



IBM Software Group

End to end security for WebSphere MQ

An Introduction to WebSphere MQ Extended Security Edition

Saad BENACHI (saad.benachi@fr.ibm.com) basée sur une pres de
Mark Hiscock (mark.hiscock@uk.ibm.com)

Tivoli software

WebSphere software

Agenda

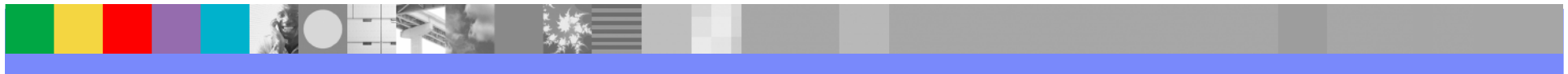
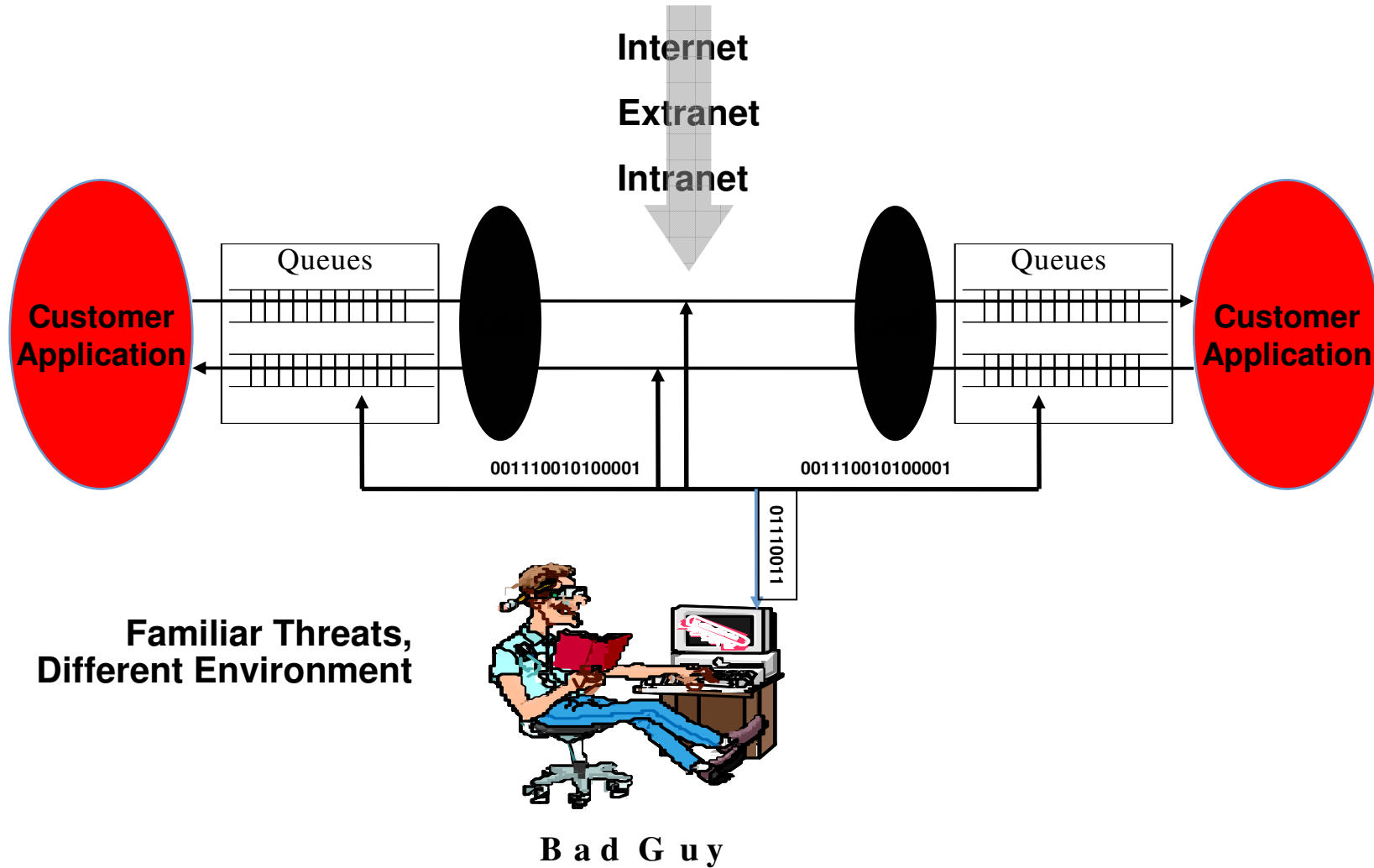
- Problem statement
- Introduction and product overview
- Architecture review
- Implementation details
- Product administration
- Conclusion



Robbing the bank - yesterday



Robbing the bank – today



Controlling access to data - What organisations want

- **A**uthorisation /Control
- **A**uthentication
- Integrity
- Privacy
- **A**udit trail
- Centrally managed
- Availability



What do we need for MQ?

