

For Your Eyes Only ! MQ Advanced Message Security

Jon Rumsey
IBM

Wednesday 10th August
Session # 9417

Agenda

- Message Level Security
- Digital Cryptography 101 (Alice & Bob)
- WebSphere MQ Advanced Message Security
- Architecture
- Administration
- Availability

Why Message Level Security ?

- Messaging that does not involve humans
 - Command & control scenarios
 - Application to Application, no “human” checking
- 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
 - Personal information e.g. healthcare
 - Data at rest, administrative privileges, etc

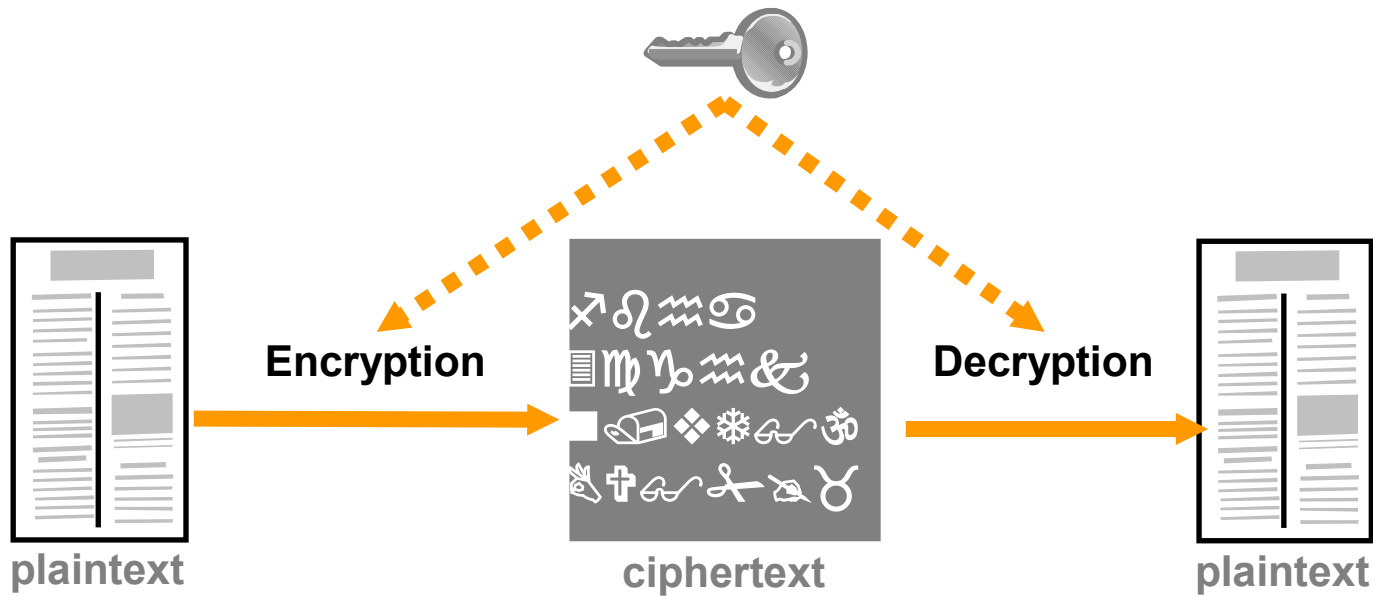
Message Level Protection

- 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

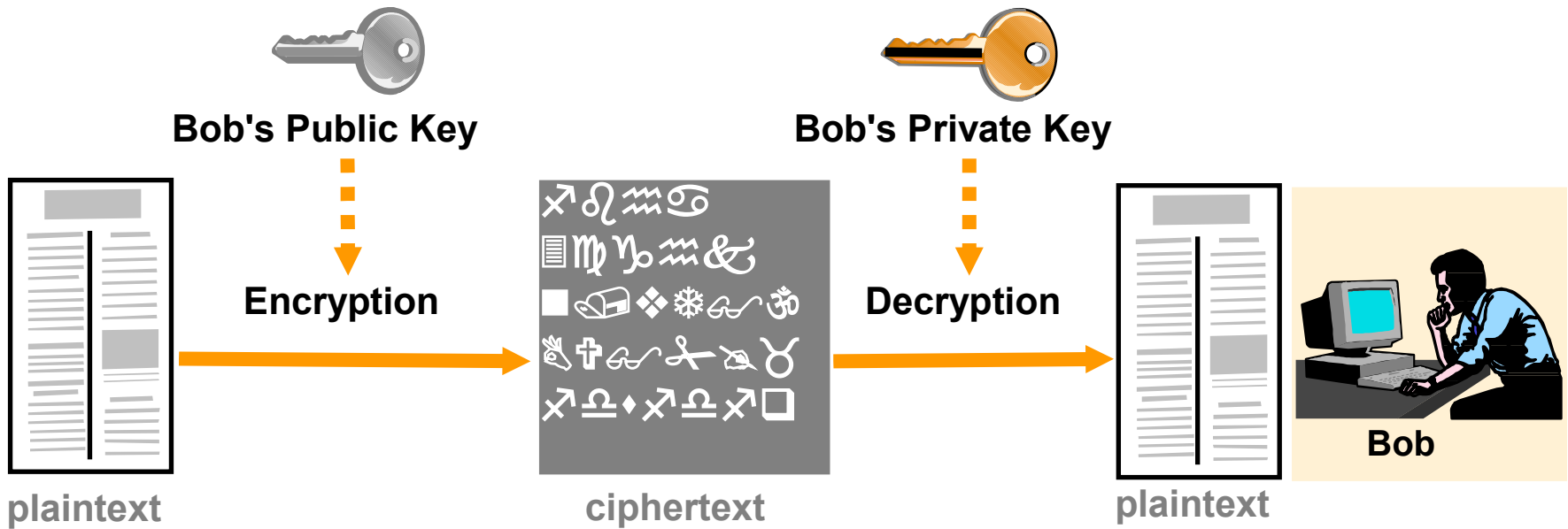
Cryptography

- Symmetric Keys
 - Relatively fast
 - Poses key distribution challenges when faced with large numbers of senders/receivers
 - The key has to be known by the sender and receiver
- Asymmetric Keys
 - Message encrypted with one key can only be decrypted by the other one
 - Slower than symmetric key cryptography
 - Asymmetric Keys can be used to solve the key distribution challenges associated with symmetric keys

