Securing Access to CICS

Nigel Williams | Certified IT Specialist | IBM
IBM Client Center, Montpellier, France

nigel_williams@uk.ibm.com

Thanks to: Phil Wakelin, Colin Penfold, James O'Grady, Ivan Hargreaves, Fraser Bohm and Rob Jones

Abstract and agenda

CICS applications and their associated data constitute some of the most valuable assets owned by an enterprise. These applications are rarely used in isolation anymore, instead, they form an integral part of a wider set of business processes that span several platforms and architectures. This session outlines the main planning considerations to help you to choose between different options for securing access to CICS. Security consideration for the strategic CICS integration technologies are reviewed, including:

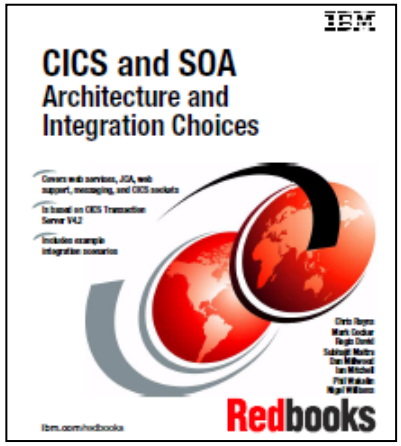
- Web services

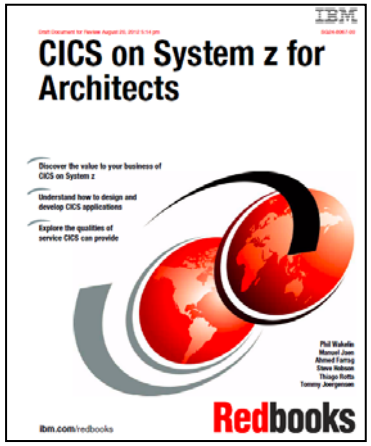
- CICS Transaction Gateway

- WebSphere MQ

This presentation is based on some new IBM ITSO Redbooks publications

- Transaction processing trends
- CICS integration scenarios
- Security challenges
- Sample solutions
- What's new in CICS TS V5.1
- What's new in CICS TG V9.0
- Summary





Transaction processing trends

Transaction Processing: Past, Present and Future

Published October 2012

Business

- New business services to attract customers and maintain their loyalty
- Business agility and optimization
- Control of risks and ability to respond to regulatory scrutiny
- Requirement to build partner relationships,and manage acquisitions and mergers
- Pressure to reduce costs

Technical

- Continued evolution of SOA
- Mobile
- Web 2.0
- Business events and rules
- BPM

"We try to provide a friendly and pleasant online experience to our customers and that also rewards them for their loyalty." ***(Misha Kravchenko, Marriott International)***

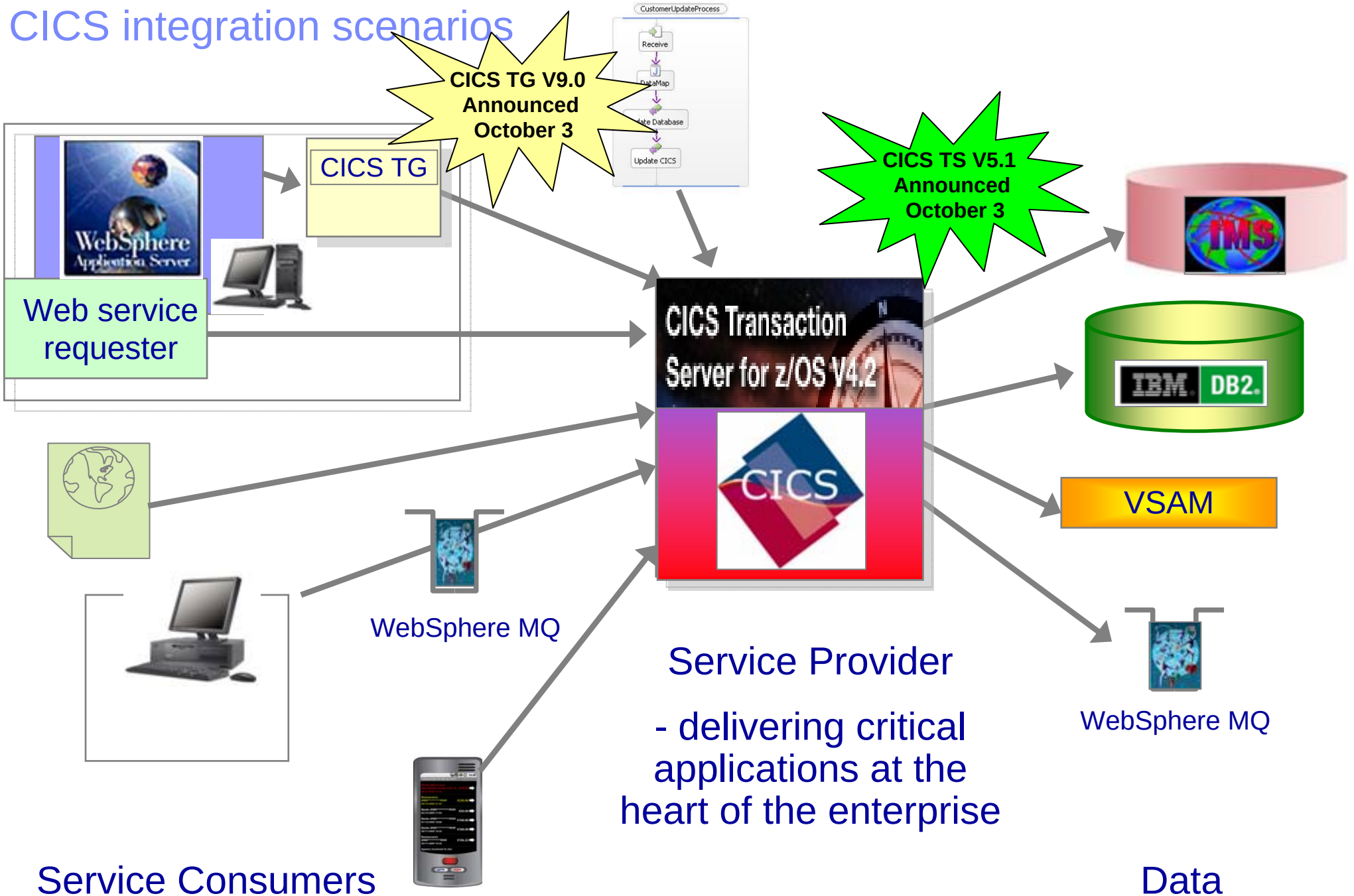
"The major business trends impacting our TP systems are increasing customer expectation, the need for quicker delivery of applications and more partner integration" ***(China Merchants Bank)***

"The overall cost of the service layer is greater than the process layer, which in turn is greater than the media access layer. This means that the best ROI is achieved through service reuse."

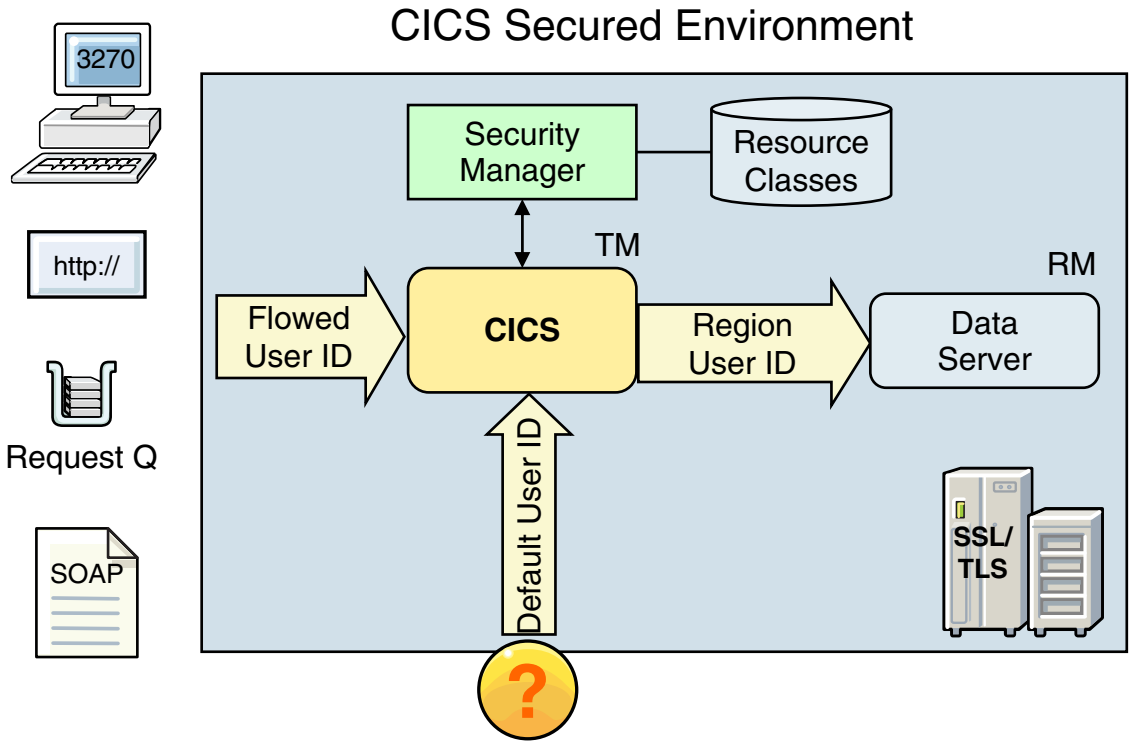
"The use of web services is strategic for the bank." ***(Marcel Däppen, UBS WM&SB)***