To provide end to end security for the MQ network

AAA

- ▶ **Authentication** of users into the network
- ▶ **Authorisation** of their access to queues / queue managers
 - Can't access messages you are not authorised to
- ▶ Keeping an **Audit** trail of which queues have been accessed and by whom

Protect message payloads

- ▶ When messages are on queues or in transit
- ▶ Do not allow message data to be tampered with
- ▶ Know without a doubt, the sender of a message

Centrally managed



What WMQ Provides Today

- Users are based on Operating System ID
 - ▶ Users are unique to machines and not across the enterprise
 - ▶ No passwords are used for authorisation
 - ▶ Not 100% secure

- SSL channels
 - ▶ Protects messages in transit
 - ▶ Messages at rest are in the clear

- Object Authority Manager (OAM) / RACF limits access to resources
 - ▶ OAM is on a per machine basis, hard to administer a large network
 - ▶ RACF applies to a single sysplex



What WMQ ESE Provides beyond WMQ

- Authentication
 - ▶ PKI approach to uniquely identify users
 - ▶ Users are stored in a LDAP repository and map onto certificates

- Authorisation
 - ▶ Users can be granted or denied access to put and get to queues
 - ▶ Users can be granted access to client connect to the queue manager
 - ▶ Policies centrally managed

- Auditing
 - ▶ User access to queues can be audited
 - ▶ The user, object name and success or failure of the access attempt are logged



Other WMQ ESE Benefits

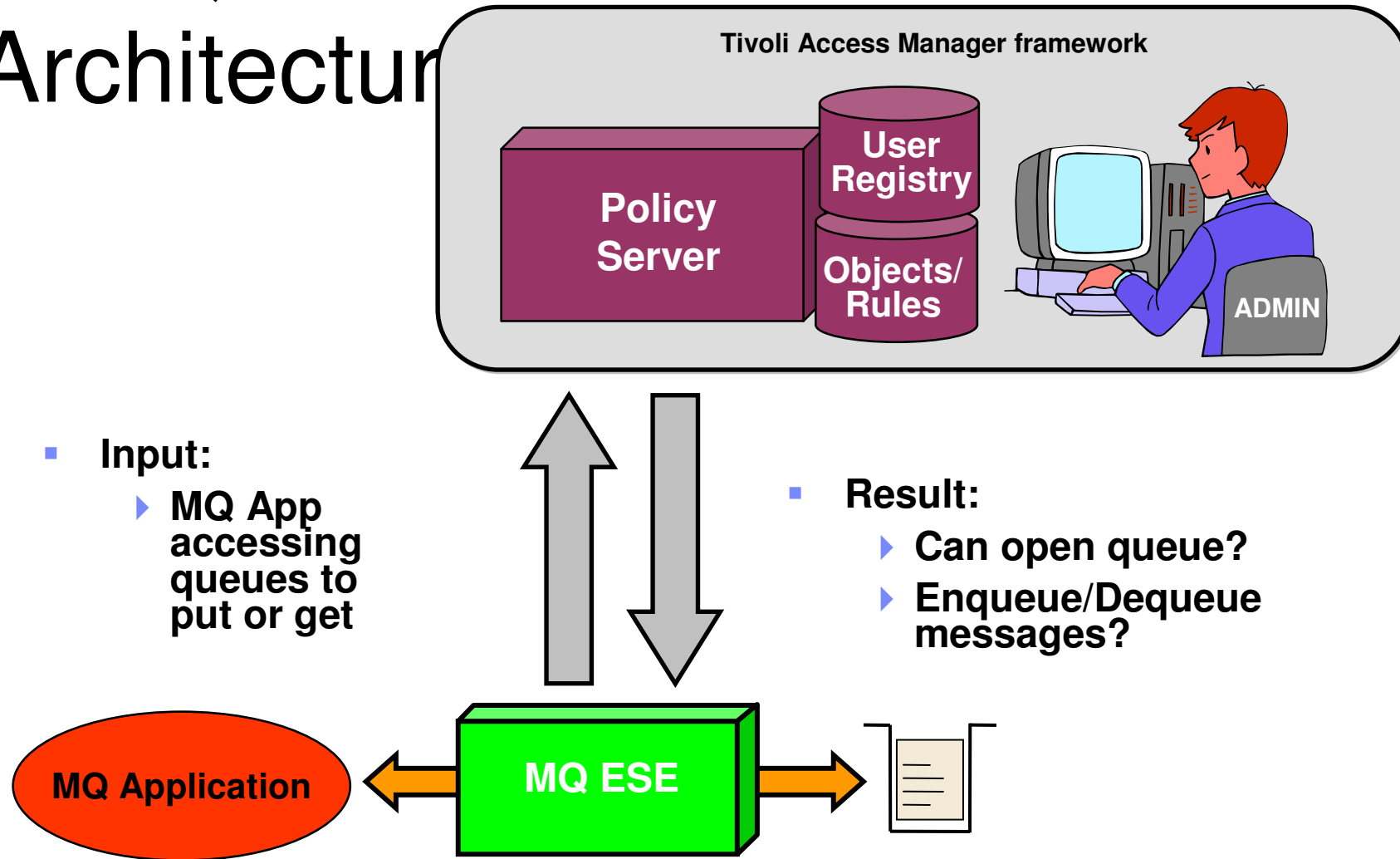
- Message protection
 - ▶ Users are based on certificates making them unique across enterprises
 - ▶ Sign messages
 - Tells us who the message came from
 - Ensures that the message hasn't been tampered with
 - ▶ Can encrypt the message payload for end-to-end security
 - Messages protected on the queues