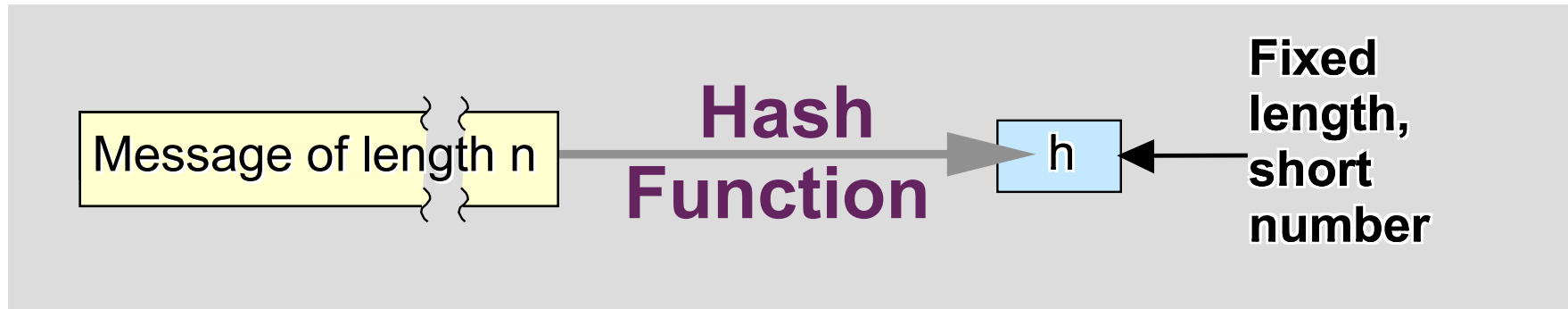
Symmetric Key Cryptography



Asymmetric Key Cryptography

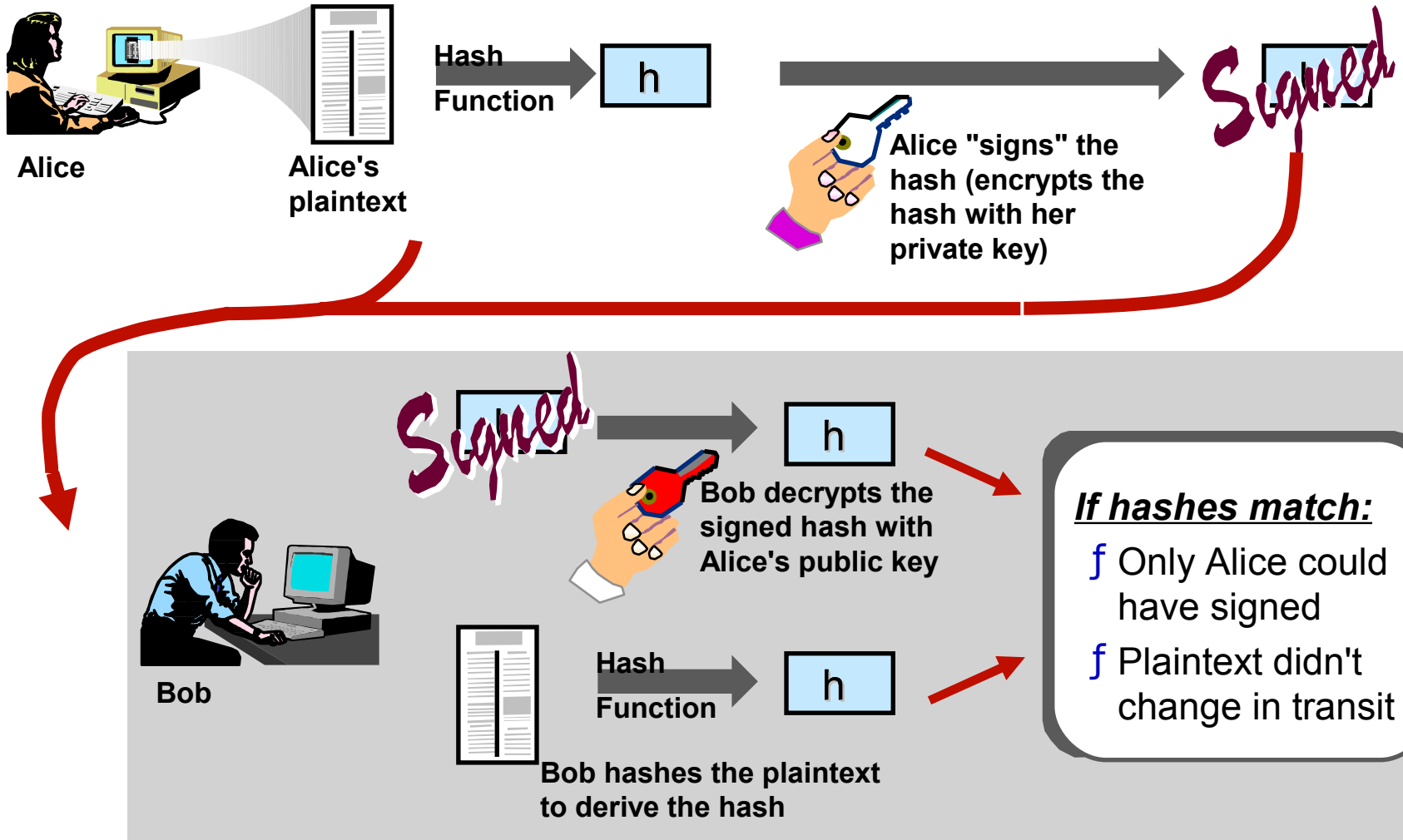


Hash Functions

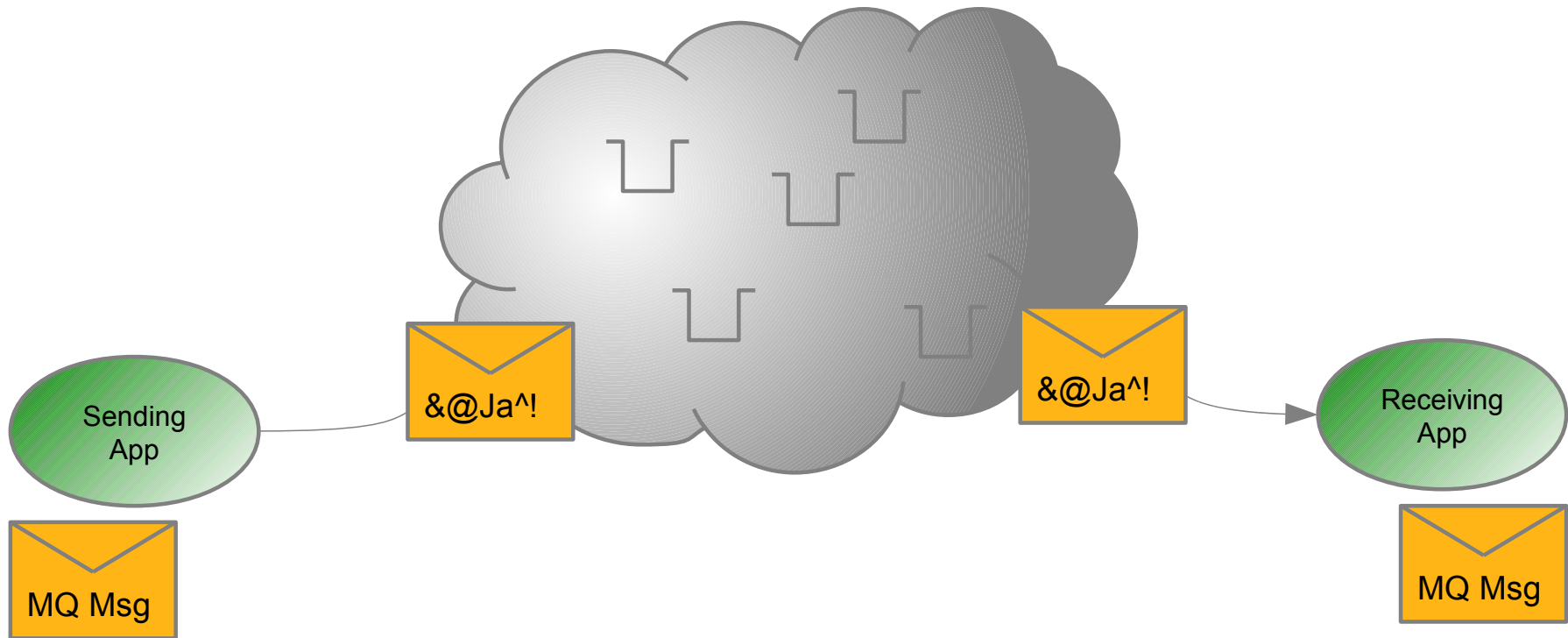


- Hash Function
 - Computes the message MAC (Message Authentication Code)
 - Easy to compute
 - Very difficult to reverse
 - Computationally infeasible to find two messages that hash to the same value