"We expect more growth coming from the mobile channel and we also foresee a workload increase from new self-service applications." ***(ABN AMRO Bank)***

CICS integration scenarios



CICS secure integration



Flowed User ID - authentication token for external user

Region User ID – used for checking CICS region access to system resources

Default User ID – used when no credentials have been established

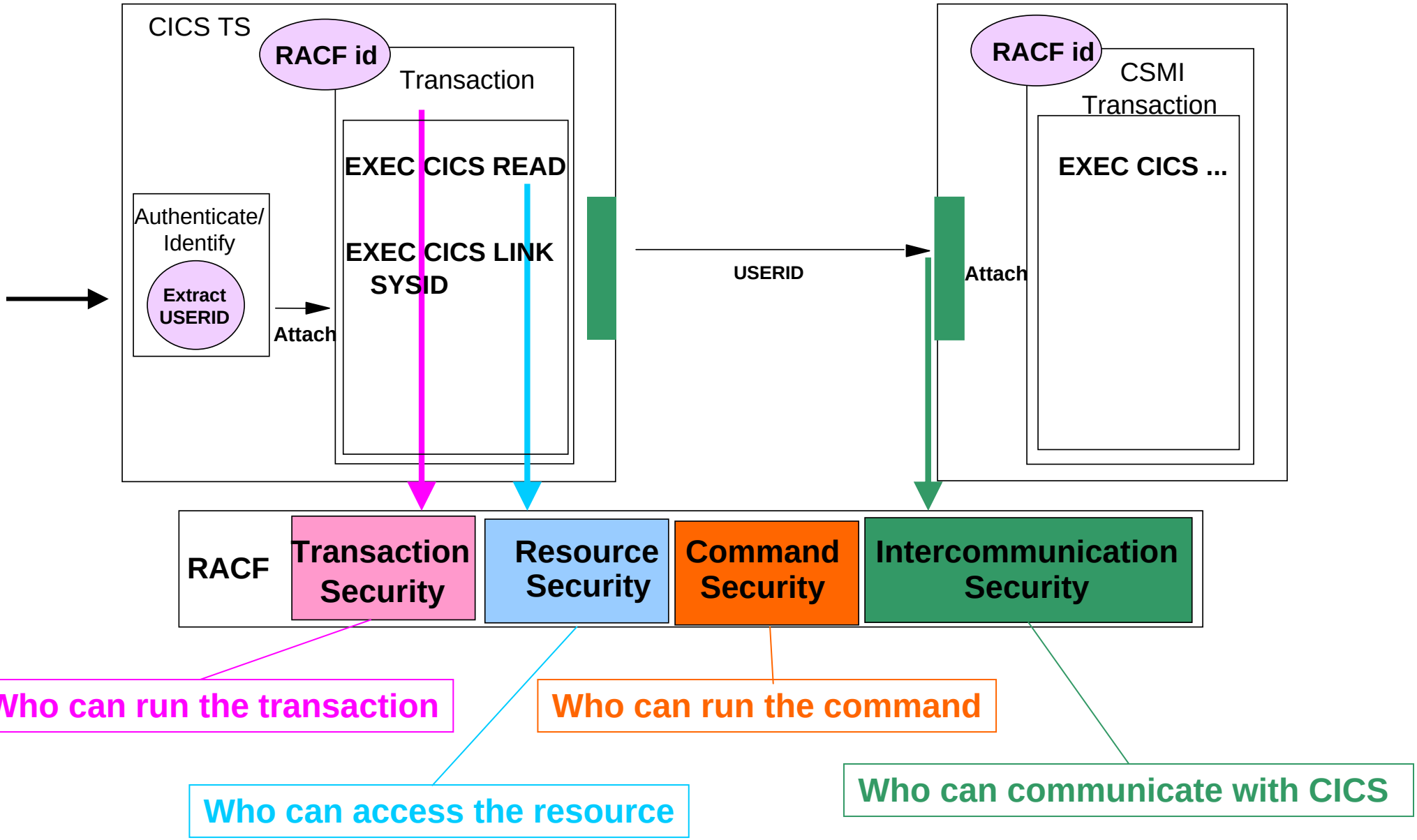
Authentication - CICS requires a password/pass phrase, digital certificate or identity assertion

Identification - CICS requires an 8-character userid for use with its external security manager

Authorization - CICS uses ESM to authorize the userid to a specified resource class

Confidentiality/Integrity - CICS uses TLS/SSL or WS-Security

CICS base security



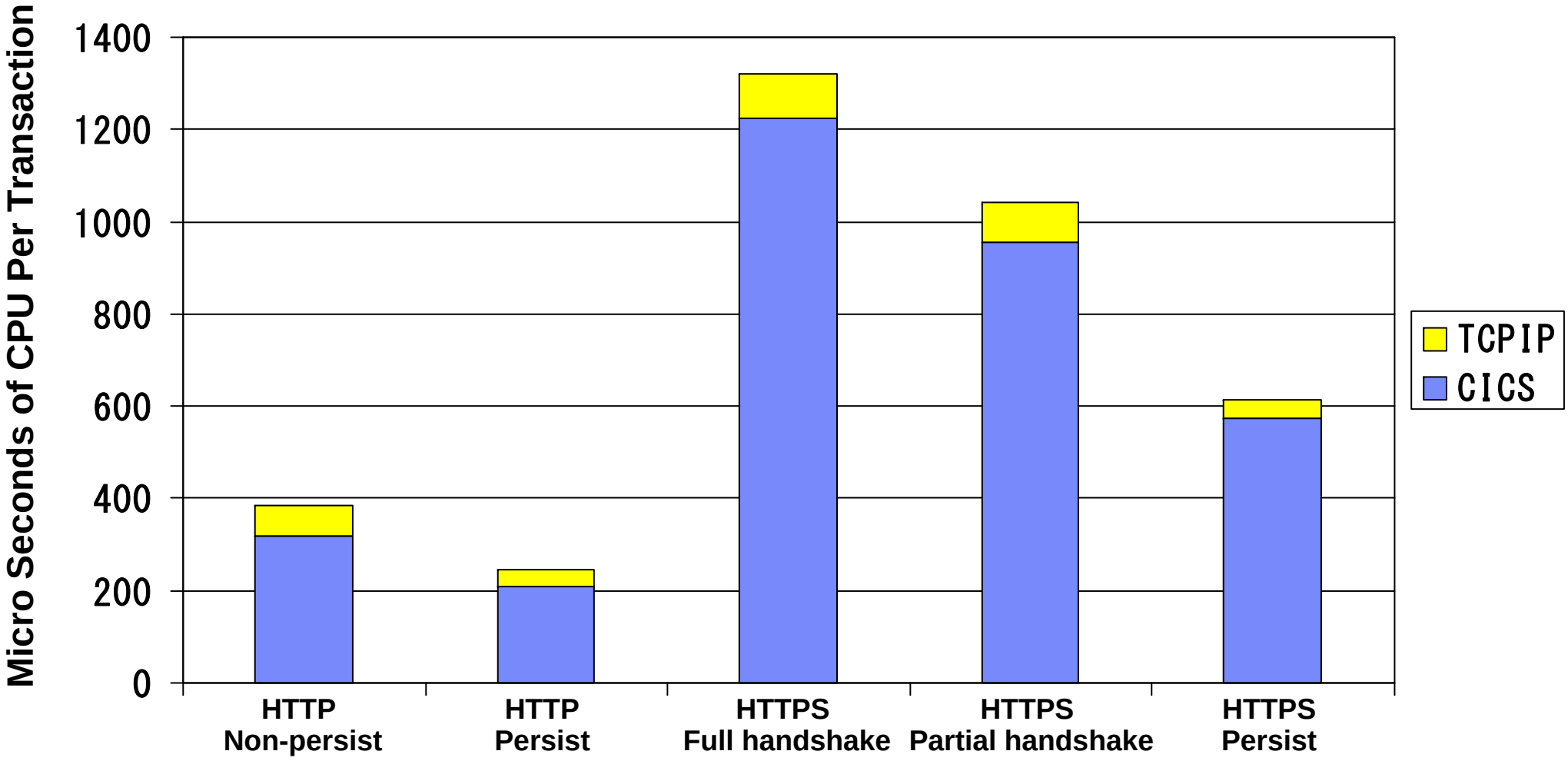
Common challenges to securing access to CICS