- Addresses audit and other requirements of Sarbanes-Oxley

- Central Administration
 - ▶ WMQ security policies, users, groups and audit levels are centrally managed
 - ▶ GUI or command line interfaces

WMQ ESE Architecture

WMQ ESE Architecture

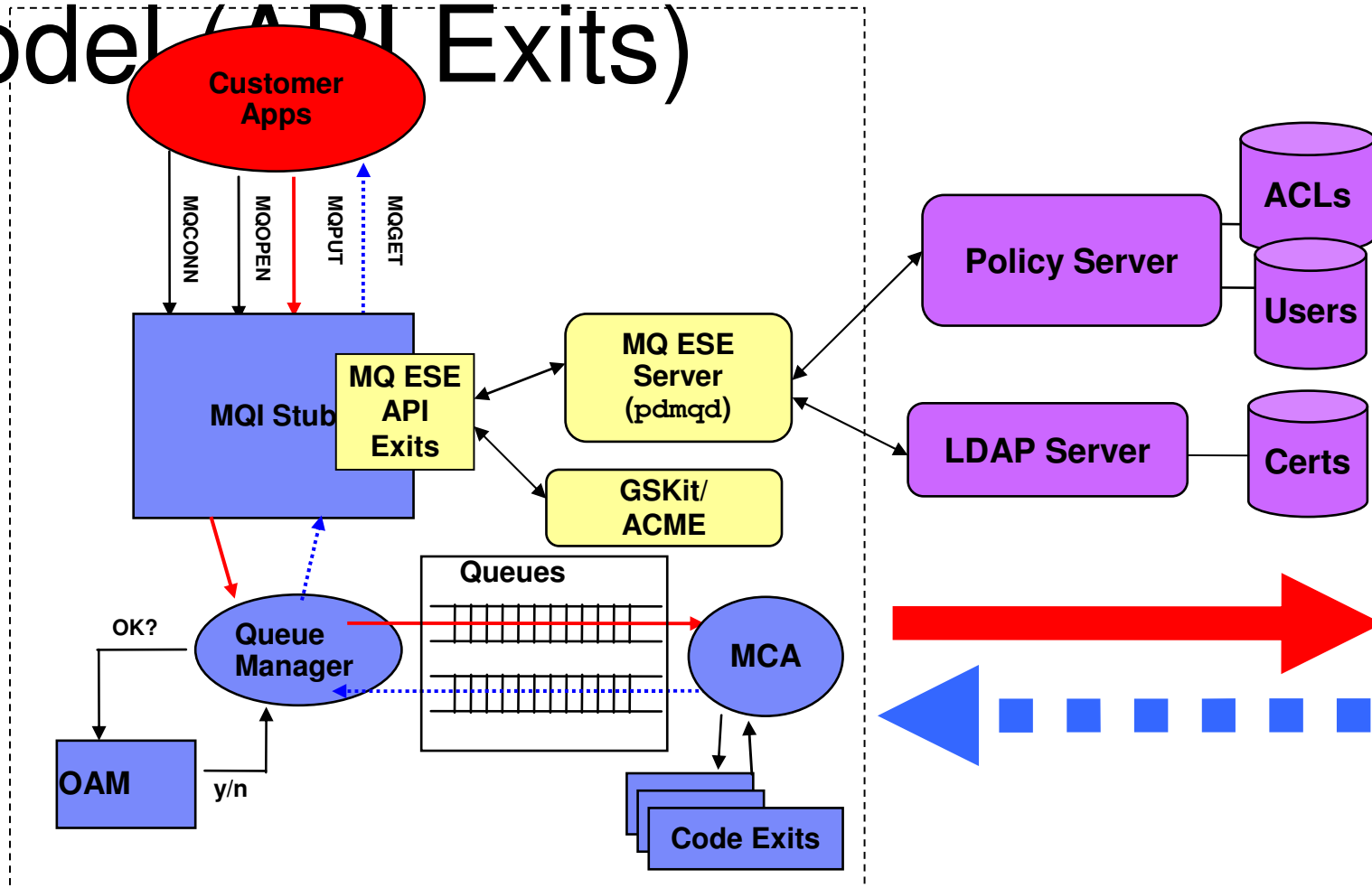


Methods of interception

- WMQ ESE needs to intercept the application API calls to subject them to security

