

IMS Soap Gateway ...

- IMS SG support for the ***IMS as a provider*** scenario ***(inbound to IMS)***
  - Authentication of users on either a per-web-service or per-message basis

    - Per-web-service
      - Userid and password are specified in the connection bundle (properties that specify IMS SG to IMS Connect connection)
        - » *All requests for that service send the same userid to IMS*

    - Per-Message
      - Support for WS-Security
        - » Userid and password are enclosed as tokens in the WS-Security header in each message
        - » > Requests can reflect different userids (cont'd ....)

WS-Security (Web Services Security or WSS) is a published SOAP extension standard (XML-based) that allows security (authentication and authorization) information to be exchanged in support of web services. Its goal is to protect the integrity and confidentiality of a message as well as the ability to authenticate the sender. The protocol specifies how to enforce integrity and confidentiality on messages and supports a variety security token formats, e.g., UNTP, SAML, x.509 certificates, kerberos tickets, etc Of the various security token formats supported, IMS Soap Gateway allows UNTP and SAML.

IMS Soap Gateway ...

- IMS SG support for the *IMS as a provider* scenario (contd)
  - Authentication of users on either a per-web-service or per-message basis ...

  - Per-Message ...
    - Security tokens supported for WS-Security header (only one type per web service)
      - *UsernameToken Profile (UNTP) 1.0 user name tokens*

        - User name and password in the message header
      - *Security Assertion Markup Language (SAML) 1.1 and 2.0 unsigned sender-vouches tokens*

        - Minimal sender-vouches SAML assertion. No signatures or certificates required
      - *SAML 1.1 and 2.0 signed sender-vouches tokens with two trust types:*

        - Token is signed by a Security Token Service (STS) or signed by sender

        - IMS Soap Gateway can be configured to:

Trust any - any valid security certificate in the SOAP header is allowed.

Trust one - the security certificate in the SOAP header must be configured with the server trustore path and password

Use of WS-Security supports a custom authentication module that can perform additional checking by using a Java Authentication and Authorization Service (JAAS) module

IMS Soap Gateway ...

- IMS SG support for the *IMS as a Consumer* scenario *(IMS is the client)*
  - – Synchronous Callout - Supports callout to web services that require authentication of users on a per-web service or per-message basis
    - Per-message
      - – Userid is enclosed as a token in the WS-Security header in each message
        - » Originating Userid (PSTUSID) for the IMS synchronous callout application is passed to the external web service for further authentication and authorization
      - – Security tokens supported for WS-Security header (only one type per callout request)
        - » SAML 1.1 unsigned sender-vouches tokens
        - » SAML 2.0 unsigned sender-vouches tokens
    - Per-web service
      - – Userid used is what is specified in the connection bundle
    - When WS-Security is enabled, you can also provide your own custom authentication module to perform additional checking by using a JAAS module
  - – Business event processing (asynchronous callout)
    - Security on a transport level – Client, Server, or Basic authentication