Digital Signatures



WebSphere MQ Advanced Message Security



WebSphere MQ Advanced Message Security

- Provides additional security services over and above base MQ
- Application to Application protection for messages
 - Well suited to point to point, publish/subscribe limited
 - Have to know your authorized parties ahead of operation
- Asymmetric cryptography used to protect each message
- Non-invasive
 - No changes required to applications
- Administrative interfaces for policy management
 - Command line
 - MQ Explorer Plug-In (GUI)

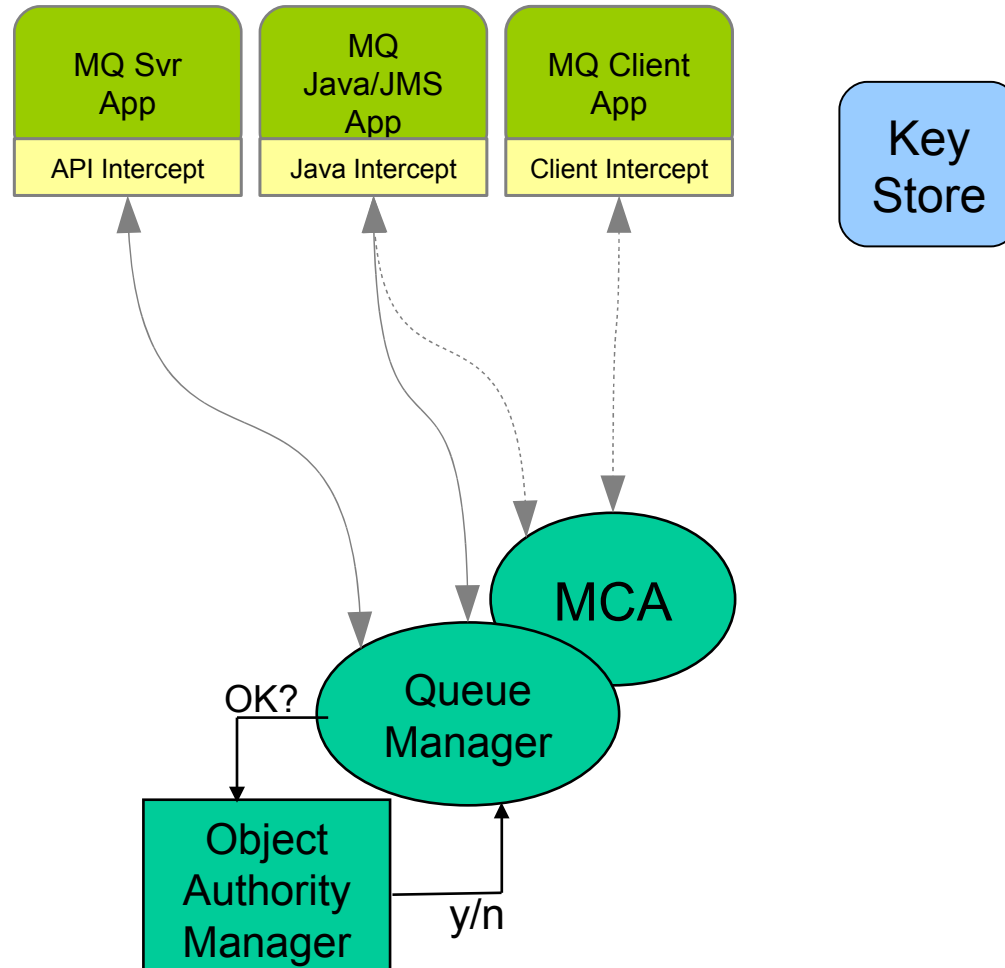
WMQ vs WMQ AMS Security

- AMS is a complimentary offering, not a replacement to WMQ security
- WebSphere MQ
 - Authentication (Local OS user id, SSL peer for clients)
 - Authorization (OAM on distributed, RACF on z/OS)
 - Integrity (SSL for channels)
 - Privacy (SSL for channels)
- WebSphere MQ Advanced Message Security
 - Integrity (Digital signing of messages)
 - Privacy (Message content encryption)