- **End-to-end security** is often hampered by the issue of how to provide secure access between middleware components that use disparate security technologies, such as user registries and security token formats

- Often security is at odds with performance, because the most secure techniques require the most processing overhead

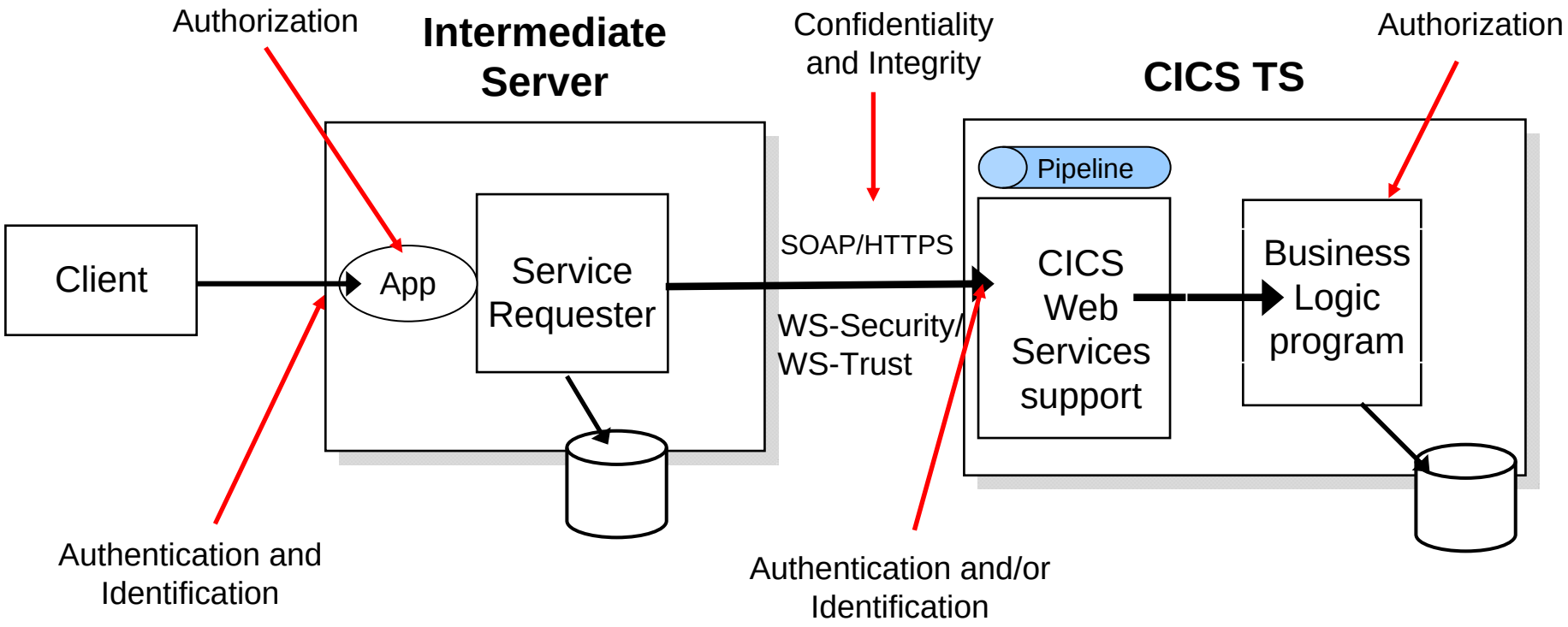
- The range of options is vast and the required skill level is high, both of which can sometimes slow down the implementation

CPU cost comparison (to get 32K bytes of data in/out of CICS)



Tests conducted on a z196 M80 running CICS TS V4.2 and using Triple DES, 168 key length, SHA-1, RSA. This data is planned for publication later this year. Thanks to the CICS Performance team - John Burgess, Graham Rawson and Arndt Eade)

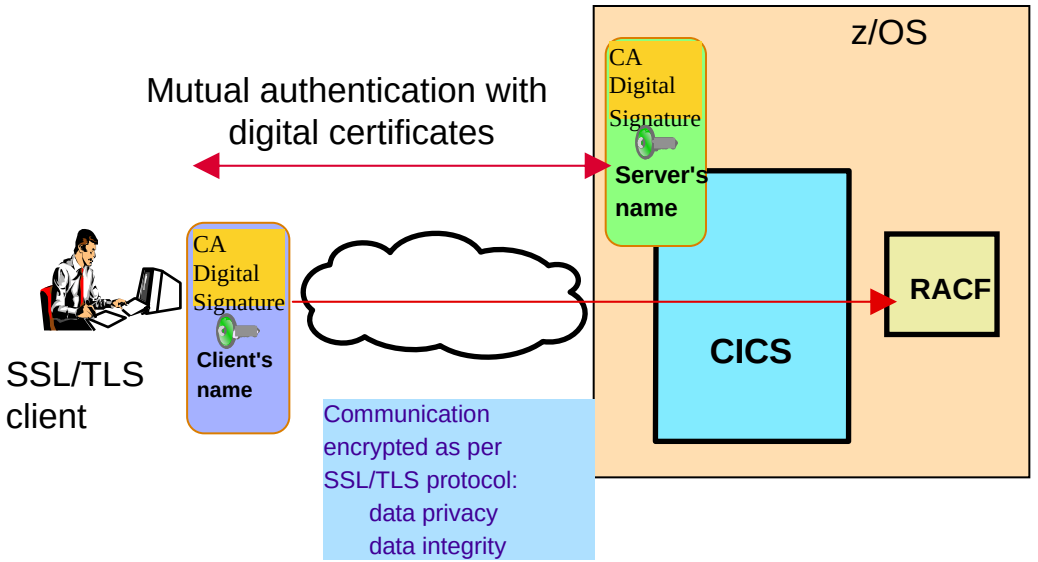
CICS web services security considerations



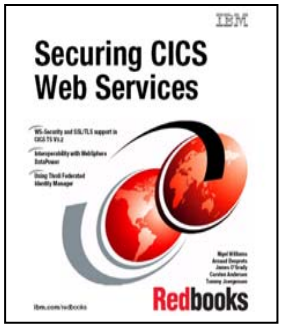
- Transport security alone (e.g SSL/TLS) may be sufficient simple environments
- Message security (WS-Security) can be used for more advanced requirements
- Some security functions can be 'offloaded' to WebSphere DataPower
- z/OS identity propagation is supported
- CICS can interoperate with a Secure Token Service (STS) to provide support for a wide range of security tokens

CICS web services are the most widely adopted CICS feature in the last 10 years

CICS support for SSL/TLS



- CICS uses System SSL to support both the SSL 3.0 and TLS 1.0 protocols
- CICS service provider application can be secured using HTTPS
- CICS service requester application can also use HTTPS
- CICS supports SSL session id reuse
- HTTPS provides
  - **Confidentiality** for the data passed between the service requester and the service provider by using efficient secret key cryptography
  - **Integrity** for the data passed between the service requester and the service provider
  - **Client authentication** through either HTTP basic authentication or a client X.509 certificate
  - **Mutual trust** through exchange of certificates
- It can be used with hardware cryptographic devices when ICSF (Integrated Cryptographic Services Facility) is enabled
- Enabled by SIT parameters and attributes of the **TCPIPService**
- Site certificates can be used to simplify certificate administration
- New **PERFORM SSL REBUILD** command to refresh the certificates used by a CICS region for SSL handshakes