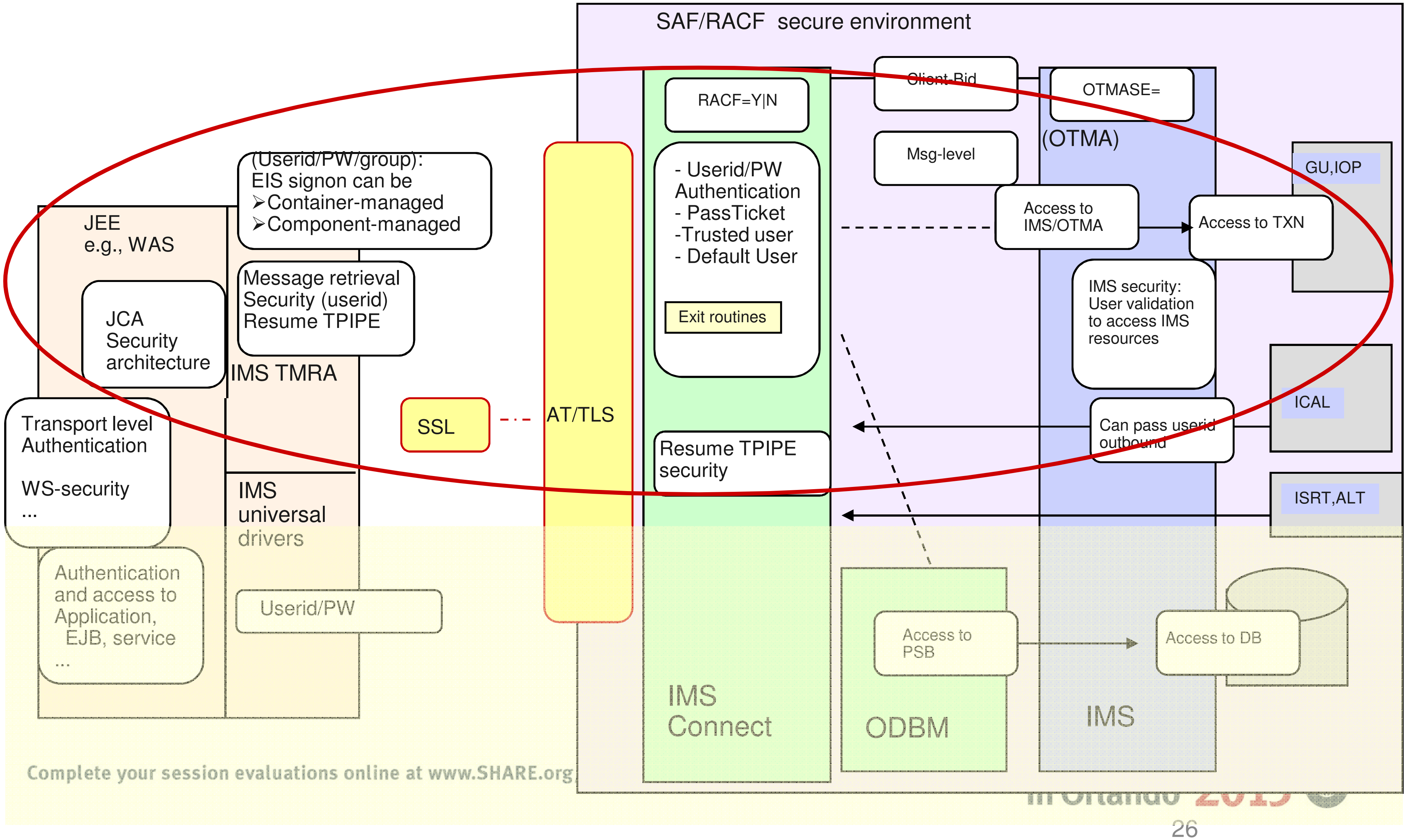
IMS Soap Gateway -> IMS Connect -> OTMA

- IMS Connect
  - *When WS-Security is enabled*, depending on the token type, SOAP Gateway passes the following information to IMS Connect:
    - For user name tokens: userid, password, and the payload data
      - if IMS Connect security is enabled (RACF=Y)
        - IMS Connect authenticates the user ID and password
        - Passes userid and data to OTMA. IMS Connect does not pass any password information to OTMA.
      - If IMS Connect security is disabled (RACF=N)
        - Passes on the userid and data to OTMA without authentication
    - For SAML tokens, SOAP Gateway passes the user ID and the payload data
      - IMS Connect security must be turned off because SAML tokens do not contain password information
        - **If IMS Connect security is turned on, the authentication will fail !!!**
  - *When WS-Security is disabled*
    - IMS SG passes the userid and password information in the connection bundle for the web service to IMS Connect
      - As above, IMS Connect actions depend on the RACF= specification

IMS Soap Gateway > IMS Connect > OTMA

- OTMA
  - If OTMA security is enabled (OTMASE={CHECK|PROFILE|FULL}), OTMA authorizes the user to access transactions or OTMA commands
  - If OTMA security is set to OTMASE=NONE, then no authorization check is performed
  - For callout requests (asynchronous or synchronous)
    - Resume TPIPE processing (connection bundle) can invoke Resume TPIPE security in IMS (RIMS class and DFSYRTUX exit)

IMS TM Resource Adapter (IMS TMRA)



SAF/RACF secure environment

JEE
e.g., WAS

JCA
Security
architecture

(Userid/PW/group):
EIS signon can be
➢Container-managed
➢Component-managed

Message retrieval
Security (userid)
Resume TPIPE

IMS TMRA

Transport level
Authentication

WS-security
…

IMS
universal
drivers

Authentication
and access to
Application,
EJB, service
…

Userid/PW

SSL

AT/TLS

RACF=Y|N

- Userid/PW
Authentication
- PassTicket
-Trusted user
- Default User

Exit routines

Resume TPIPE
security

IMS
Connect

Client-Bid

Msg-level

OTMASE=

(OTMA)

Access to
IMS/OTMA

Access to TXN

GU,IOP

IMS security:
User validation
to access IMS
resources

Can pass userid
outbound

ICAL

ISRT,ALT

Access to
PSB

ODBM

Access to DB

IMS

JEE - WAS basics...

