



WebSphere MQ Advanced Message Security

v7.0.1

Jonathan Rumsey
jrumsey@uk.ibm.com
Last Update: 12/07/2011

Why Message Level Security?

Messaging that does not involve humans

Command & control scenarios

Large MQ networks : difficult to prove security of messages

Against message injection / message modification / message viewing

Data subject to standards compliance (PCI, HIPAA, etc)

Credit card data protected by PCI

Confidential government data

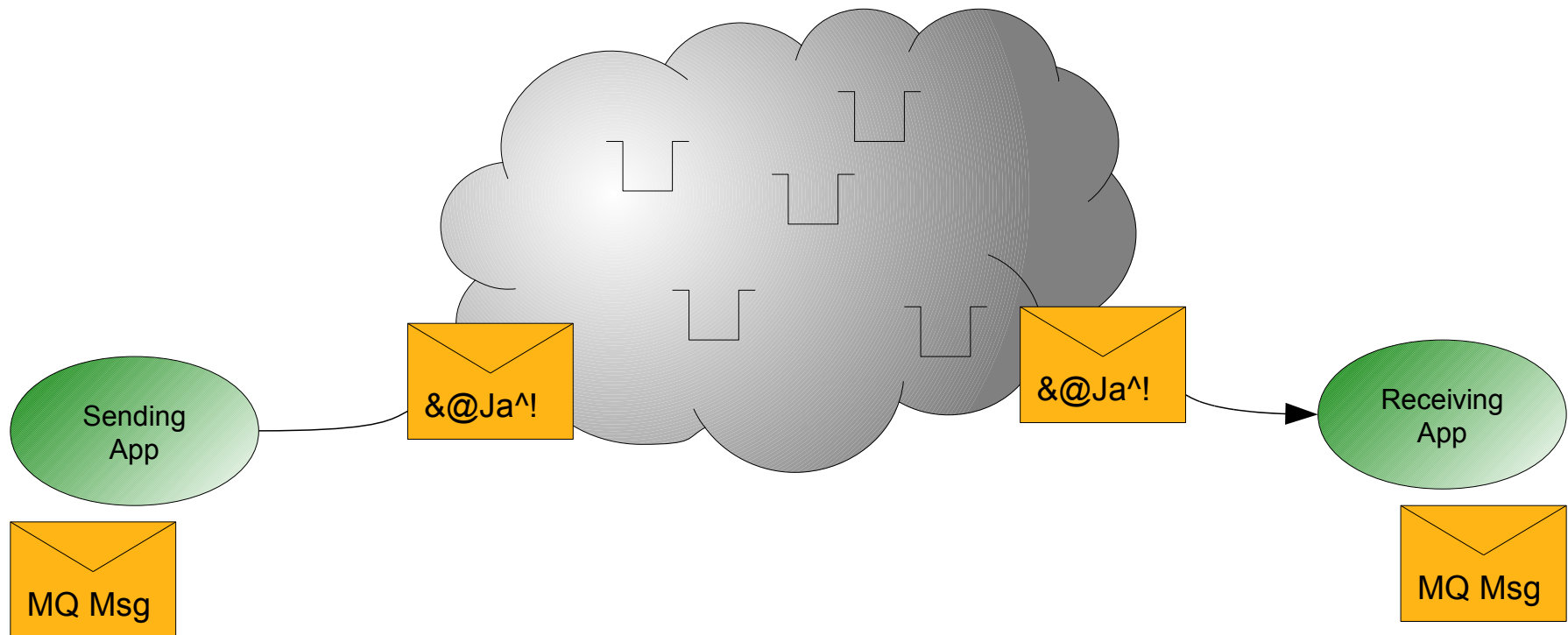
Message Level Protection

- Assurance that messages have not been altered in transit
 - When issuing payment information messages, ensure the payment amount does not change before reaching the receiver

- Assurance that messages originated from the expected source
 - When processing control messages, validate the sender

- Assurance that messages can only be viewed by intended recipient(s)
 - When sending confidential information

WebSphere MQ Advanced Message Security



WebSphere MQ Advanced Message Security

- Provides additional security services over and above base MQ
- App → App data protection for **point to point** messaging
 - Asymmetric cryptography used to protect individual messages
- Administratively controlled policies applied to queues
 - Command line
 - MQ Explorer
- Non-invasive
 - No changes required to MQ applications