Defining a TCPIPSERVICE for SSL/TLS

```
CEDA  DEFine TCpipservice( TCPIPABC )
   TCpipservice   : S3C1SSL
   GROup          : S3C1
   DEscription  ==> Example TCPIPSERVICE
   Urm          ==> DFHWBADX
   POrtnumber   ==> 20002              1-65535
   STatus       ==> Open               Open ! Closed
   PROtocol     ==> Http               Iiop ! Http ! Eci ! User
   TRansaction  ==> CWXN
   Backlog      ==> 00005              0-32767
   TSqprefix    ==>
   Ipaddress    ==>
   SOcketclose  ==> 000030             No ! 0-240000 (HHMMSS)
   Maxdatalen   ==> 000032             3-524288
 SECURITY
   SSl           ==> Clientauth         Yes ! No ! Clientauth
   Certificate   ==> 'leave blank for default or specify label'
   Ciphers       ==> 0A1613100D05042F30313233
   Authenticate  ==> CERTIFICATE  NO|ASSERTED|AUTOMATIC|AUTOREGISTER|BASIC|CERTIFICATE
```

Mapping cypher codes

Cipher	Algorithm	Key length	Hash	Key exchange	Certificate
04	RC4	128 bits	MD5	RSA	RSA
05	RC4	128 bits	SHA-1	RSA	RSA
0A	Triple DES	168 bits	SHA-1	RSA	RSA
0C	DES	56 bi			
0D	Triple DES	168			
0F	DES	56 bi			
10	Triple DES	168			
12	DES	56 bi			
13	Triple DES	168 bits	SHA-1	ephemeral Diffie-Hellman	DSS
15	DES	56 bits	SHA-1	ephemeral Diffie-Hellman	RSA
16	Triple DES	168 bits	SHA-1	ephemeral Diffie-Hellman	RSA
2F	AES	128 bits			
30	AES	128 bits	SHA-1	fixed Diffie-Hellman	DSS
31	AES	128 bits	SHA-1	fixed Diffie-Hellman	RSA
32	AES	128 bits	SHA-1	ephemeral Diffie-Hellman	DSS
33	AES	128 bits	SHA-1	ephemeral Diffie-Hellman	RSA
35	AES	256 bits	SHA-1	RSA	RSA
36	AES	256 bits	SHA-1	ephemeral Diffie-Hellman	DSS
37	AES	256 bits	SHA-1	ephemeral Diffie-Hellman	RSA
38	AES	256 bits	SHA-1	ephemeral Diffie-Hellman	DSS
39	AES	256 bits	SHA-1	ephemeral Diffie-Hellman	RSA

CICS Sockets Level 1 trace showing cypher and certificate selection

SO 0802 SOSE EXIT - FUNCTION(SECURE_SOC_INIT) RESPONSE(OK)
GSK_RETURN_CODE(0) CERTIFICATE_user ID(**USERWS02**)
CIPHER_SELECTED(**0A**) CIPHER_NAME(**SSL_RSA_WITH_3DES_EDE_CBC_SHA**)

New monitoring fields to list the SSL cipher suite used

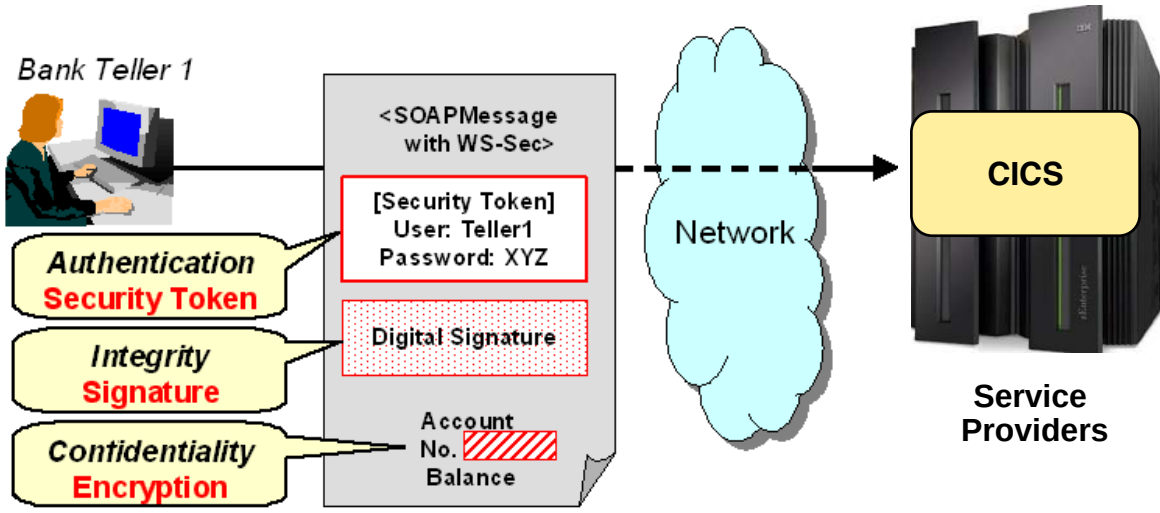
PERFORM SSL REBUILD

- New **PERFORM SSL REBUILD** command
  - via SPI program, CEMT, Web User Interface or CICS Explorer

- The scenarios this changes are:
  - Adding new certificate to a keyring
    - Update the URIMAP or TCPIPSERVICE resource definition with the label name of new certificate
    - Install definition
    - Issue **SSL REBUILD** and CICS will then use new certificate
  - Certificate is about to expire
    - Renew the certificate in the keyring
    - Issue **SSL REBUILD** and CICS will then use new certificate

CICS support for message security

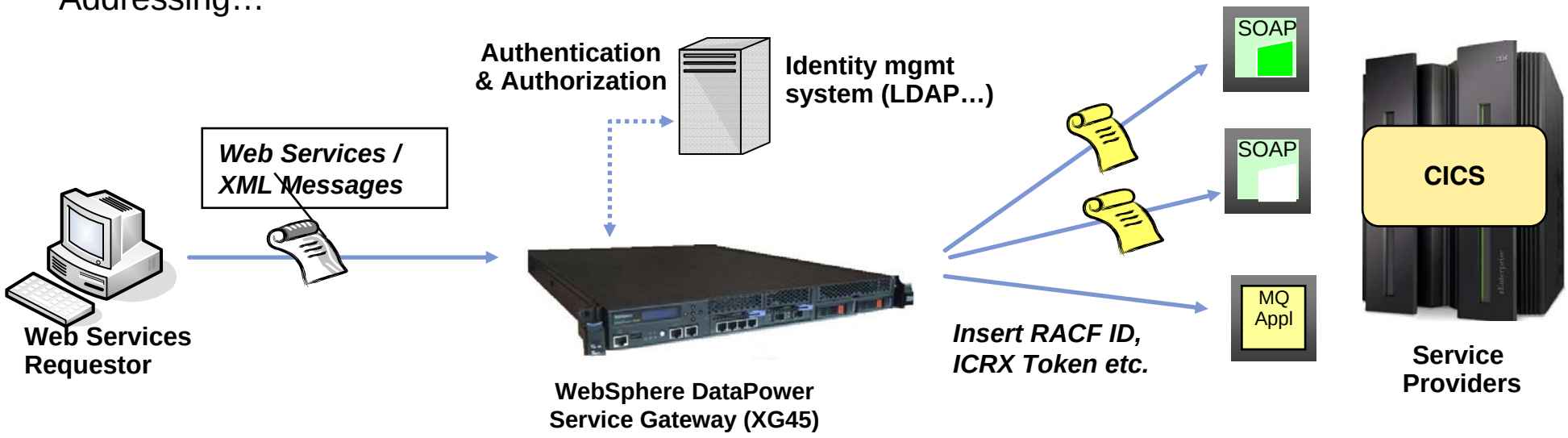
- Various mechanisms for deriving a user ID from an inbound message, including:
  - Basic authentication
  - X.509 certificate
  - Identity assertion
  - Interoperation with a trusted third party