- The JCA security architecture extends the end-to-end security model for JEE-based applications to include integration with EISs (e.g., IMS)
  - Supports the specification that WAS and IMS must collaborate to ensure that only authenticated users are allowed access to the IMS environment
    - through a set of system-level contracts such as:
      - Connection management: enables WAS to pool connections to IMS (IMS Connect) for a scalable environment that can support a large number of clients
      - Transaction management: enables WAS manage transactions across multiple resource managers
      - Security management: reduces security threats and protects access to IMS
- ***IMS TM resource adapter (IMS TMRA)***
  - Follows the Java EE Connector Architecture (JCA) security architecture, and works with the WebSphere Application Server (WAS) security manager

WAS – IMS TMRA

- Connectivity between IMS TMRA and IMS Connect
  - Transport Level: recommendation is to use AT/TLS with IMS Connect
  - Message Level: Supports passing the userid/password/groupid authentication credentials that are supported by IMS Connect
    - Supplied either by
      - The WAS application component (component-managed signon)
      - Or by the application server (container-managed signon).

IMS TMRA

- *IMS as a provider* scenario *(Inbound to IMS)*
  - Container-managed signon:
    - Relies on the security manager in the application server to provide and manage the security information
      - Uses the directive <res-auth>Container</res-auth> specified in the deployment descriptor of the application to provide the userid, password, groupid
    - Local Option
      - This is a z/OS-only feature where both WAS and IMS Connect run in the same z/OS image
      - WAS authenticates the user based on the security information that is defined in the container-managed alias
        - » Creates and passes a user token that represents the authenticated user to IMS TMRA which passes the token to IMS Connect
  - Alternatively,
    - WAS configuration can request that the user identity that is associated with the current thread of execution be used during user authentication
      - » No need to specify a JAAS container-managed authentication alias in the J2C connection factory that is used by the application.

IMS TMRA ...

- *IMS as a provider* scenario (contd)
  - Component-managed signon:
    - Relies on the application (the component) in WAS to provide and manage the security information to be used for signing on to IMS Connect
      - Uses the <res-auth> element in the resource reference of the deployment descriptor of the application
    - Provides the security information (user ID, password, and optional group name) in IMSConnectionSpec object and passes it to IMS TMRA
      - » IMS TMRA passes this security information to IMS Connect for use in signing on (authentication and authorization)
  - Note:
    - If the application is generated by a Rational or WebSphere development environment, the security information is passed as application input data
      - To pass the security information as input data the userName, password, and groupName properties of the IMSConnectionSpec class must be exposed
    - If the application does not use one of the methods to provide security information, WAS obtains the security information from the J2C connection factory custom properties

