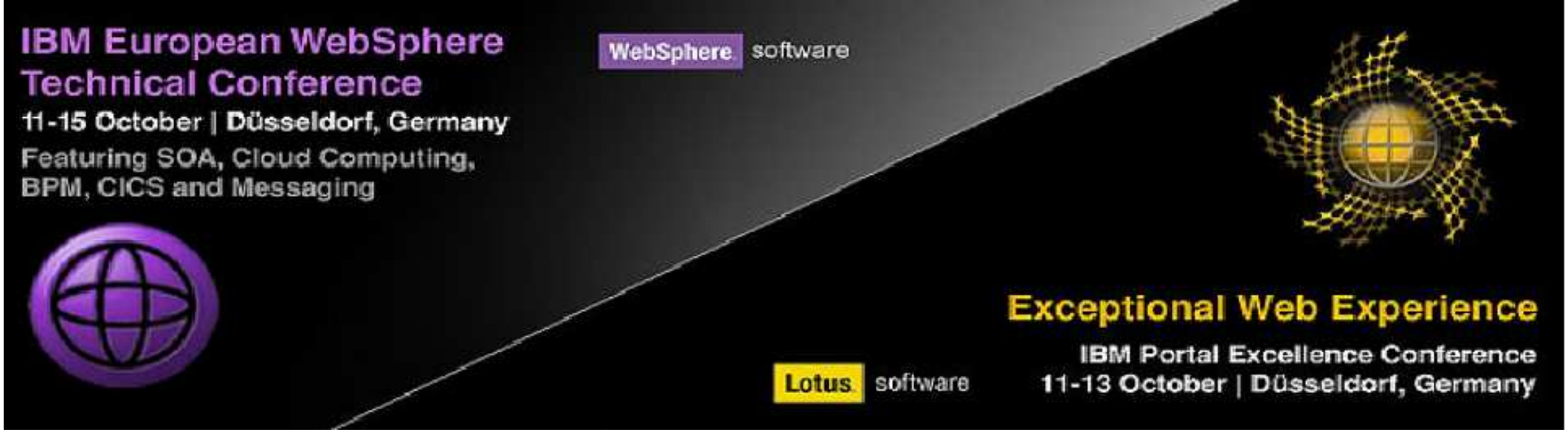


End to end security for WebSphere MQ

An Introduction to WebSphere MQ Advanced Message Security

T.Rob Wyatt
(t.rob.wyatt@us.ibm.com)