Certificates, Interceptors and Policies

- AMS uses X.509 digital certificates for digital signing and encryption
- Interceptors installed in the application process to sign, encrypt and decrypt message data
 - No code changes to the application
- Policies are defined to control the interceptors
 - Matched against queue names
 - What level of protection, none, integrity or privacy
 - Which certificates are involved (DN)
 - Authorised signer(s)
 - Authorised recipient(s)

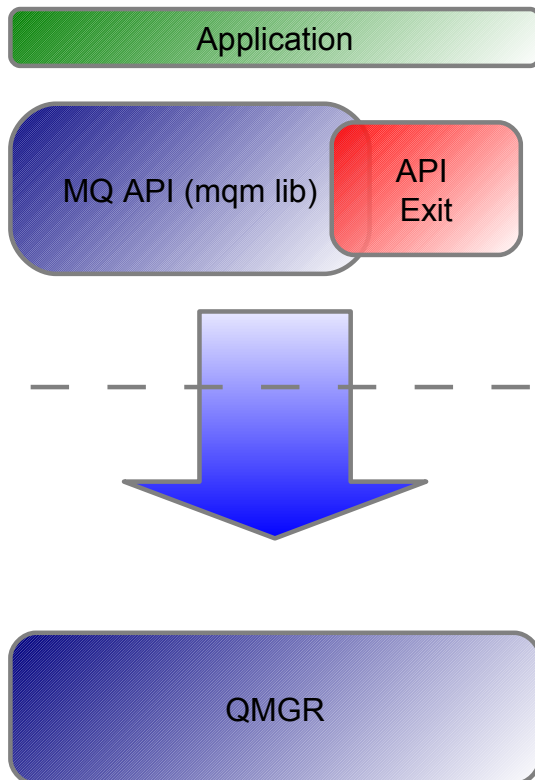
WMQ + AMS v7.0.1 Architecture



AMS Interceptors

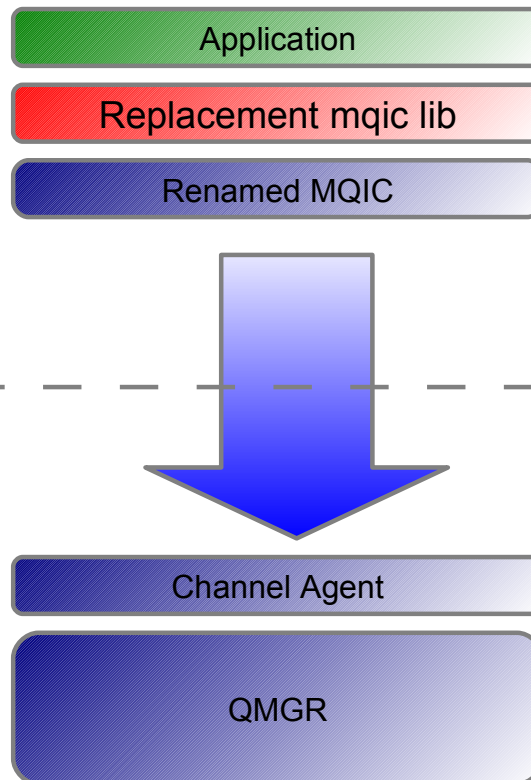
Server

- API Exit



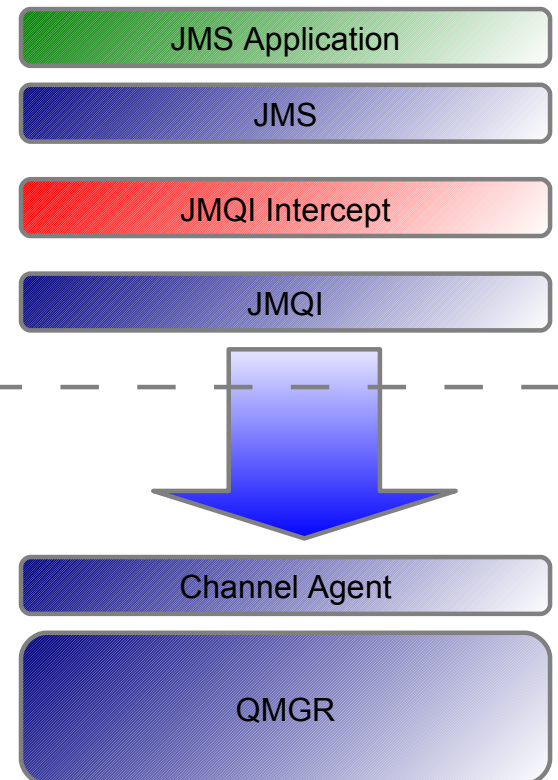
Client

- Library Replacement



JMS

- JMQUI Intercept