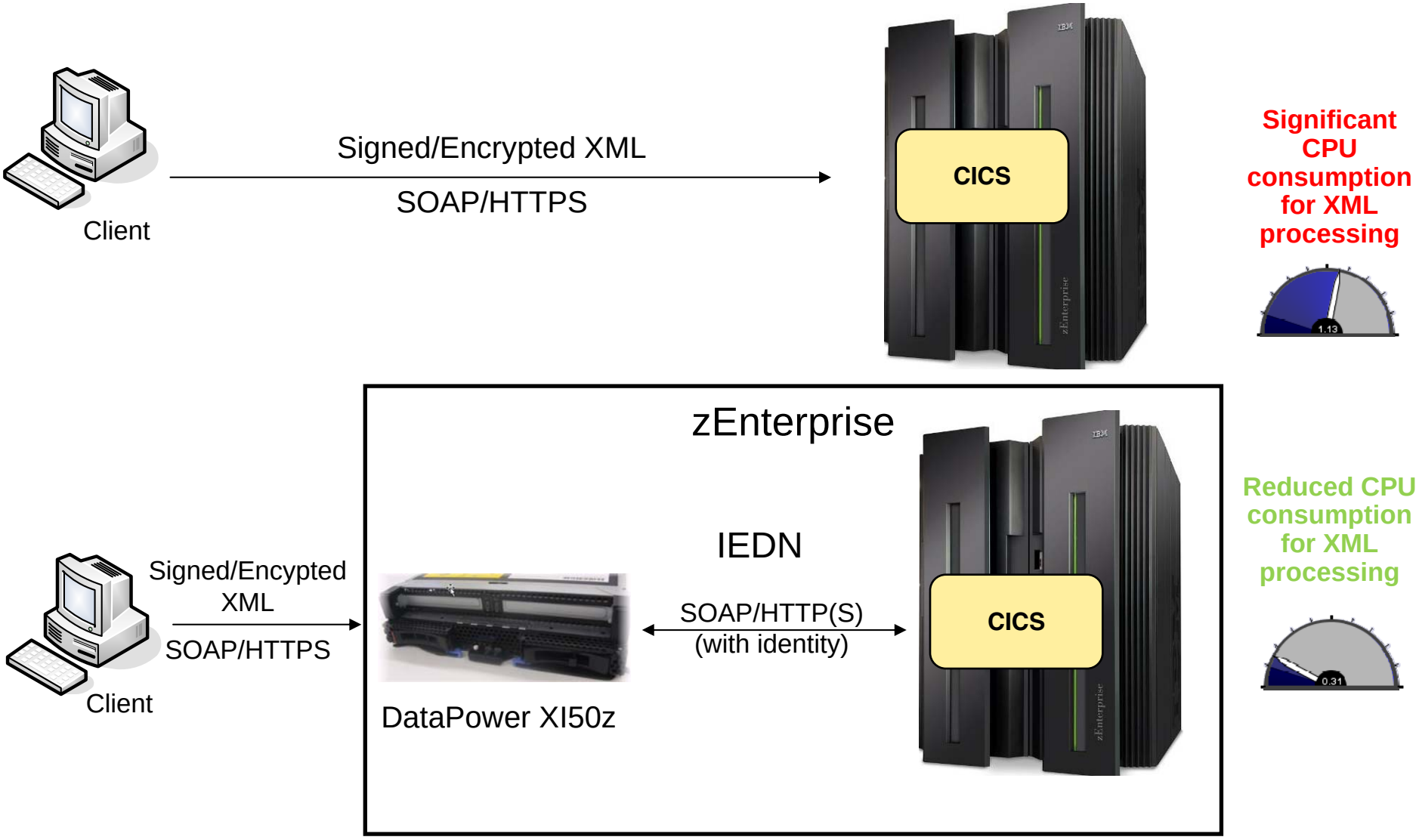
- Various mechanisms for attaching a security token to outbound message, including:
  - X.509 certificate
  - Identity assertion
  - Interoperation with a trusted third party
- Signature **validation** of inbound message signatures and signature **generation** for the SOAP body on outbound messages
- **Decryption** of encrypted data in inbound messages and **encryption** of the SOAP body content on outbound messages
- Enabled by including the <wsse-handler> element in the pipeline configuration file

Using DataPower to secure CICS web services

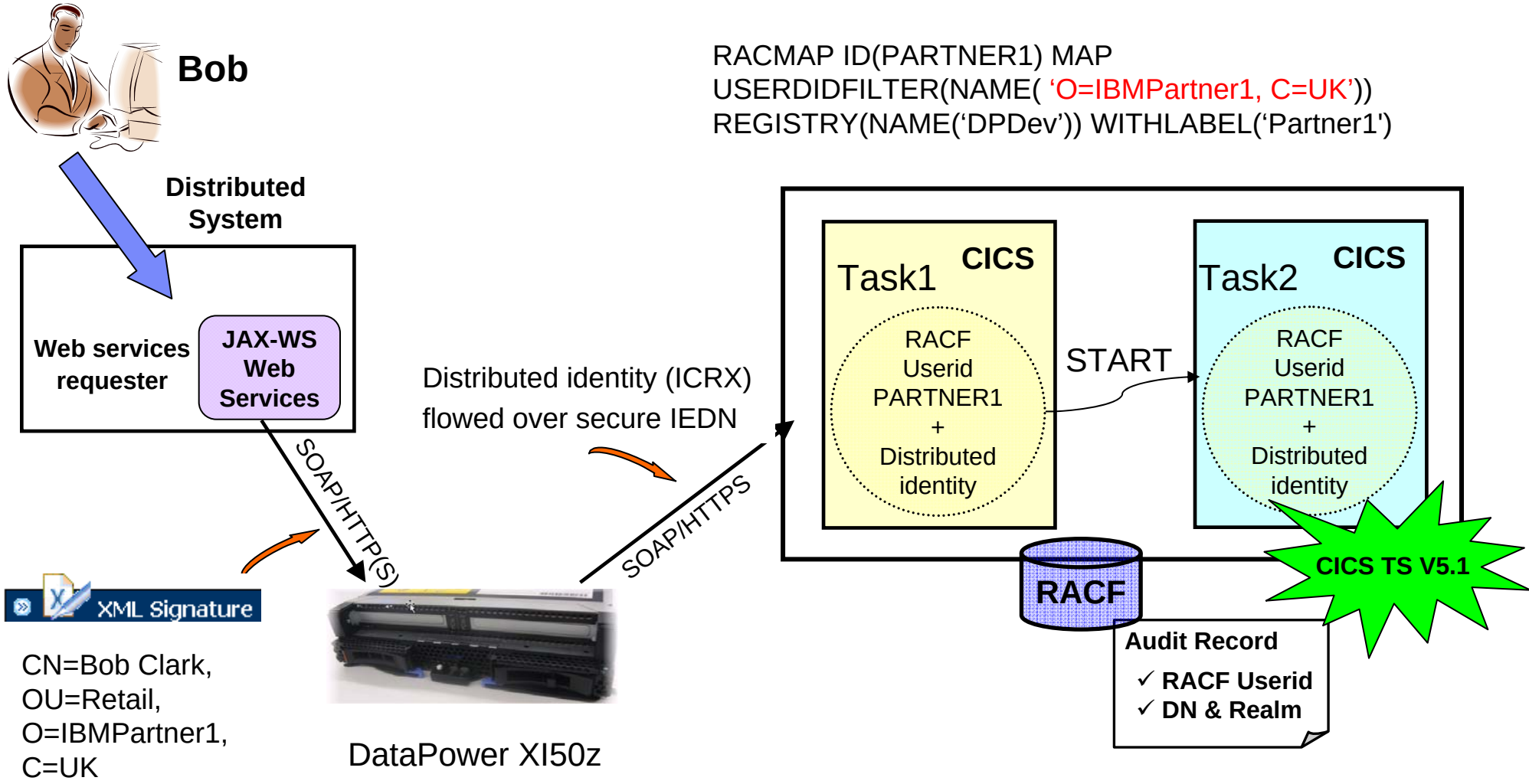
- Encryption of transport layer - HTTP, HTTPS, SSL
- XML/SOAP Firewall - Filter on any content, metadata or network variables
- Data Validation - Approve incoming/outgoing XML
- Field Level Security - WS-Security, encrypt & sign individual fields, non-repudiation
- Access Control (AAA) - enforces access policy stored in an Identity Management Solution
- Message Enrichment – Insert header info, SAML token, Kerberos token, RACF ID, ICRX …
- Anti Virus Protection - integrates with corporate virus checking through ICAP protocol
- Security standards - WS-Security, WS-Policy, SAML, Kerberos, WS-Trust, WS-Addressing…



Why use DataPower to offload security functions?