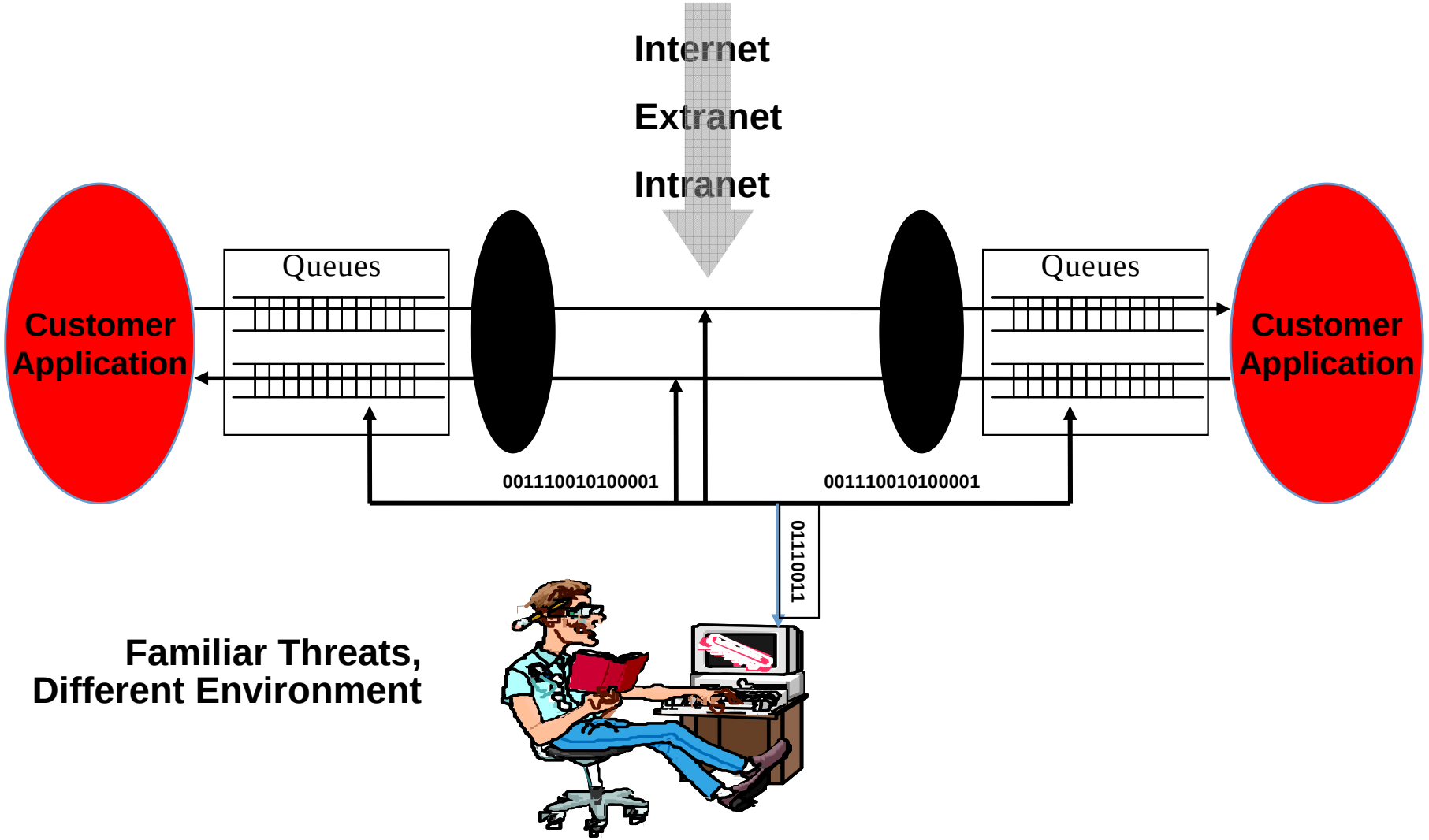
WebSphere software

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
- **A**udit trail
- Integrity
- Privacy
- 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

What is MQ AMS?

WebSphere MQ Advanced Message Security V7.0.1

- New product announced in Oct 5, 2010.
- Replacement for WebSphere MQ Extended Security Edition.
- It is a component that is added to WebSphere MQ V6/V7.
- It uses digital certificates (X.509) and Public Key Infrastructure (PKI) to protect MQ messages.
- Security policies are used to define the security level required.

Key Features

- Secures sensitive or high-value MQ messages.
- Detects and removes rogue or unauthorized messages before they are processed by receiving applications.
- Verifies that messages are not modified in transit from queue to queue.
- Protects messages not only when they flow across the network but when they are at rest in queues.
- Messages from existing MQ applications are transparently secured using interceptors.