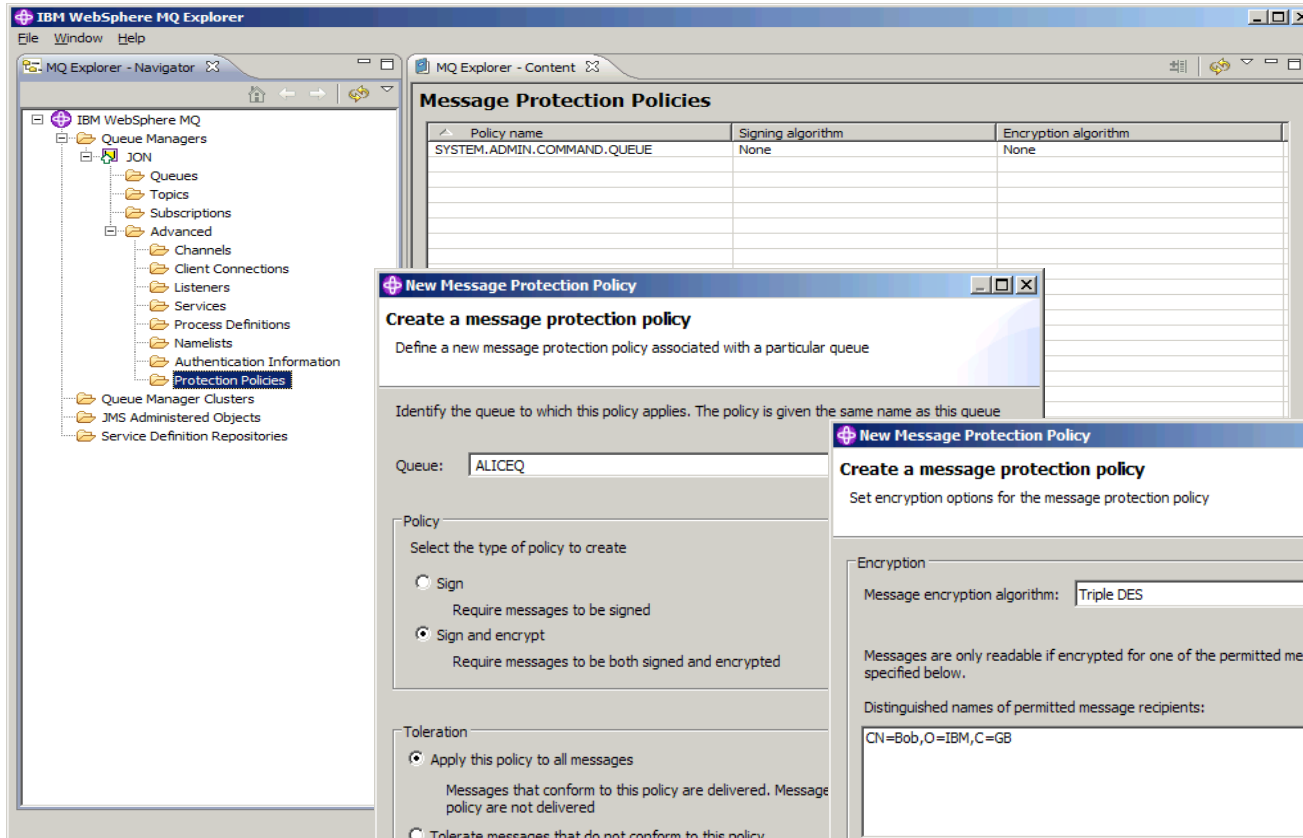
AMS Policies

- Stored on SYSTEM.PROTECTION.POLICY.QUEUE
- Signature Algorithm
 - MD5 or SHA1
- Encryption Algorithm
 - RC2, DES, 3DES, AES128 or AES256
- Acceptable Signer(s)
 - Applicable when signing messages
- Message Recipient(s)
 - Applicable when signing and encrypting messages

Policy Administration

- 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]

Policy Administration



The screenshot shows the IBM WebSphere MQ Explorer interface. On the left is a tree view of the MQ environment, including Queue Managers, Queues, Topics, Subscriptions, Advanced, Channels, Client Connections, Listeners, Services, Process Definitions, Namelists, Authentication Information, and Protection Policies. The main pane displays the 'Message Protection Policies' table.