WMQ vs WMQ AMS

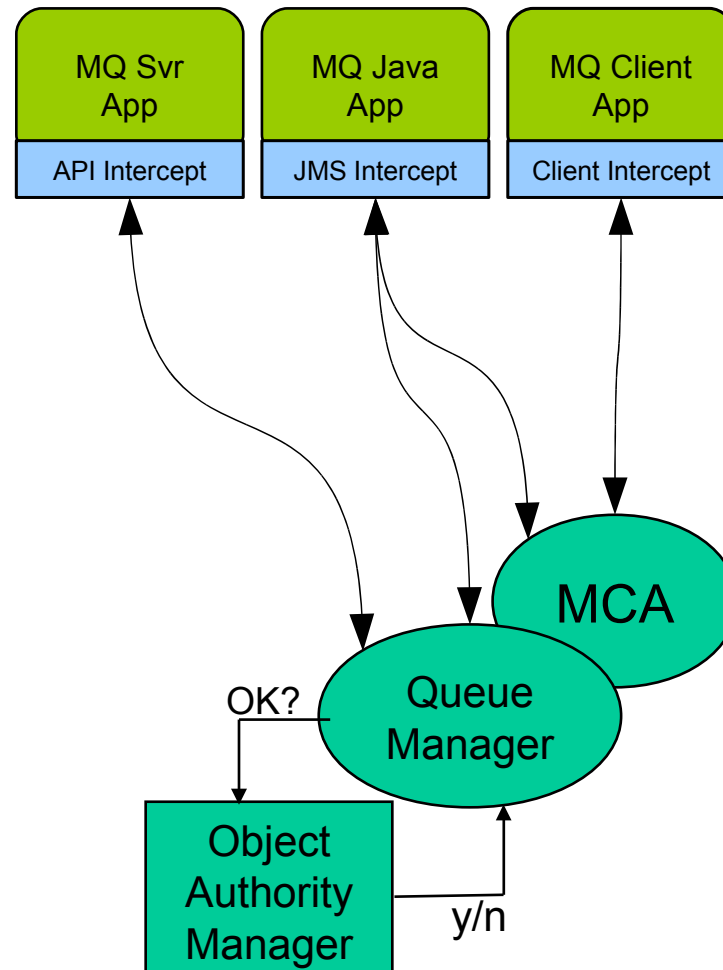
■ WebSphere MQ

- Authentication (local OS for server apps or peer authenticated SSL for client apps)
- Authorisation (OAM on distributed, RACF on z/OS)
- Integrity (SSL for channels)
- Privacy (SSL for channels)

■ WebSphere MQ AMS

- Integrity (Digital signature of message content)
- Privacy (Message content encryption)

WMQ + AMS v7.0.1 Architecture



Administration : Distributed

- Command line tools
 - **setmqspl** : *Set message protection policy*
 - -m QMGR
 - -p Policy_Name
 - -s Signing_Algorithm
 - -a Authorised Signers
 - -e Encryption_Algorithm
 - -r Message_Recipients

 - **dspmqspl** : *Display message protection policies*
 - -m QMGR
 - [-export]
 - [-p Policy_Name]

Administration : Distributed

Protection Policies

Policy Name	Signing Algorithm	Encryption Algorithm
Q1	SHA1	AES256
Q2	SHA1	AES256
MyQueue	SHA1	AES256
Delete...		
Properties...		

MyQueue - Properties

Policy Name: MyQueue
 Note – the Policy Name is the same as the queue name to which it applies.

Tolerance

Strictly apply this policy to all messages
 Apply policy to protected messages, but tolerate unprotected messages

Signing

Signature algorithm: NONE

List the distinguished names (DNs) that are permitted message originators. Only messages with signatures containing one of these DN's will be accepted.

Add Signature DN... Remove

Valid signature DN

cn=Robert Smith,ou=IBM Software Group,o=IBM,c=UK
 cn=Lisa Jones,ou=IBM Software Group,o=IBM,c=UK

Encryption

Encryption algorithm: NONE

Applications put directly to the queue protected by this policy (uncheck this option if the queue is only accessed by another queue manager)

List the permitted message recipients. Messages will only be readable if encrypted for one of these recipients.