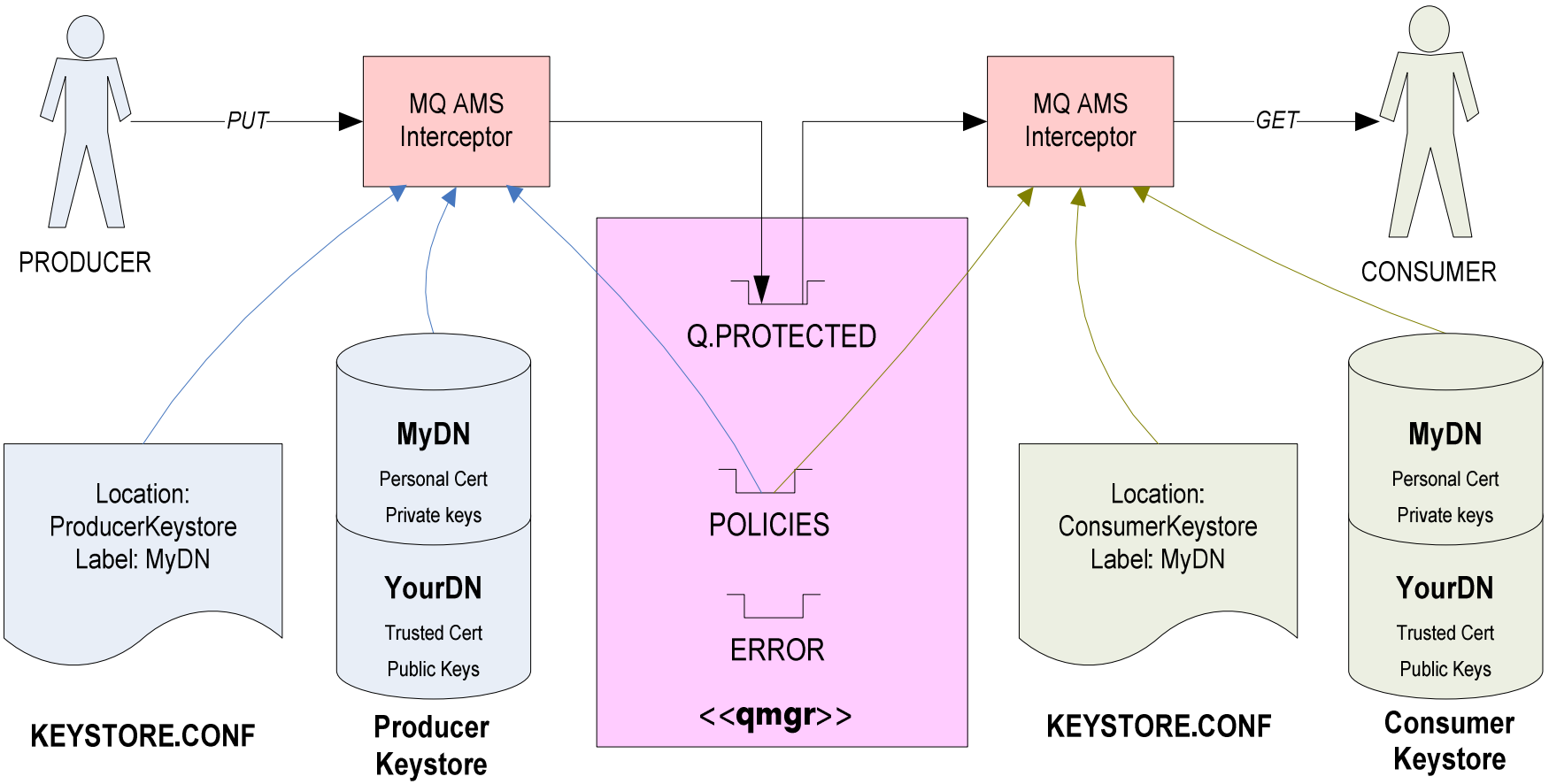
MQ AMS compared to MQ ESE

- Support for WebSphere MQ v6 and v7.
  - Pub/Sub is not supported.
  - Channel data conversion is not supported.
  - Distribution lists are not supported.
- IBM Tivoli software is not longer a pre-requisite.
- Full MQ java support (J2EE and J2SE)
  - MQ JMS 1.0.2 and 1.1.
  - MQ classes for java.
- Support for asynchronous consumers (MQ V7).
- Support for message properties (MQ V7).
- Authentication and authorization is delegated to MQ.
  - MQ SSL and Security exits.
  - MQ OAM.
- MQ AMS plug-in for MQ Explorer for policy administration
- MQ AMS command-line tools for policy administration

Platforms supported

- HP-UX Itanium
- HP-UX PA-RISC
- Linux for System p
- Linux for System x (32 bit and 64-bit)
- Linux for System z
- Solaris for Intel X86 (64-bit)
- Solaris for Sun SPARC
- AIX for System p
- Windows (32-bit and 64-bit)
- z/OS for System z

Logical Architecture Design – Distributed Platforms



MQ AMS interceptors

- MQ AMS functionality is implemented in interceptors.
  - There are no long running processes or daemons (Except in z/OS).
- Existing MQ applications do not require changes.
- Three interceptors are provided:
  1. **Server interceptor** for local (bindings mode) MQI API and Java applications.
     - Implemented as queue manager API exit.
  2. **MQI API client interceptor** for remote (client mode) MQ API applications.
     - MQ AMS interceptor imbedded in MQ client code.
  3. **Java client interceptor** for remote (client mode) MQ JMS and MQ classes for java applications (J2EE and J2SE).
     - MQ AMS interceptor imbedded in MQ java client code.
     - MQ V7.0 java client required.
     - SupportPac MQC7 WebSphere MQ V7.0 clients.

Message protection policies

- Created or updated or removed by command ‘setmqspl’
- Or by MQ AMS plug-in for MQ Explorer (GUI).
- Policies are stored in queue ‘SYSTEM.PROTECTION.POLICY.QUEUE’.
- Each protected queue can have only one policy.
- Two types of policies:
  - Message Integrity policy.
  - Message Privacy policy.
- Display policies with command ‘dspmqspl’.