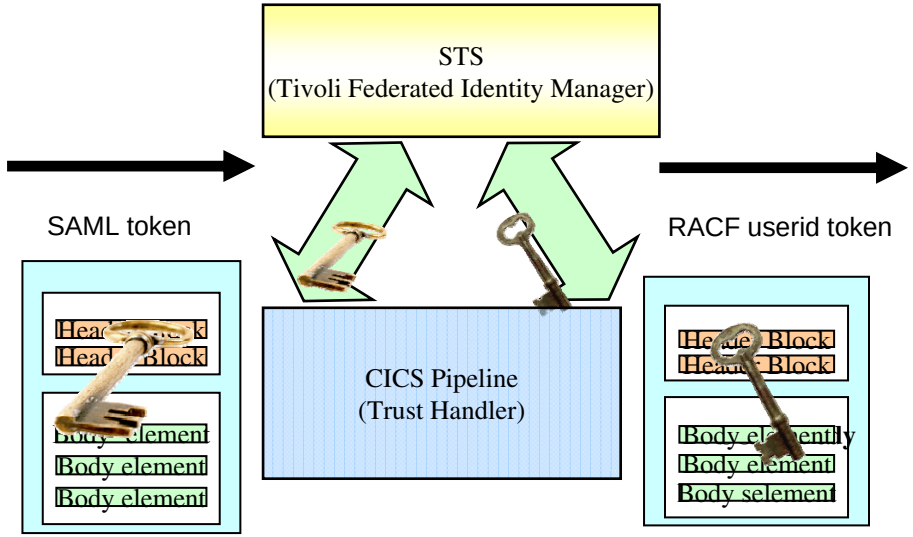
Implementing z/OS identity propagation with CICS web services



ICRX=Identity Context Reference

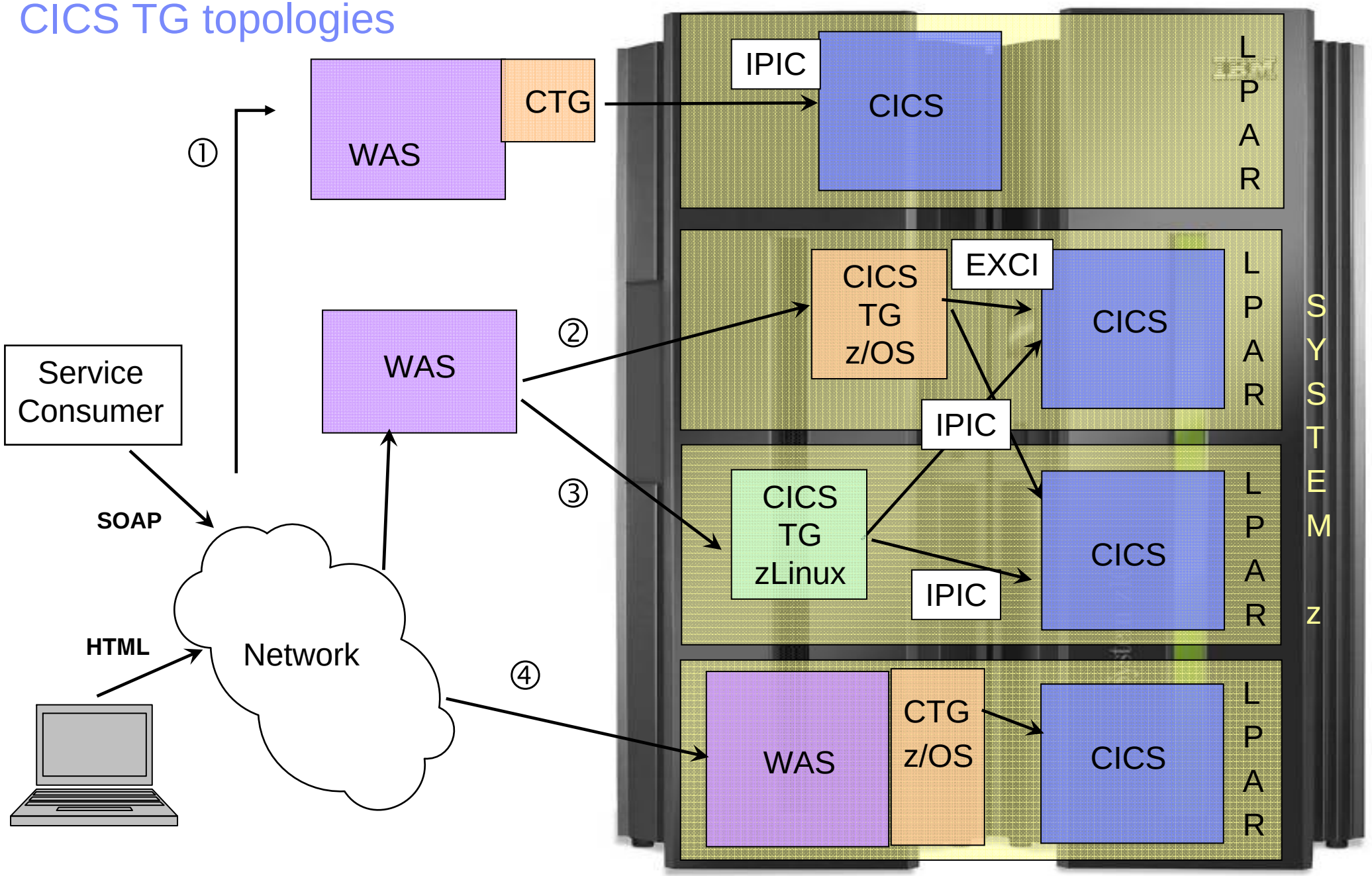
CICS support for WS-Trust

- **WS-Trust** provides a framework for building trust relationships
  - Sender and Receiver in different security domains
  - Security tokens must be vouched for by trusted third party
  - Trusted third party called a Security Token Service (STS)

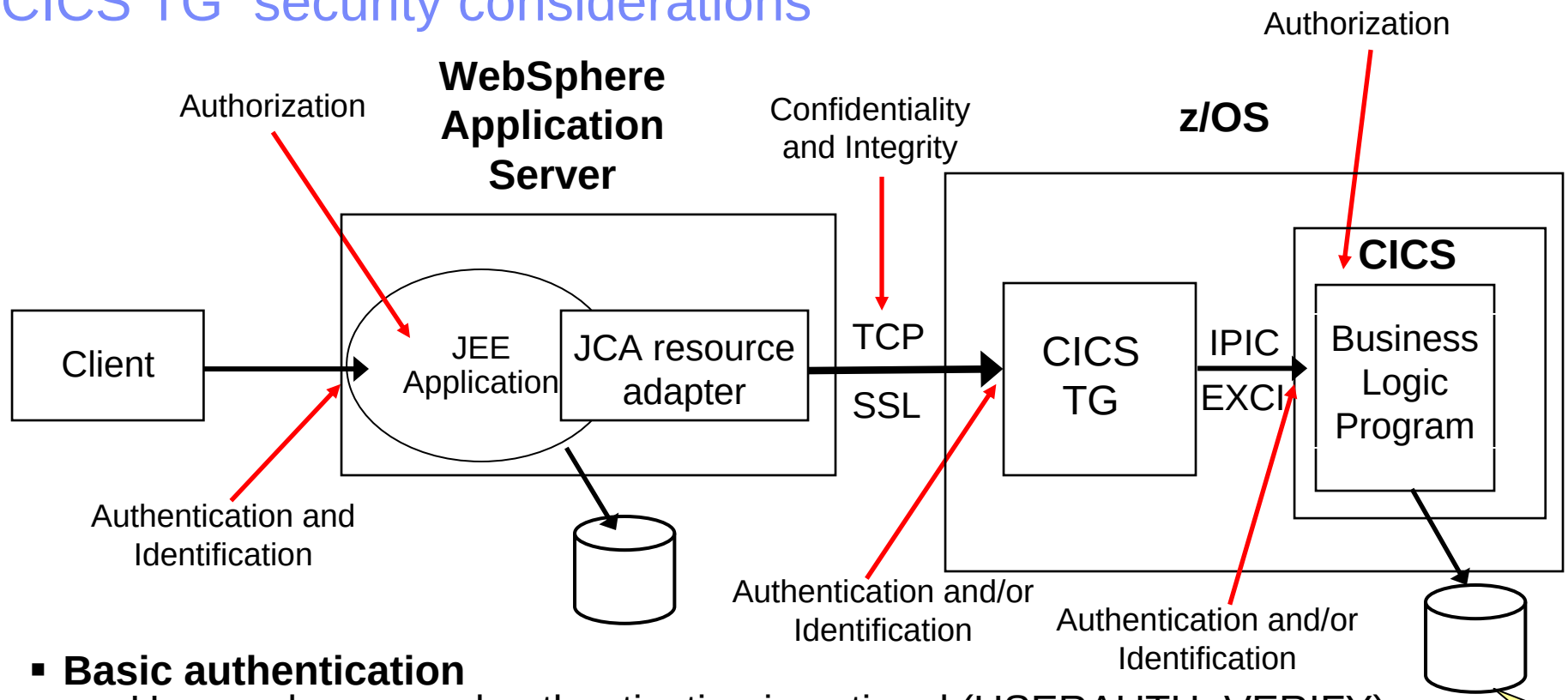


- STS can be used to transform one form of user identification into another form
- **Tivoli Federated Identity Manager** (TFIM) can act as an STS
  - Provides framework to support standards-based, federated identity management between enterprises that have established a trust relationship
- TFIM supports a wide range of security tokens, including SAML, UsernameTokens, Kerberos, LTPA, Passticket and X.509 tokens
- Enabled by including the <wsse-handler> and <sts_authentication> elements in the CICS Web services pipeline configuration file