Add Recipient DN... Remove

Permitted recipient

cn=Robert Smith,ou=IBM Software Group,o=IBM,c=UK
 cn=Lisa Jones,ou=IBM Software Group,o=IBM,c=UK

OK Cancel

Callouts:

- Right click node to create a new policy
- Double click policy to view properties
- Name of policy is not editable once created.
- Tolerance group is extended content and may not be present in the initial release.
- Removes the selected DN's from the list below.
- Pops up a dialogue asking the user to supply a DN.
- If selected, at least one DN is required. If deselected, a DN is not required.

WebSphere MQ AMS : Security Policy

Signature Algorithm

MD5

SHA1

Encryption Algorithm

RC2

DES

3DES

AES128

AES256

Acceptable signer(s)

Applicable when signing messages

Message recipient(s)

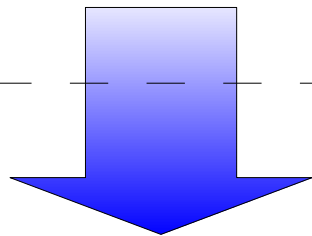
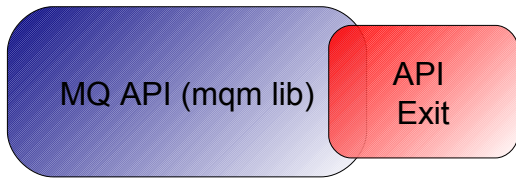
Applicable when encrypting and signing messages