IMS TMRA –> IMS Connect

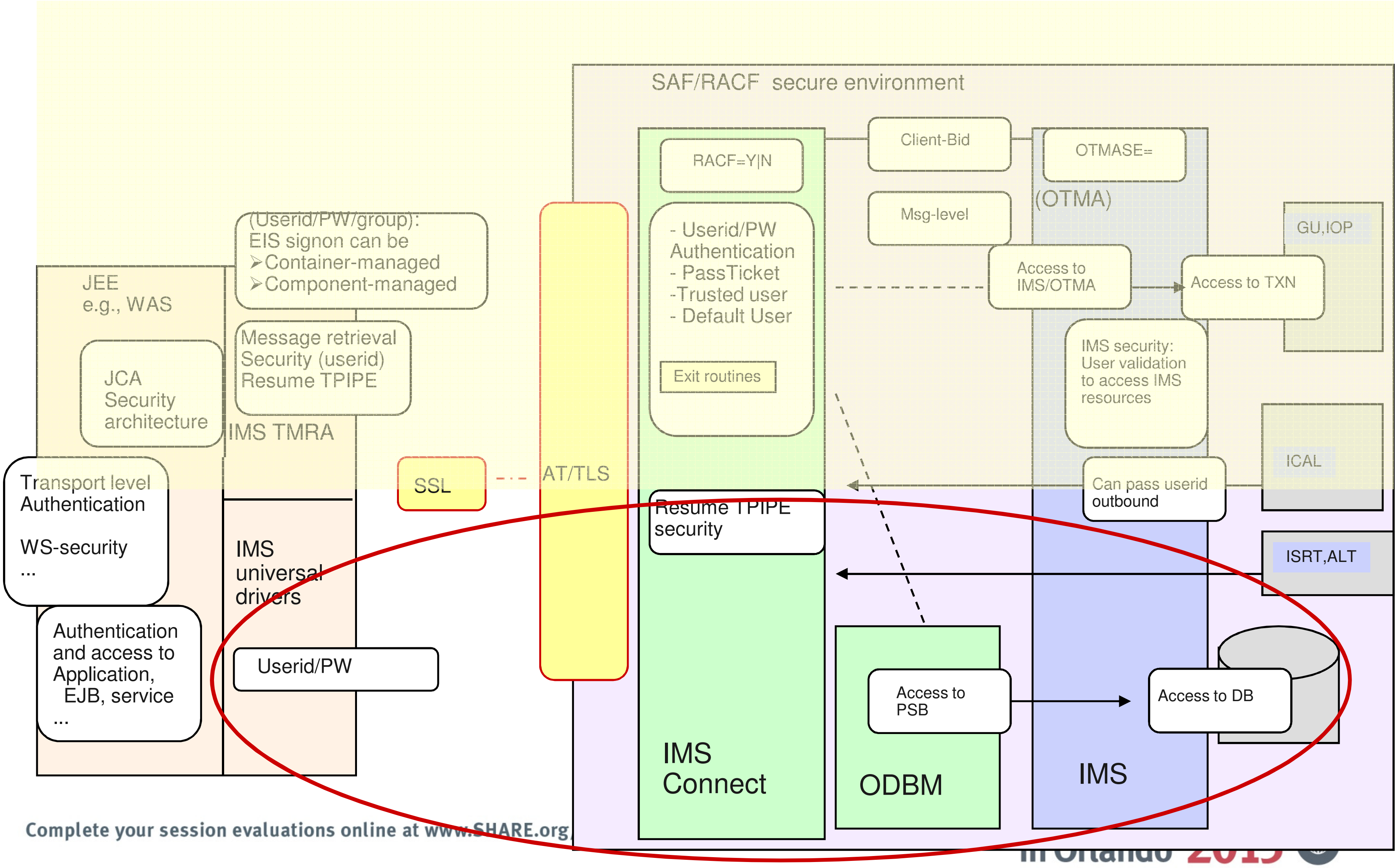
- When WAS/IMS TMRA connects from a distributed platform or from z/OS with TCP/IP:
  - With either component-managed signon or container-managed signon:
    - If RACF=Y in IMS Connect
      - IMS Connect authenticates the userid/password (SAF call)
        - Successful authentication results in passing the userid, optional group, and UTOKEN to IMS OTMA for authorizing access to IMS resources
    - If RACF=N in IMS Connect
      - No authentication is done.
        - However, if the message header contains login information, then the userid and optional group name are passed to IMS OTMA for authorization

- When WAS on z/OS uses Local Option with Container-managed signon
  - Authentication is performed only by the application server and not IMS Connect
    - Regardless of the RACF setting in IMS Connect
      - WAS calls SAF/RACF to create the user token
      - IMS TMRA passes the user token to IMS Connect
      - When IMS Connect sees the user token, it passes the user token to IMS OTMA to authorize access IMS resources

IMS TMRA

- *IMS as a consumer* scenario (*IMS is the client)*
  - IMS callout requests (synchronous ICAL or asynchronous) are retrieved from IMS Connect by using the Resume TPIPE call
    - Resume TPIPE security ensures that the userid associated with the Resume TPIPE is authorized against the TPIPE
    - If security is enabled and the tpipe does not exist at the time the RESUME TPIPE call is issued, the call is rejected
  - For message-driven beans (MDBs)
    - SSL authentication is supported for communication with IMS
    - Security information is specified in the J2C activation specification (IMSActivationSpec) that is configured in WAS
  - For non-MDB applications
    - Userid must be specified in the connection specification of the WAS application or the connection factory that is used by the application

Open DB Security



Open DB Security

- The IMS Universal DB resource adapter (driver) provides JDBC SQL access to IMS data from JEE (and non-JEE) environments on any platform
  - Access to IMS DBs use IMS Connect and ODBM
    - IMS Connect provides authentication of the userid/password sent in by the IMS Universal drivers on WAS

- IMS Connect to ODBM
  - RACF=Y
    - IMS Connect authenticates the Userid/Password/Group
      - Passes a RACF Object (RACO) to ODBM
    - ODBM uses this information for security
  - RACF=N
    - IMS Connect bypasses authentication and does not pass a RACO
    - ODBM used the ODBM Job Userid/Group

  - HWSAUTH0 (Security exit routine)

Open DB Security...