CICS TG topologies



CICS TG security considerations



- **Basic authentication**
  - User and password authentication is optional (USERAUTH=VERIFY)
  - Pass phrase support available when IPIC connection is used
  - Pass phrase also available when EXCI connection is used (CICS TG V9.0)

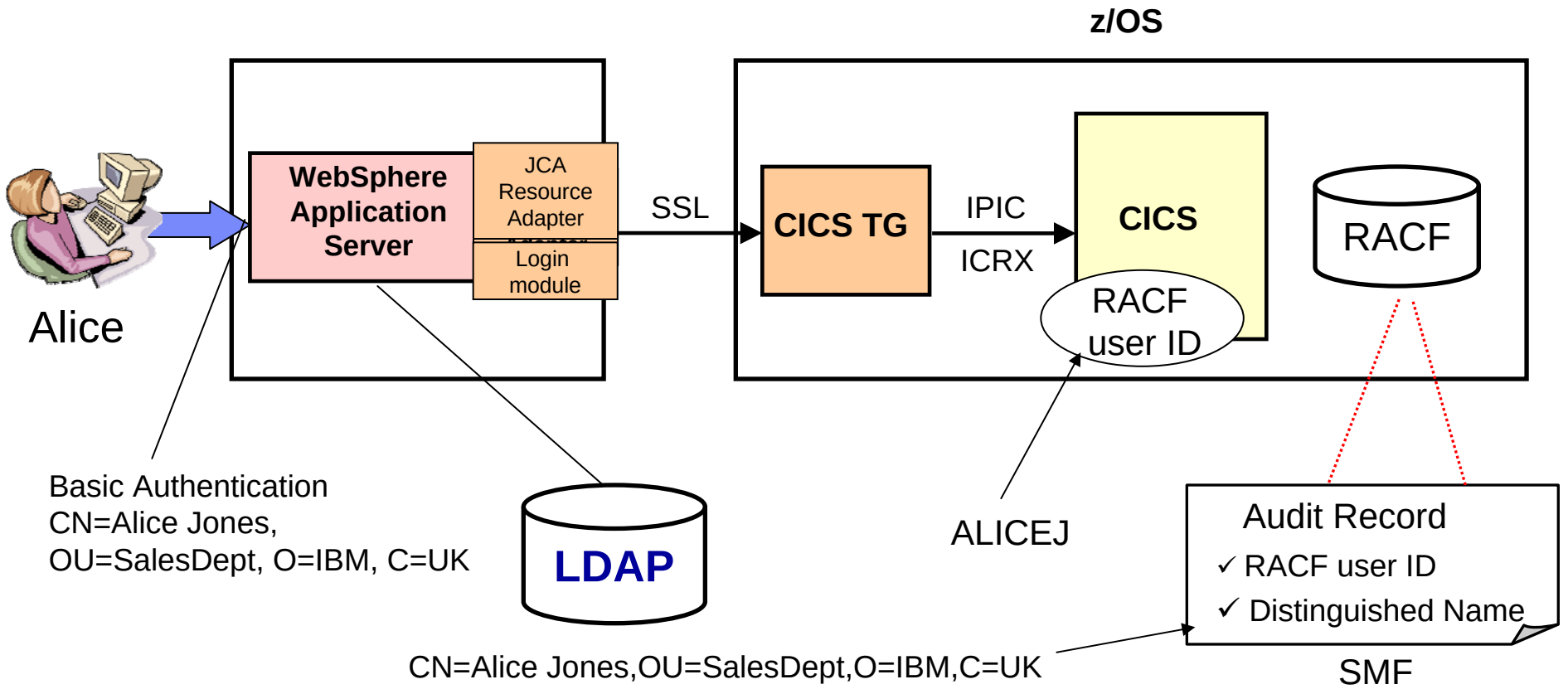
CICS TG V9.0

- **Identity assertion is a common model**
  - User authenticates with WebSphere Application Server
  - RACF identity is asserted to CICS TG and CICS (USERAUTH=IDENTIFY)
  - Trust should be established between servers
- **z/OS identity propagation is supported**
- **CICS TG supports SSL/TLS based on JSSE**
  - IPIC connection from CICS TG V9.0 daemon to CICS supports SSL/TLS

CICS TG V9.0

Implementing z/OS identity propagation with CICS TG

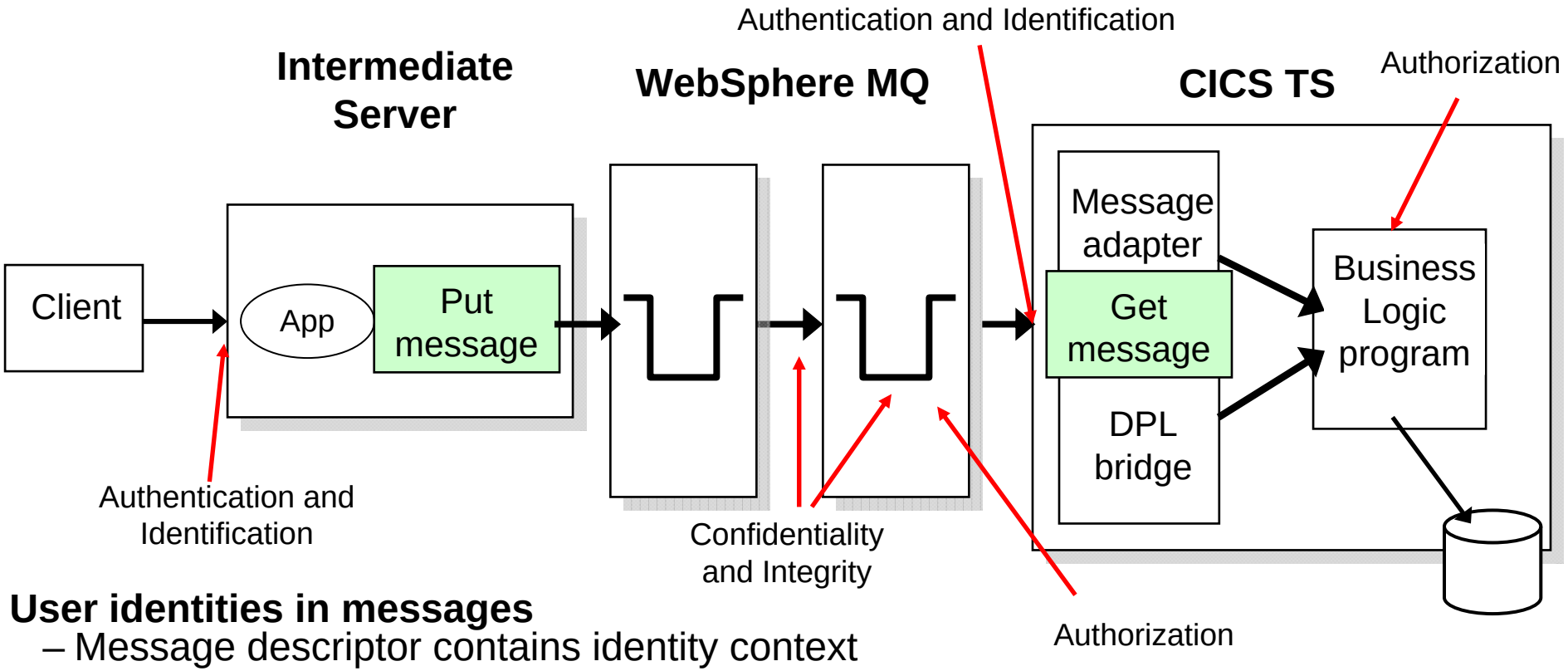
RACMAP ID(ALICEJ) MAP USERDIDFILTER(NAME('CN=Alice Jones, OU=SalesDept,O=IBM,C=UK')) REGISTRY(NAME('ldaps://myldap.uk.ibm.com')) WITHLABEL('Alice')



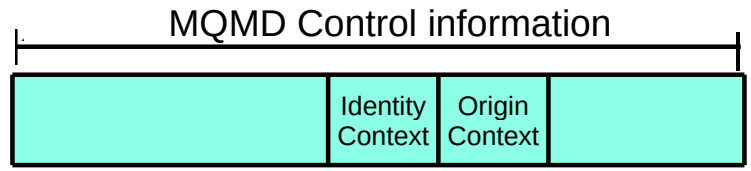
Note: CICS TG V9.0 introduces z/OS identity propagation support for remote connections to CICS TG daemon running on a non-z/OS platform