Message integrity policies

- There are two message signing algorithms: SHA1 and MD5.
- Recommended to use SHA1.
- The list of authorized signers is optional
  - If no authorized signers are specified then any application can sign messages.
  - If authorized signers are specified then only messages signed by these applications can be retrieved.
  - Messages from other signers are sent to the error queue.

setmqspl
-m <queue_manager>
-p
<protected_queue_name>
-s <SHA1 | MD5>
-a <Authorized signer DN1>
-a <Authorized signer DN2>

Message integrity policy example

- This policy is to enforce integrity protection (signature) for messages put on queue Q.INTEGRITY in queue manager QM.
- The message signing algorithm is SHA1.
- Messages can only by signed by one authorized application.
- Messages signed by any other signer are sent to the SYSTEM.PROTECTION.ERROR.QUEUE and an error returned to the receiving application.

```
setmqspl -m QM
-p Q.INTEGRITY
-s SHA1
-e NONE
-a
  'CN=pdmqss,O=tivoli,
  C=US'
```

Message privacy policy

- Encryption algorithms: RC2, DES, 3DES, AES128 and AES256.
- Message privacy requires that encrypted messages are also signed.
- The list of authorized signers is optional.
- It is mandatory to specify at least one message recipient.

setmqspl
-m <queue_manager>
-p <protected_queue_name>
-s <SHA1 | MD5>
-e <encryption algorithm>
-a <Authorized signer DN1>
-a <Authorized signer DN2>
-r < Message recipient DN1>
-r < Message recipient DN2>

Message privacy policy example

- This policy enforces privacy protection (signature and encryption) for messages put on queue Q.PRIVACY in queue manager QM.
- The message signing algorithm is SHA1.
- The message encryption algorithm is AES128.
- Two message recipients are listed using their certificates DN.
- Messages retrieved by un-authorized recipients cause messages to be sent to the SYSTEM.PROTECTION.ERROR.QUEUE.

```
setmqspl -m QM
-p Q.PRIVACY
-s SHA1
-e AES128
-r
  'CN=pdmqss,O=tivoli
  ,C=US'
-r 'CN=Vicente
Suarez,OU=ISSW,O=IB
  M,L=Hursley,C=GB'
```