- The different interfaces are:
 1. WMQ applications binding locally to a distributed queue manager
 2. WMQ applications binding to a z/OS queue manager
 3. WMQ Client and JMS applications client side interception
 4. WMQ Client and JMS applications server side interception

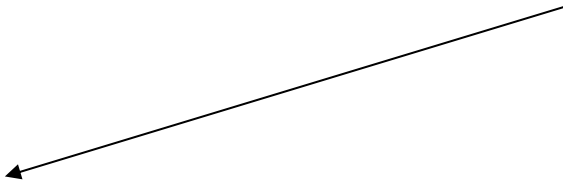
1. Distributed server interceptor model (API Exits)



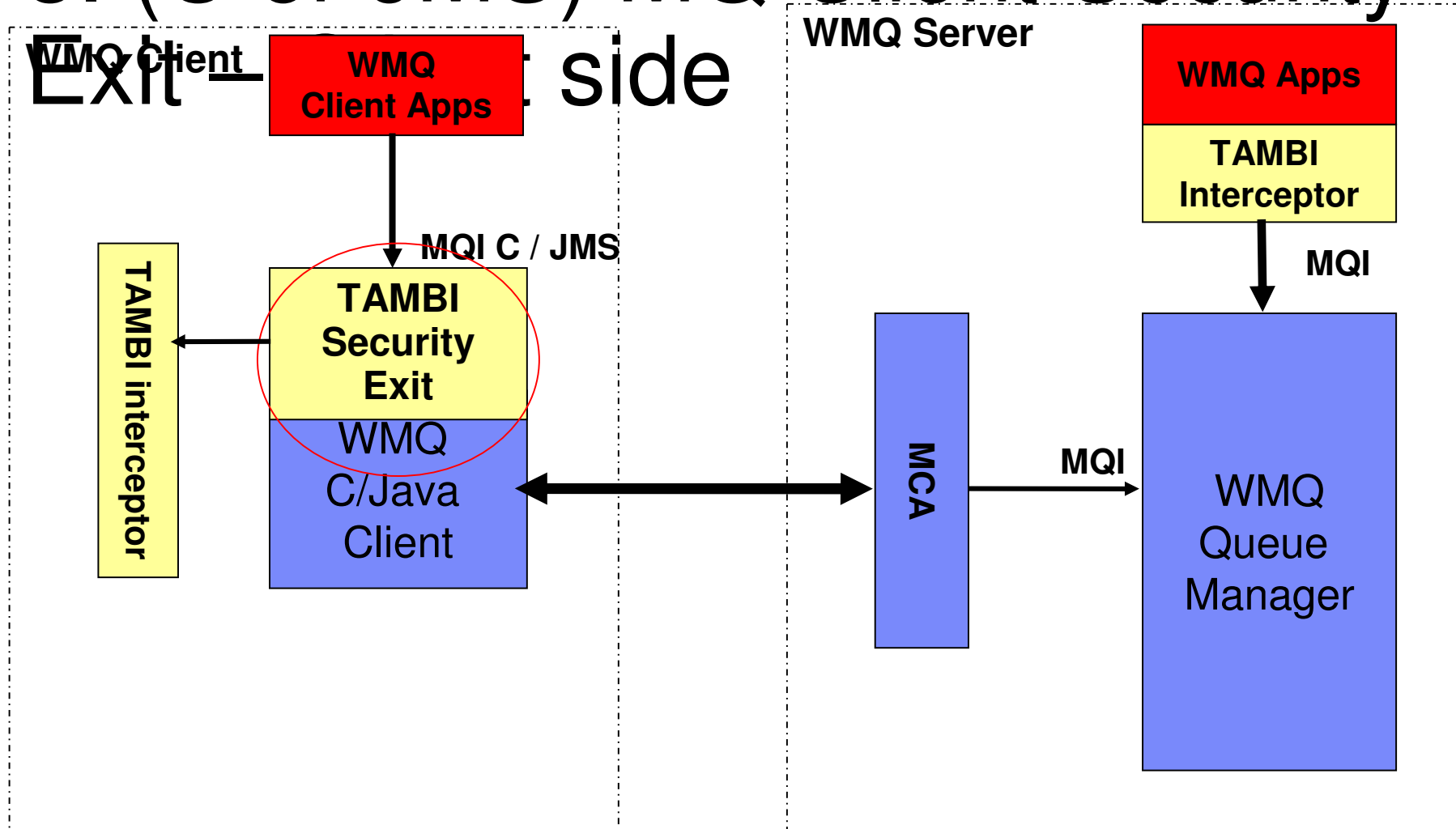
2. z/OS server interceptor model

```
//CL00PUT JOB 1,MSGCLASS=H
//*
// EXEC PGM=OEMPUTX,REGION=0M,
// PARM=('-mVCT7 -N1. -X -clear -pm -s12 ')
//SYSIN DD *
-QCLASS00_NONE
-FILEDD:MSGIN
//STEPLIB DD DISP=SHR,DSN=PP.ACCMAN.V4R1.SDRQAUTH
//          DD DSN=PUBVIC.V531.SCSQAUTH,DISP=SHR
//          DD DSN=PUBVIC.V531.SCSQANLE,DISP=SHR
//          DD DISP=SHR,DSN=PAICE.IP13.LOAD
//MSGIN DD DISP=SHR,DSN=CLASS00.TAMBI.MSGDATA(HELLO)
//SYSPRINT DD SYSOUT=*
```