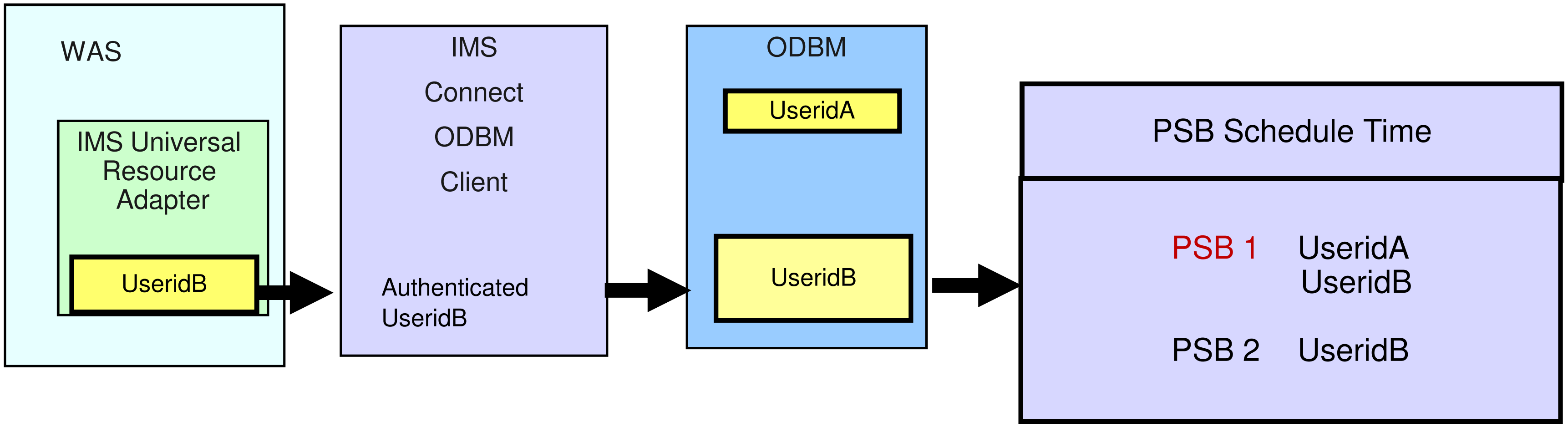
- ODBM to IMS
  - Security information is either the RACO from IMS Connect or, if no RACO then it is the userid/group from the ODBM jobcard

- ODBM and RRS=Y
  - ODBM uses the ODBA interface to IMS
    - Creates and passes ACEE in the Thread TCB
  - In IMS, ODBASE parameter is in effect
    - ODBASE=Y invokes APSB security
      - IMS uses RACF to verify the Userid using the AIMS or Axxxxxxx resource class
      - The ISIS parameter is not used
    - ODBASE=N invokes RAS
      - IMS uses the ISIS parameter to determine the RACF call using the IIMS or Ixxxxxxx resource class
      - ISIS=N – No RACF checking
      - ISIS=R – RACF call
      - ISIS=C – DFSRAS00 exit
      - ISIS=A – RACF call and DFSRAS00 exit

- ODBM and RRS=N
  - ODBM uses the CCTL interface to IMS (like CICS)
    - Pass Userid/Group in PAPL
  - In IMS, the ISIS parameter to determine the RACF call using the IIMS or Ixxxxxxx resource class
    - ISIS=N – No RACF checking
    - ISIS=R – RACF call
    - ISIS=C – DFSRAS00 exit
    - ISIS=A – RACF call and DFSRAS00 exit

Open DB Security...

- Example



WAS

IMS Universal Resource Adapter

UseridB

IMS Connect ODBM Client

Authenticated UseridB

ODBM

UseridA

UseridB

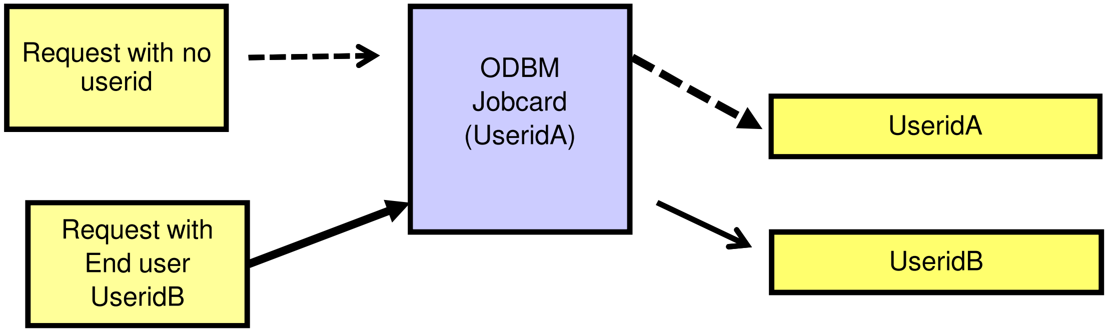
PSB Schedule Time

PSB 1 UseridA UseridB

PSB 2 UseridB

Use of resource classes AIMS or IIMS|JIMS is based on use of SAF/APSB versus RAS

Or optionally the DFSRAS00 exit decision when using RAS



Request with no userid

Request with End user UseridB

ODBM Jobcard (UseridA)