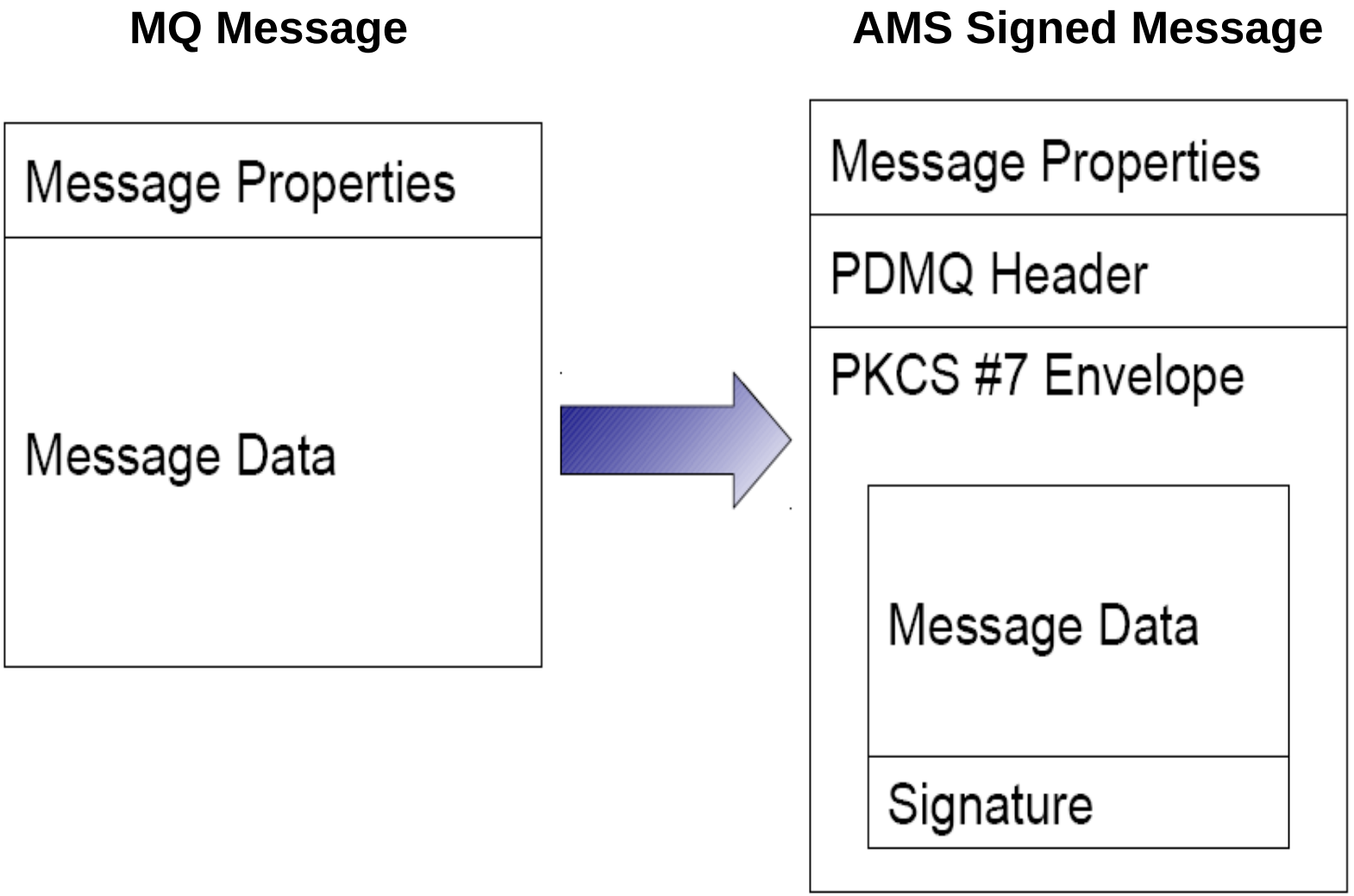
Keystores and X.509 certificates

- Each MQ application producing or consuming protected messages requires access to a keystore that contains a personal X.509 (v2/v3) certificate and the associated private key.
- The keystore and certificate is accessed by the MQ AMS interceptors.
- Several types of keystore are supported: CMS, JKS and JCEKS.
- The keystore must contain trusted certificates to validate message signers or to obtain the public keys of encrypted message recipients.