Add TAMBI as the first library to load

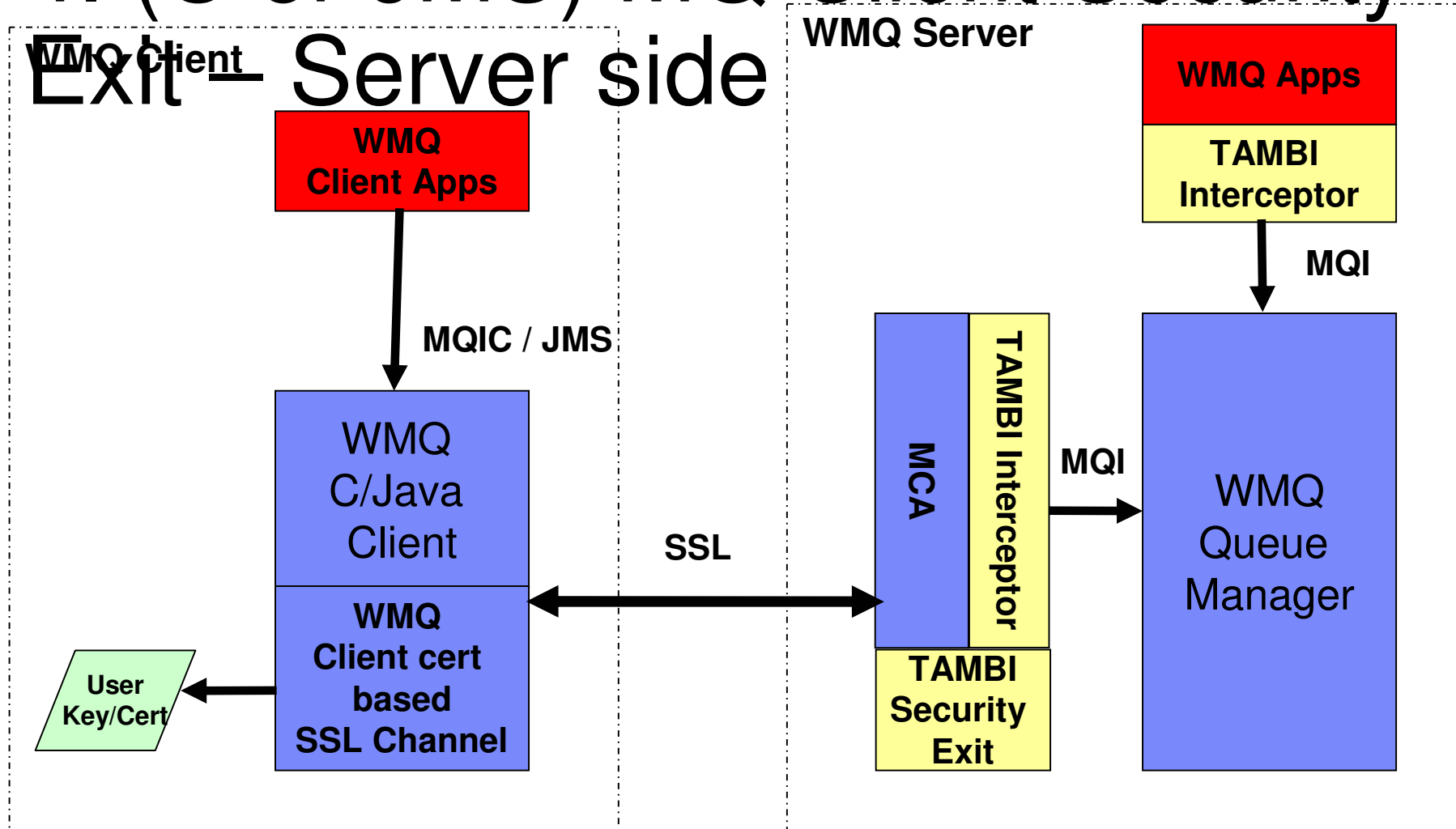


3. (C or JMS) MQ Client Security



“R” = new permission bit to allow/deny connection

4. (C or JMS) MQ Client Security



“R” = new permission bit to allow/deny connection

WMQ ESE Administration

Interfaces for Administrators

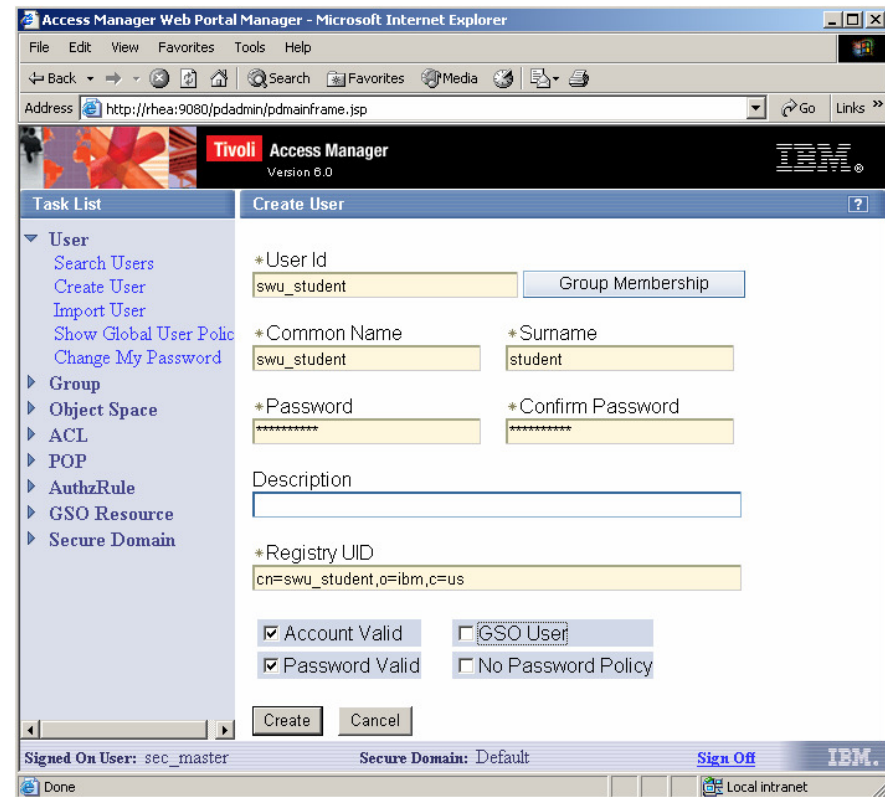
- Command line interface
- Web Based GUI interface

```
pdadmin
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\mhiscock>pdadmin -a sec_master -p Secure99
pdadmin sec_master> object show /PDMQ/Queue/UCT?