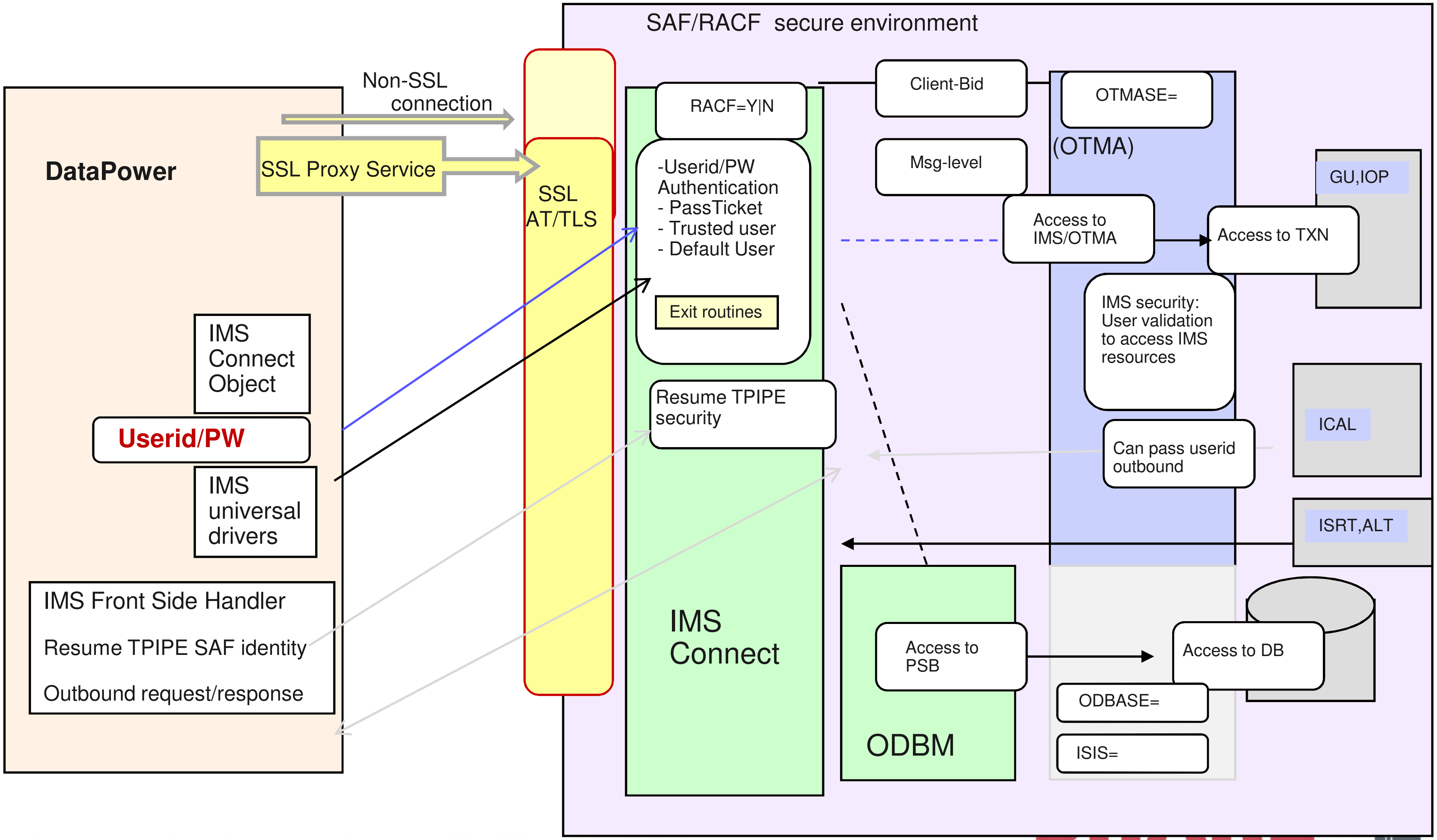
UseridA

UseridB

If defaulting to the ODBM userid, Can only access PSB1

Can access both PSB1 and PSB2

DataPower


SAF/RACF secure environment
DataPower
Non-SSL connection
SSL Proxy Service
SSL AT/TLS
IMS Connect Object
Userid/PW
IMS universal drivers
IMS Front Side Handler
Resume TPIPE SAF identity
Outbound request/response
RACF=Y|N
-Userid/PW Authentication
- PassTicket
- Trusted user
- Default User
Exit routines
Resume TPIPE security
IMS Connect
Client-Bid
Msg-level
OTMASE=
(OTMA)
Access to IMS/OTMA
Access to TXN
GU,IOP
IMS security: User validation to access IMS resources
ICAL
Can pass userid outbound
ISRT,ALT
ODBM
Access to PSB
Access to DB
ODBASE=
ISIS=