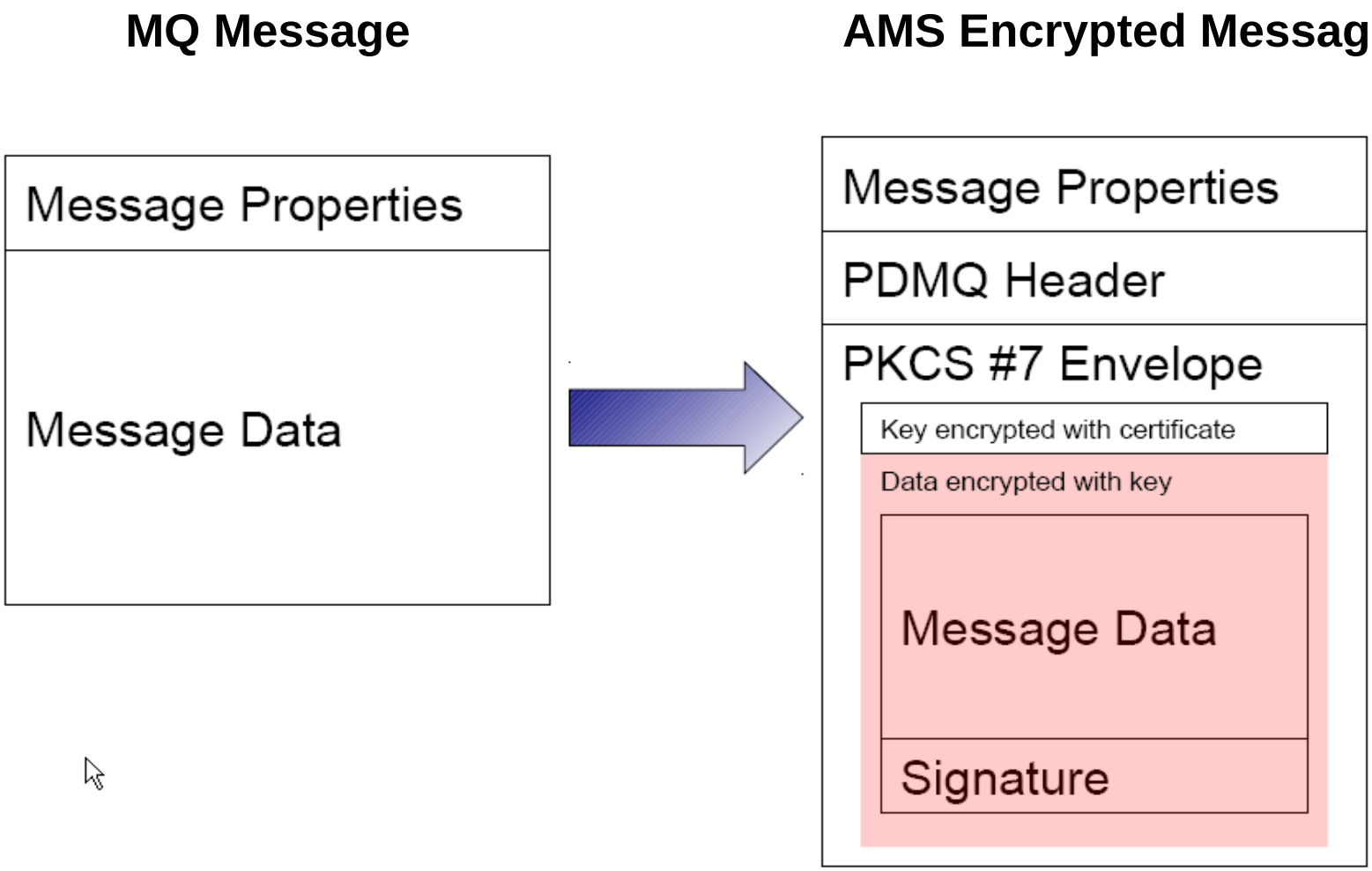
MQ AMS configuration file

- MQ AMS interceptors require a configuration file.
  - Type of keystore: CMS, JKS, JCEKS
  - Location of the keystore.
  - Label of the personal certificate.
  - Passwords to access keystore and private keys.
- Interceptors locate the configuration file using one of the following methods:
  - Environment variable MQS_KEYSTORE_CONF=<path to conf file>.
  - Checking default locations and file names.
    - Platform dependent. For example in UNIX: “$HOME/.mqs/keystore.conf”
    - Refer to Infocenter.

Integrity message format



Privacy message format



Migration considerations

- MQ AMS can coexist with MQ ESE.
- Migration of MQ V6 to MQ V7 should be done after migration to MQ AMS.
- Pre-migration:
  - Install MQ AMS.
  - Create MQ AMS system queues.
  - Configure MQ AMS policies mapped from TAM policies before migration.
  - MQ AMS policies can be created in toleration mode. Policies are applied if it is possible otherwise unprotected messages are accepted.
  - Prepare keystores and certificates for MQ AMS.
  - Create MQ AMS configuration files.
- On migration day:
  - Disable MQ ESE interceptors then enable MQ AMS interceptors (applications and queue manager restart are required).
- Post migration:
  - Un-configure MQ ESE interceptors.
  - Uninstall MQ ESE.
  - Migrate MQ v6.0 to v7.0.

Summary

WebSphere MQ Advanced Message Security V7.0.1

- It is new member of the WebSphere MQ family.
- It is the successor to MQ ESE V6.0
- It protects message integrity and/or privacy.
- It supports MQ V6 and V7.
- It does not support Pub/Sub.
- Existing MQ applications do not require changes.
- MQ AMS uses interceptors, policies, keystores and certificates.

Other relevant sessions

- **General Sessions**
  - Mon 15:00 - 16:15 MF1 - WebSphere Messaging and Connectivity Featured Session + Panel Q&A
  - Wed 17:45 - 18:45 BOF4 - WebSphere MQ: Birds of a Feather
- **HA and DR**
  - Wed 08:30 - 09:45 M30 - WebSphere MQ High Availability
  - Wed 10:15 - 11:30 M50 - WebSphere MQ for z/OS - Restart and Recovery
  - Thu 10:15 - 11:30 M19 - WebSphere MQ Disaster Recovery
- **Security**
  - Tue 08:30 - 09:45 M40 - MQ Security 101: Administrative Hardening
  - Fri 08:30 - 11:30 ML5 - Hands-on Lab: WebSphere MQ Security (distributed platforms)