Interceptors

Server

- API Exit

Application



QMGR

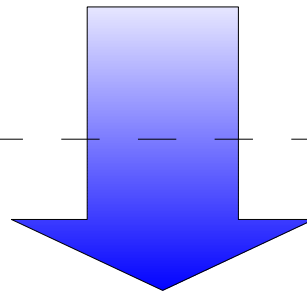
Client

- Library Replacement

Application

Replacement mqic lib

Renamed MQIC



Channel Agent

QMGR

JMS

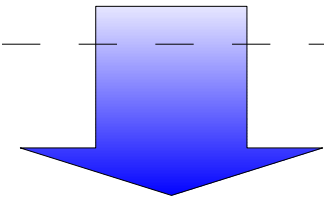
- JMQI Intercept

JMS Application

JMS

JMQI Intercept

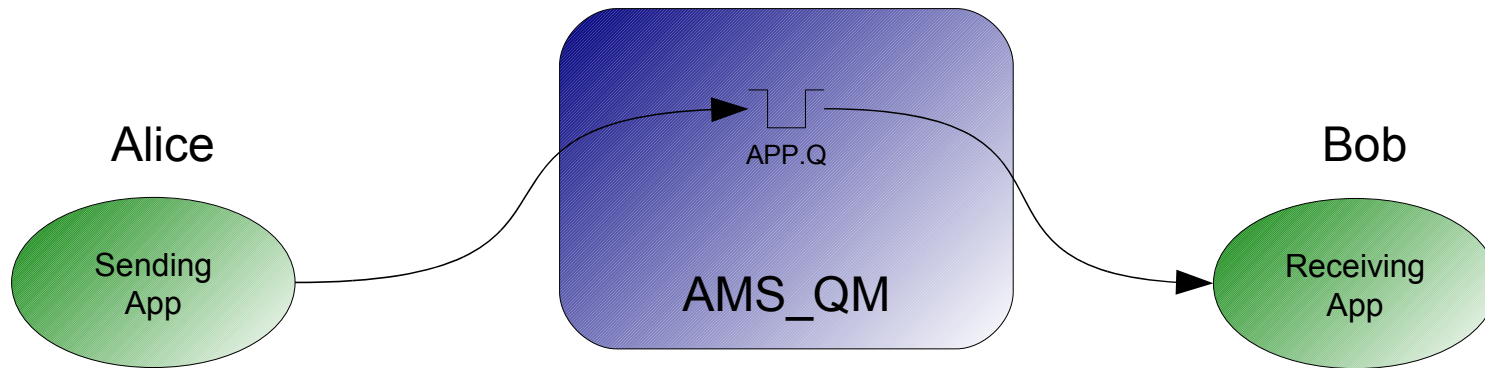
JMQI



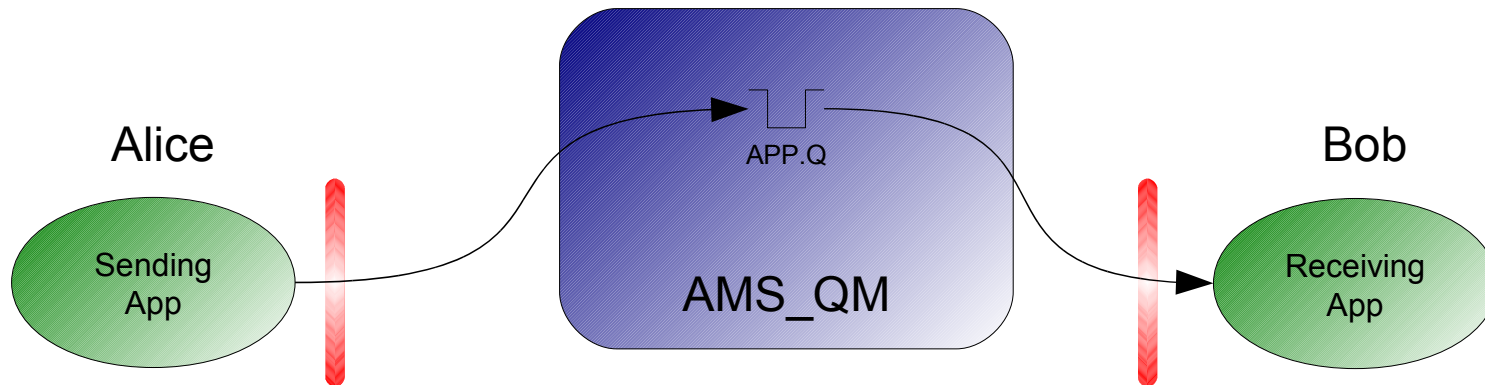
Channel Agent

QMGR

WebSphere MQ AMS

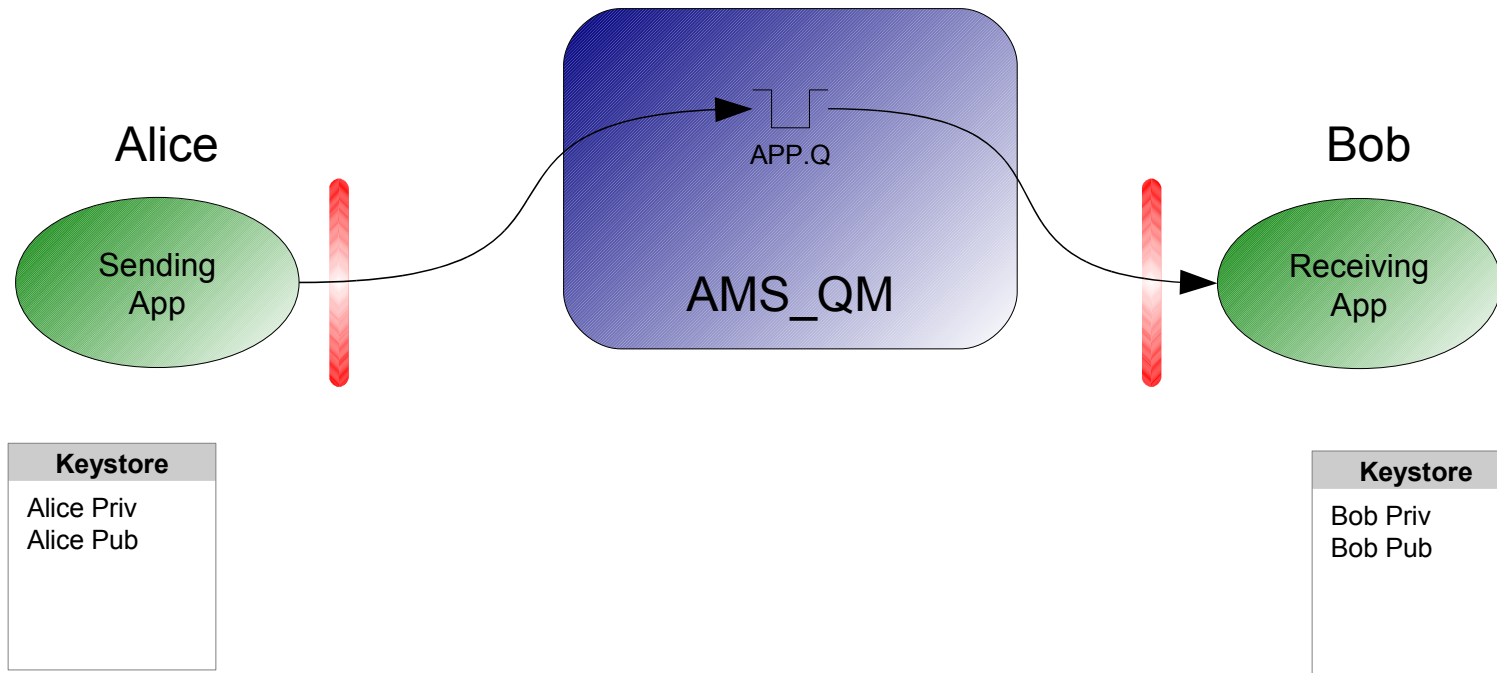