DataPower

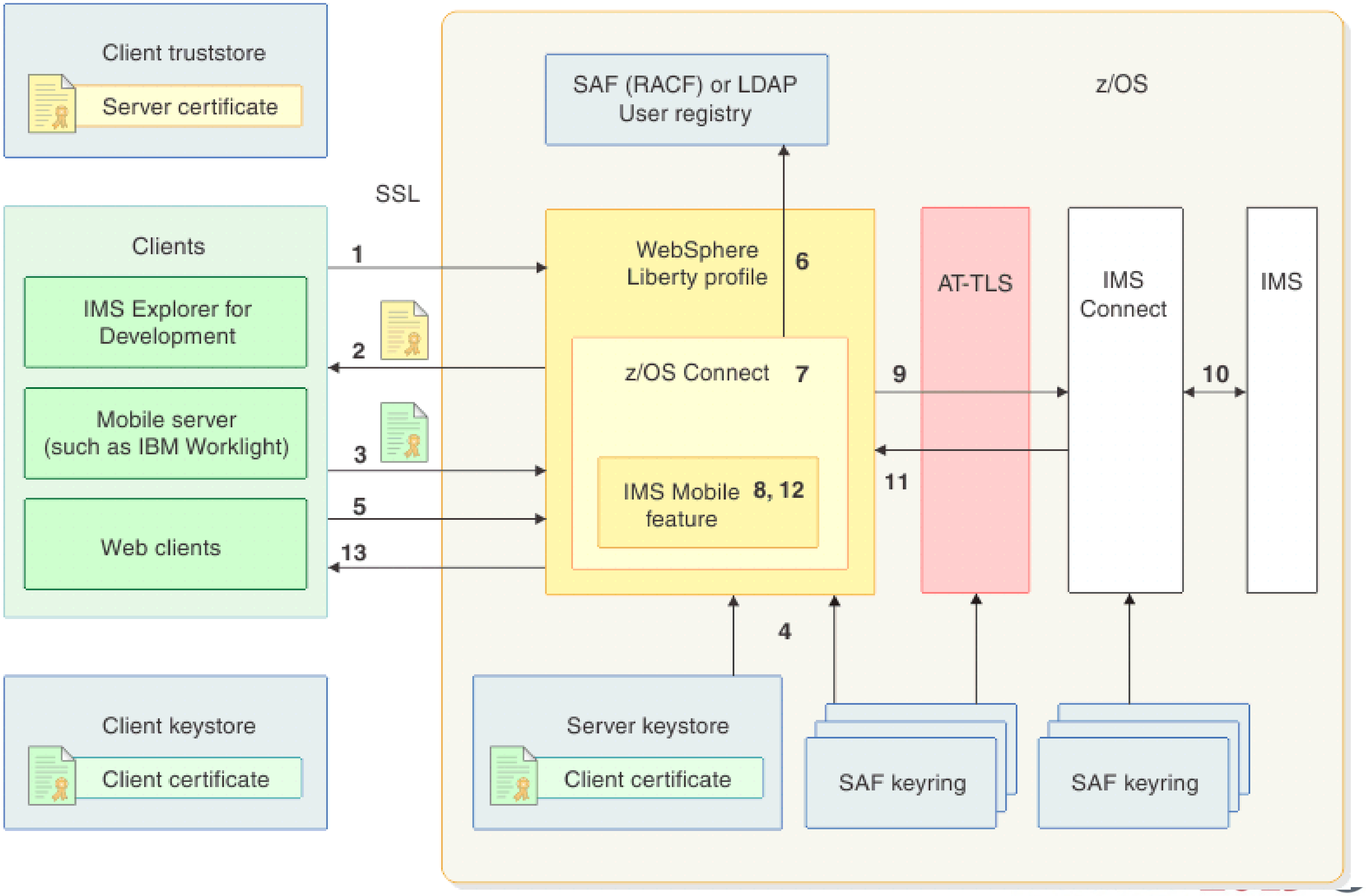
- Interfaces to get to IMS
  - Transaction access (DP appliances: ***XI50, XI50B, XI50z, XI52, XB62, …)***
    - ***IMS as a provider*** (Firmware 3.6.1, enhanced in 3.8.0 and 3.8.1)
      - ***IMS Connect Client -*** Access to IMS applications using a DataPower embedded IMSClientConnect handler to IMS Connect
        - » DP sends userid/password to be authenticated in IMS Connect
      - ***Soap -*** Access to IMS web services via the IMS SOAP Gateway
        - » Access using SOAP requests follow IMS SG security defined earlier
      - ***MQ Client -*** Access to IMS applications (MQIIH header) using an MQ server on system z and the MQ Bridge for IMS
        - » DP sends userid/password to be authenticated in IMS