Name: /PDMQ/Queue/UCT?
Description: Queue Manager UCT?
Type: 13 (Unknown)
Is Policy Attachable: Yes
Extended Attributes
Name: Error-handling-Q
Value(s): PDMQ.DEAD.LETTER.QUEUE
Attached ACL: PDMQ_all_ED
Attached POP: PDMQ_integrity_all
Attached AuthzRule:

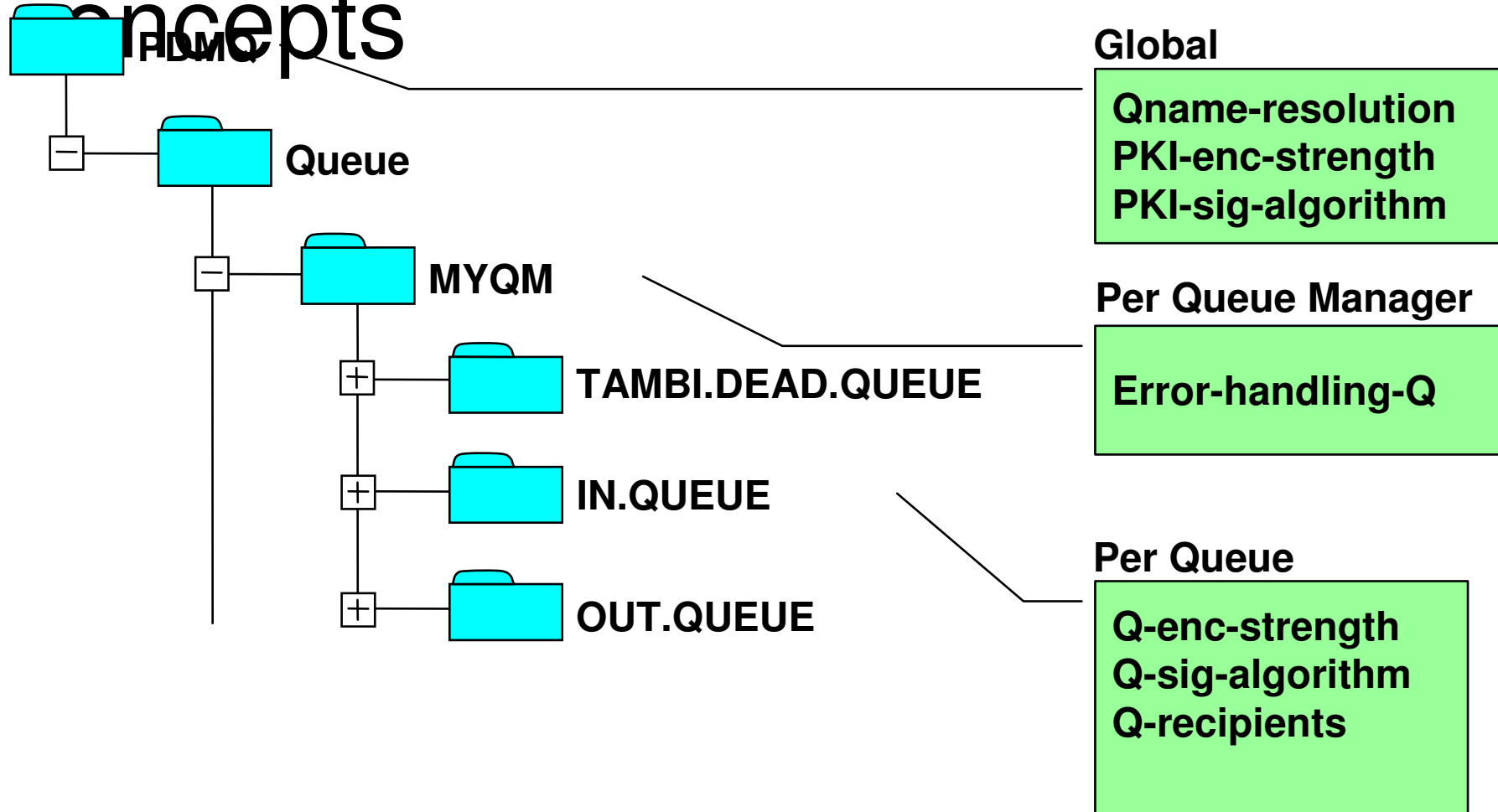
Effective Extended Attributes
Protected Object Location: /PDMQ/Queue/UCT?
Name: Error-handling-Q
Value(s): PDMQ.DEAD.LETTER.QUEUE
Effective ACL: PDMQ_all_ED
Effective POP: PDMQ_integrity_all
Effective AuthzRule:

pdadmin sec_master>
```