WebSphere MQ AMS



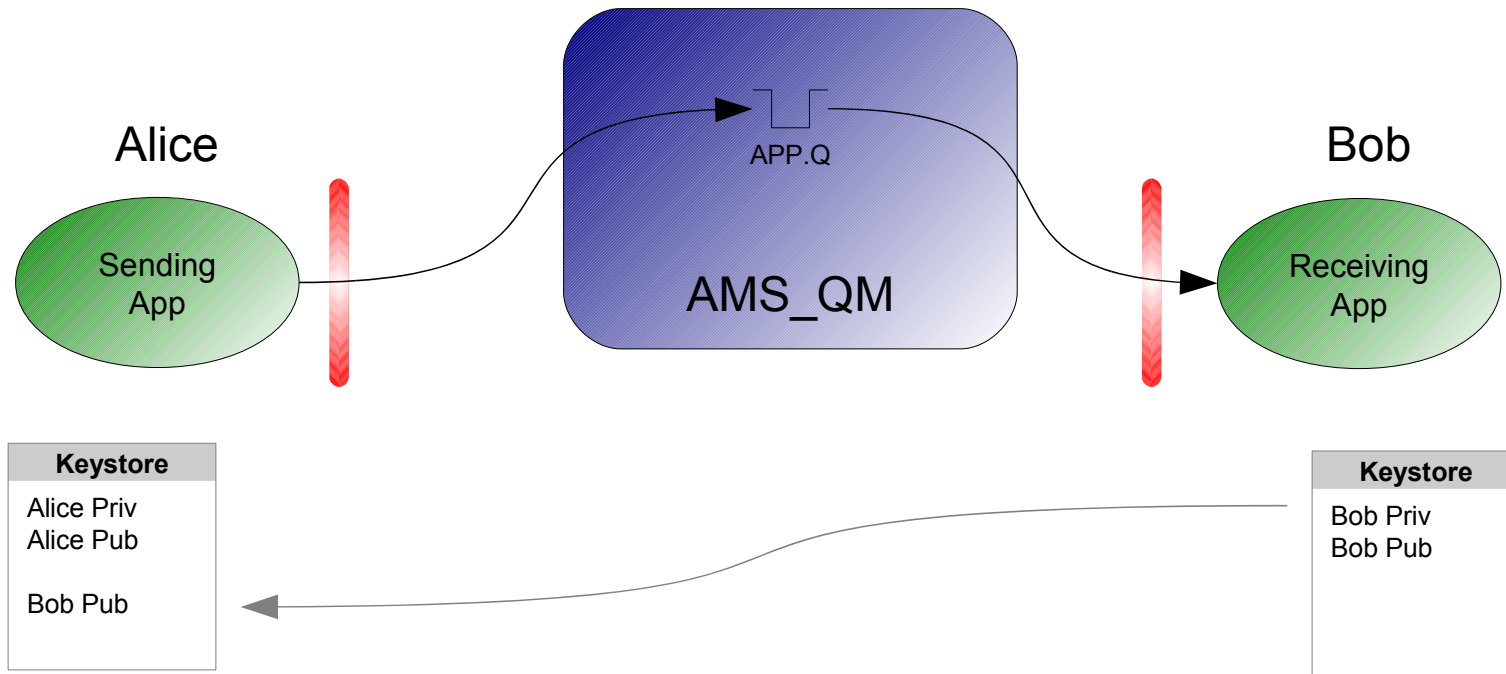
1. Install AMS Interceptor

WebSphere MQ AMS



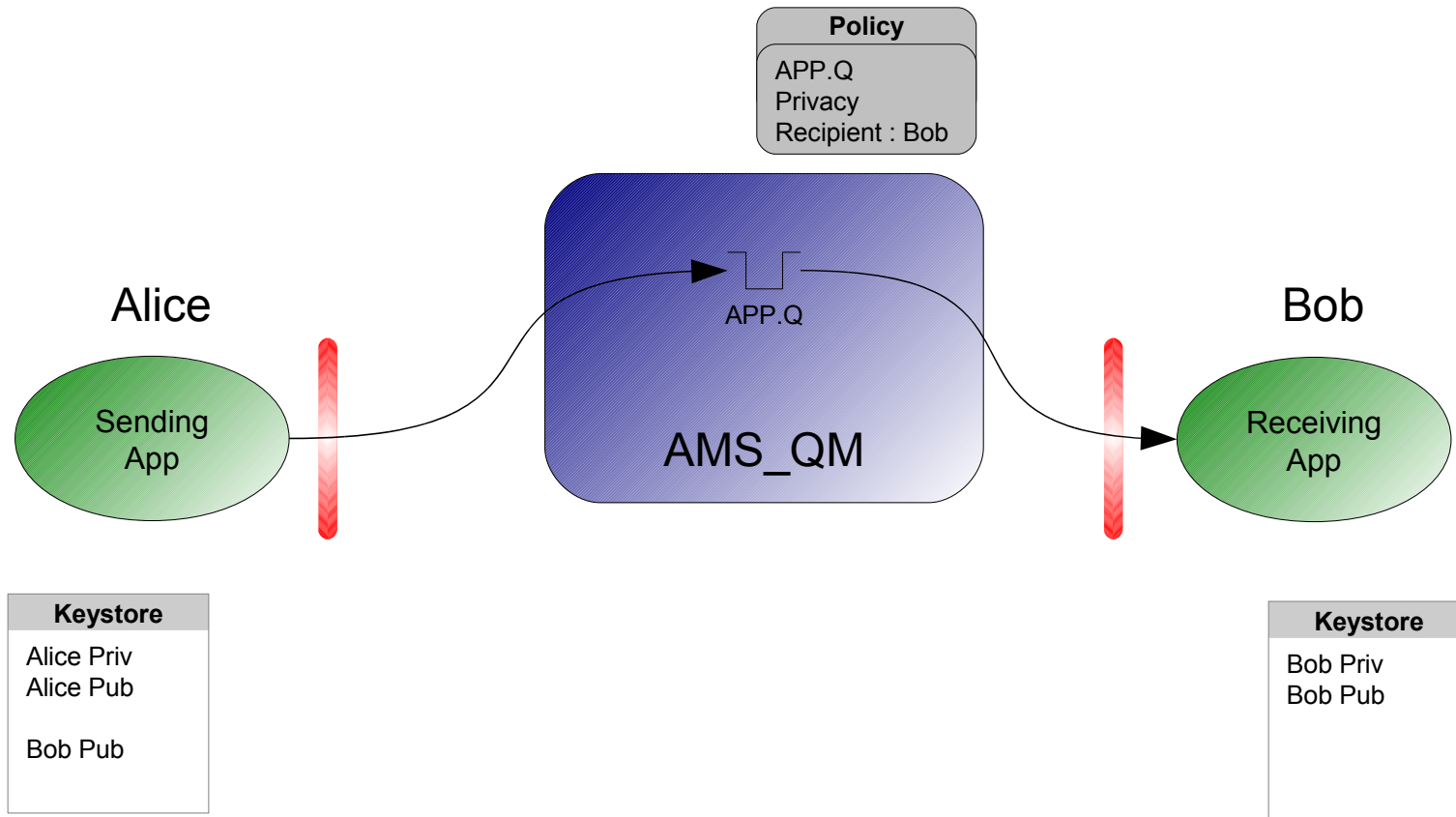
1. Install AMS Interceptor
2. Create public / private key pairs