    - ***IMS as a consumer - IMS Callout*** (Firmware 6.0)
      - ***"IMS Callout" front-side handler -*** natively connects to IMS Connect as service consumer
        - » IMS Resume TPIPE (RIMS class) can be set to validate the request to pull the message
      - Firmware 7.0 Enhancement and IMS Connect 13, IMS 13
    - In addition to the message payload, IMS includes ims-callout-user-id: IMS PSTUSID associated with the calling transaction
      - » The DataPower administrator can access the header fields in the MPG policy and set the userid as the requester for the target distributed service service

DataPower

- Interfaces to get to IMS …
  - Database access (DP appliances: ***XI50B***, ***XI52, XB62, XG45, …)***
    - ***Access to IMS DB*** (Firmware 6.0)
      - Leverages existing and proven technology
        - » IMS Universal JDBC driver
        - » IMS DRDA server: IMS Connect/ODBM
        - » IMS Catalog
      - Userid/password sent in by the IMS Universal drivers are authenticated by IMS Connect
        - » OPEN DB security as defined in previous visuals

And most recently…. Mobile access



And most recently…. Mobile access

1. The client initiates an HTTPS call to IBM WebSphere Liberty Profile

2. z/OS Connect is configured with SSL client authentication and a fallback to basic authentication

3. The client sends a client certificate. (Note: IMS Explorer does not send in the client certificate. A valid user ID (registered in the RACF® or LDAP user registry) must be specified in IMS Explorer for Development when you use the provided wizard to create and publish a mobile service. With this user ID properly configured, IMS Explorer for Development is considered a trusted client)

4. WebSphere Liberty Profile verifies the client certificate with the previously imported client certificate that is stored in the sever truststore or keyring. If the client certificate is missing, basic authentication is applied against the user registry that was configured (SAF or LDAP).

5. The client starts transmitted data over a secure connection

6. For a service request, WebSphere Liberty Profile authenticates the user credential. Then z/OS Connect authorizes the user by using a SAF call to validate that the group names in the service configuration matches one of the group names associated with the user ID in the request subject.
   - Note: WebSphere Liberty Profile must be configured with SAF registry authentication and the subject must be 8 bytes or less in order for the IMS Mobile feature to retrieve the RACF ID from the subject of the request. If authentication is disabled, or the subject is more than 8 bytes, the IMS Mobile feature retrieves the user ID from the technical ID, an IMS mobile global element that is specified during initial installation and setup.
   - If the technical ID is left blank, the IMS Mobile feature uses the z/OS Connect started job user ID.
   - The IMS technical groupname is the RACF groupname, and can be left blank.
   - The IMS technical password is the RACF password, and can be left blank

7. After authentication and authorization, z/OS Connect passes the request to the IMS Mobile feature for transforming the data from JSON to bytes. If authentication and authorization fail, an error is returned to the client.

8. The IMS Mobile feature transforms the incoming request from JSON to bytes. The user ID is extracted from the request subject from z/OS Connect

9. The IMS Mobile feature initiates a request to send the input bytes array and RACF information to IMS Connect. The request triggers SSL handshake via AT-TLS, if it is configured, to protect the communication between WebSphere Application Server Liberty Profile and IMS Connect.

10. IMS Connect flows the request with the RACF user ID, groupname, and technical password (if specified) to IMS. IMS might perform additional authorization, depending on the setting. IMS transaction runs. IMS returns response (bytes) to IMS Connect.IMS Connect returns response (bytes) to the IMS Mobile feature.

11. The IMS Mobile feature transforms the response from bytes to JSON.

12. The response is returned to the client.

The Bottom Line

- Multiple levels of security
  - OTMA
    - Validates whether an OTMA member (IMS Connect) can communicate with IMS
    - Implements transaction and command security
      - Userid that flows in on a message against the IMS resource
    - Supports callout to web services
  - ODBM
    - Passes security information to IMS for database access
  - IMS Connect
    - Supports the authentication of userids, groups, passwords and passes the utoken to IMS with the message
    - Additionally extends the security authentication
      - PassTicket support
      - Trusted User support
  - Network – connection security and encryption
    - SSL – TLS
    - AT-TLS