Policy Server

Concepts



Access Control Lists -

- (ACL)
- E → Grant Put Permission
 - ▶ Application can place messages onto the queue
 - ▶ ACL checked on MQOPEN (in PUT mode)
 - D → Grant Get Permission
 - ▶ Application can retrieve messages from the queue
 - ▶ ACL checked on MQOPEN (in GET mode)
 - R → User is allowed to connect to the queue manager remotely

	Type	ID	Permissions
ACL Entry	User	jon	Trx
	Group	sales	Trm[PDMQ]E
	Group	admin	Trxmcd[PDMQ]DE
	Any-other		Tr
	Unauthenticated		T

Protected Object Policies – (POP)

- POPs specify the security policy for a queue or queue manager:
 - The security for messages put to the queue
 - None – message is sent as normal
 - Integrity – Message is digitally signed by the sender
 - Encrypt – Message is signed and encrypted by the sender
 - The time of day that the object can be accessed
 - The audit level for the queue (none, permit, deny, error, admin)



Auditing

- Events recorded when specified auditable events occur at: MQOPEN, MQPUT, MQPUT1, MQGET, MQCLOSE
- Auditing Options allow different levels of detail to be logged:
 - **permit:** Records only successful accesses
 - **deny:** Records only denied requests for access
 - **admin:** Records OPEN, CLOSE, PUT, and GET operations on protected WMQ queues
 - **error:** Records any unsuccessful GET operations
- Audit records stored as XML on distributed and SMF on z/OS
- Audit Records Include:
 - AM User ID, WMQ Message ID
 - Sender PKI ID (if message signed)
 - Date and Time
 - Encryption and Signing algorithms