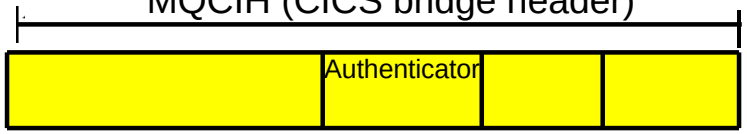
CICS TG V9.0

CICS and WebSphere MQ security considerations

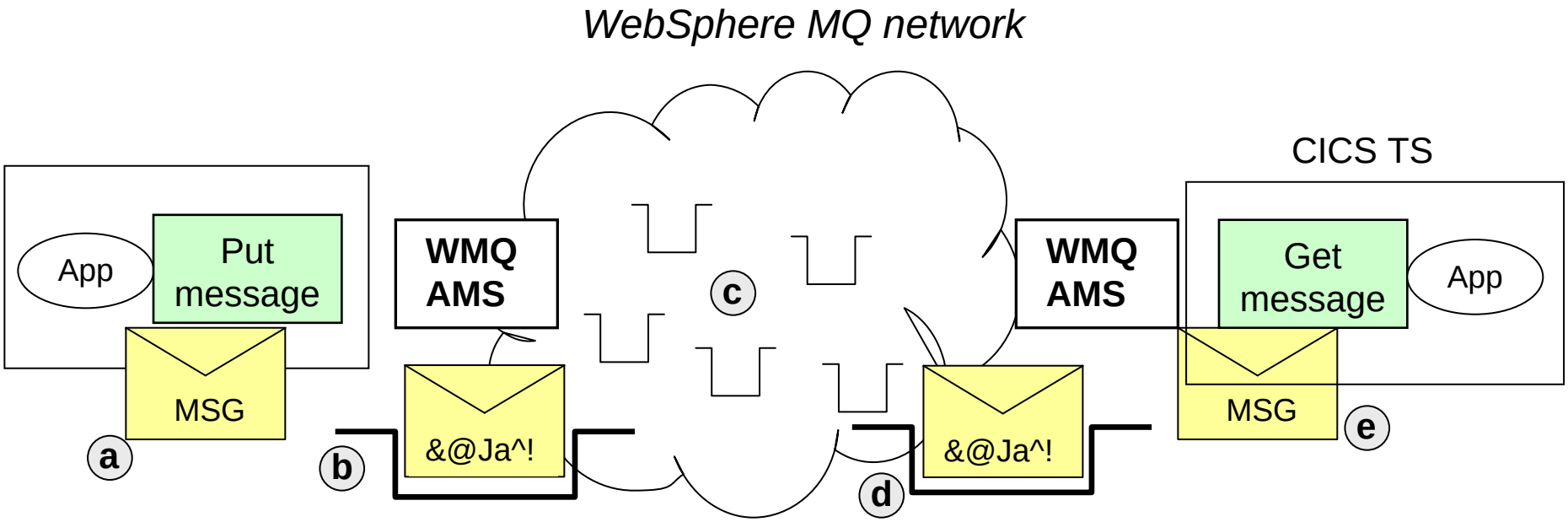


- **User identities in messages**
  - Message descriptor contains identity context
- **Securing access to WMQ resources**
  - User ids associated with task and CICS region id are checked
- **CICS DPL bridge**
  - Additional options to control authentication
- **SSL/TLS support**
  - Between queue managers
- **WMQ Advanced Message Security**
  - End-to-end confidentiality





WMQ Advanced Message Security

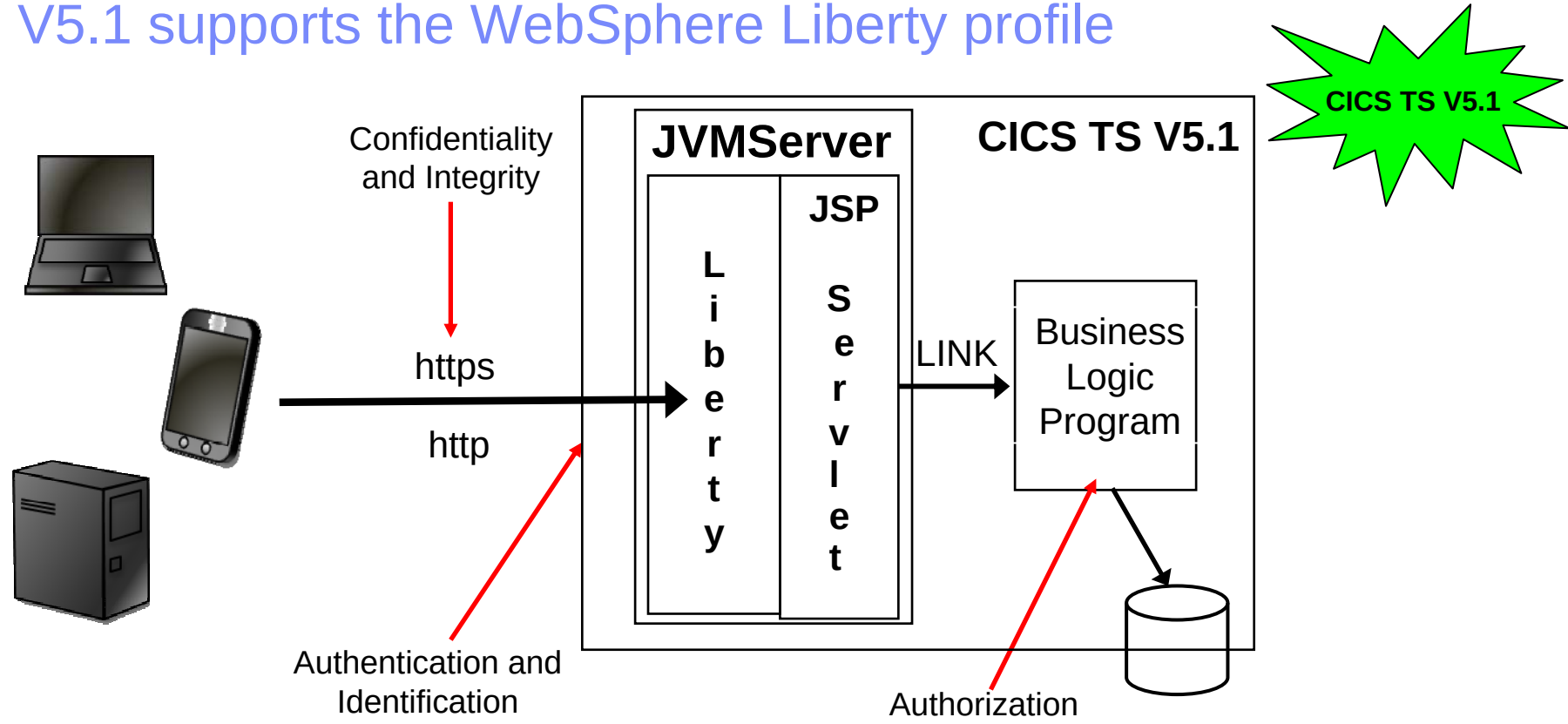


1. Sender application uses MQPUT API to put a message to a queue
2. MQPUT is intercepted by a security exit and signing/encrypting policy is applied by WMQ AMS client interceptor
3. Signed and encrypted message is transmitted across the WMQ network
4. Receiver application uses MQGET API to get the message from queue
5. WMQ AMS client interceptor performs signature checking and decryption as specified by the queue's data-protection policy, and then returns the original message to the calling application

Security options table

	CICS Web services	CICS TG	WebSphere MQ
Basic authentication	Supported	Supported	Supported
Identity assertion	Supported	Supported	Supported
z/OS Identity Propagation	Supported	Supported	Not supported
SSL/TLS	Supported	Supported	Supported
Message security	Supported	Not supported	Supported with WMQ AMS

CICS TS V5.1 supports the WebSphere Liberty profile



- **Authentication**
  - User and password authentication is optional (specified in cicsSecurity.xml file)
- **Confidentiality/integrity**
  - Supports SSL/TLS based on JSSE
  - Server authentication only
- **Authorization**
  - Default transaction CJSA can be switched using URIMAP so you can use different transactions to authorize different sets of users based on URI
- **Multiple servlet requests, as part of an application, take advantage of SSO (single sign-on)**

Summary

- Different business and technology trends are driving more and more integration with CICS applications
- Lots of options for securing access to and from CICS
- Start with a well defined set of security requirements

- Options exist for true end-to-end security
- Often need to optimize chosen solution in order to minimize impact on performance

Copyright Information