WebSphere MQ AMS



1. Install AMS Interceptor
2. Create public / private key pairs
3. Copy recipient's public key

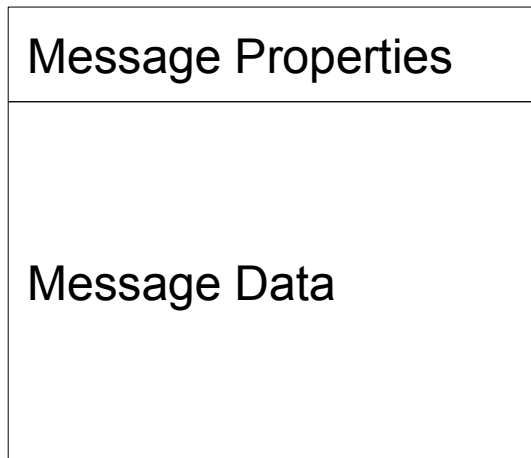
WebSphere MQ AMS



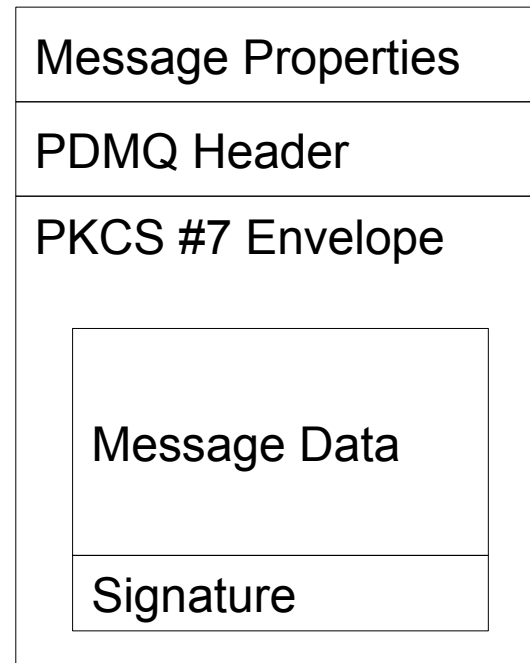
1. Install AMS Interceptor
2. Create public / private key pairs
3. Copy recipient's public key
4. Define protection policy for the queue

WebSphere MQ AMS : Integrity Message Format

Original MQ Message

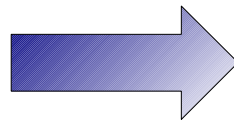
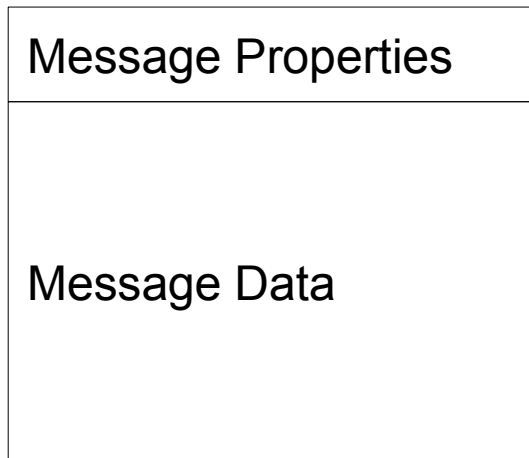


AMS Signed Message

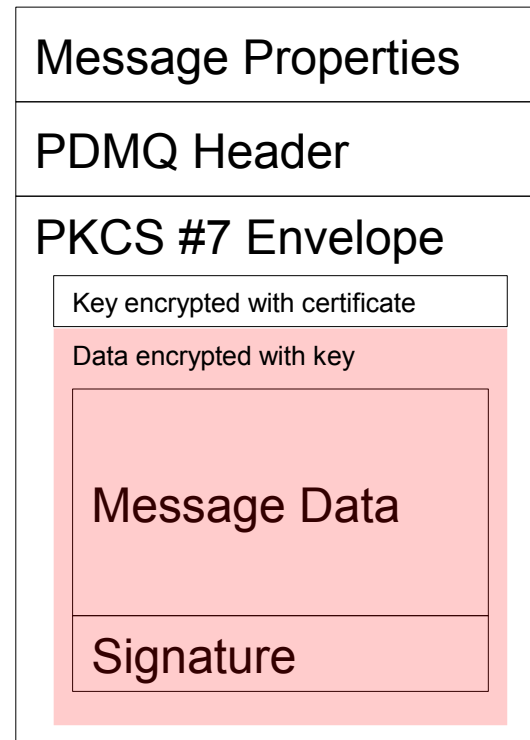


WebSphere MQ AMS : Privacy Message Format

Original MQ Message



AMS Encrypted Message



Key Points

- MQ AMS dates :
 - Released : 8th Oct 2010
 - 7.0.1.1 Released : 14th April 2011
 - Added support for cryptographic hardware acceleration
 - 90 day Trial version available to download

- Platform support
 - Same as MQ 7.0.1 (except IBM i)
 - Works with MQ 6 & MQ 7 queue managers (JMS interceptor requires v7 jars)

Thank You

Questions ?