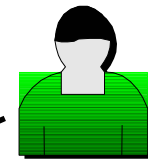


WMQ ESE Auditing

Audit Level: Permit Deny Error Admin

```

<event rev="1.2">
<date>2005-11-07-23:25:25.296-05:00I-----</date>
<outcome status="0">0</outcome>
<originator blade="ivadminapi"><component rev="0.1">pdmq</component>
<action>0</action>
<location>dropzone</location>
</originator>
<accessor name="mq_pki_ldap">
<principal auth="IV_LDAP_V3.0" domain="Default">jdement</principal>
</accessor>
<target resource="0"><object>/PDMQ/Queue/QM_dropzone/JEFF</object></target>
<data>
<data tag="action">MQOPEN</data>
<data tag="operation">E</data>
<data tag="result">access denied or azn check failed</data>
<data tag="qop">integrity</data>
<data tag="ProcessId">3456</data>
</data>
</event>
    
```



Use	jon	Trx
Group	admin	Trxmcd[PDMQ]DE
Any-other		Tr
Unauthenticated		T

Quality of Protection: Integrity

- None
- Integrity
- Privacy

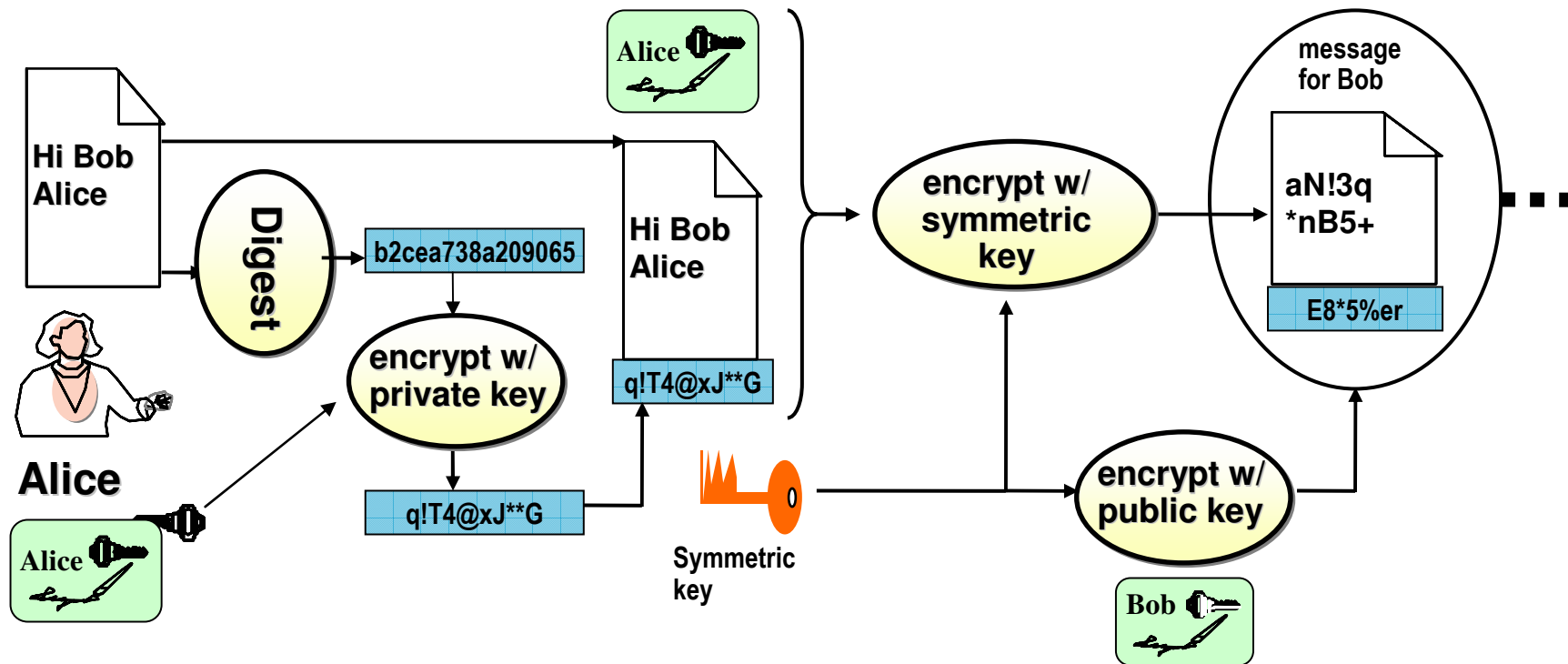
Summary

- WMQ data needs to be protected at rest and in flight
- No need to update or modify existing deployed WMQ applications.
 - ▶ ESE is transparent
- Centralised administration of both access control to queues, data protection and security audit policies
- WMQ ESE provides end to end security for WMQ networks

THANK
YOU

Public Private Key Cryptography

Cryptography explained – slide 1



Cryptography explained - slide 2