Policy name	Signing algorithm	Encryption algorithm
SYSTEM.ADMIN.COMMAND.QUEUE	None	None

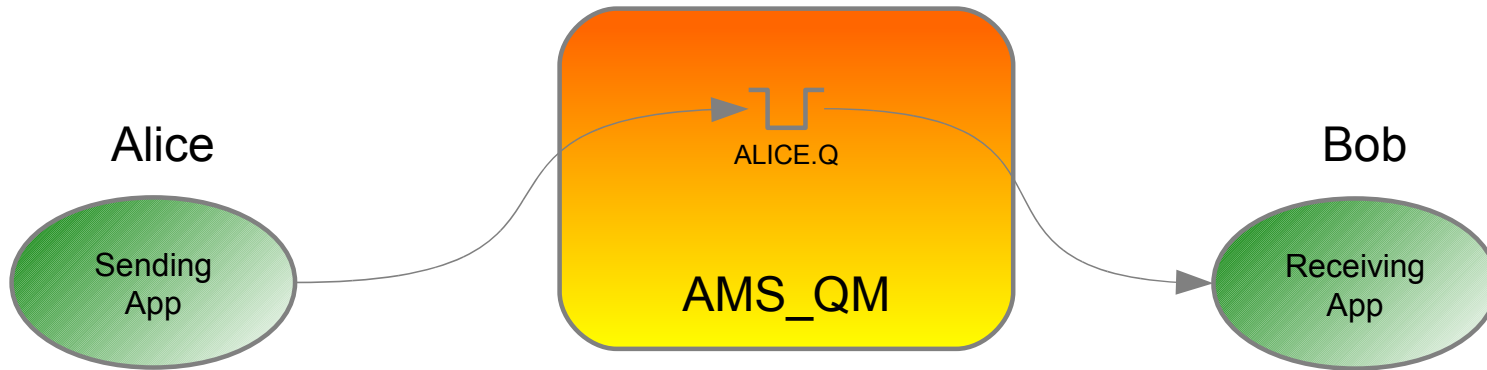
Two 'New Message Protection Policy' dialog boxes are overlaid. The first dialog is titled 'Create a message protection policy' and contains the following fields and options:

- Queue:
- Policy: Select the type of policy to create
 - Sign
Require messages to be signed
 - Sign and encrypt
Require messages to be both signed and encrypted
- Tolerance:
 - Apply this policy to all messages
Messages that conform to this policy are delivered. Message policy are not delivered
 - Tolerate messages that do not conform to this policy
All messages are delivered

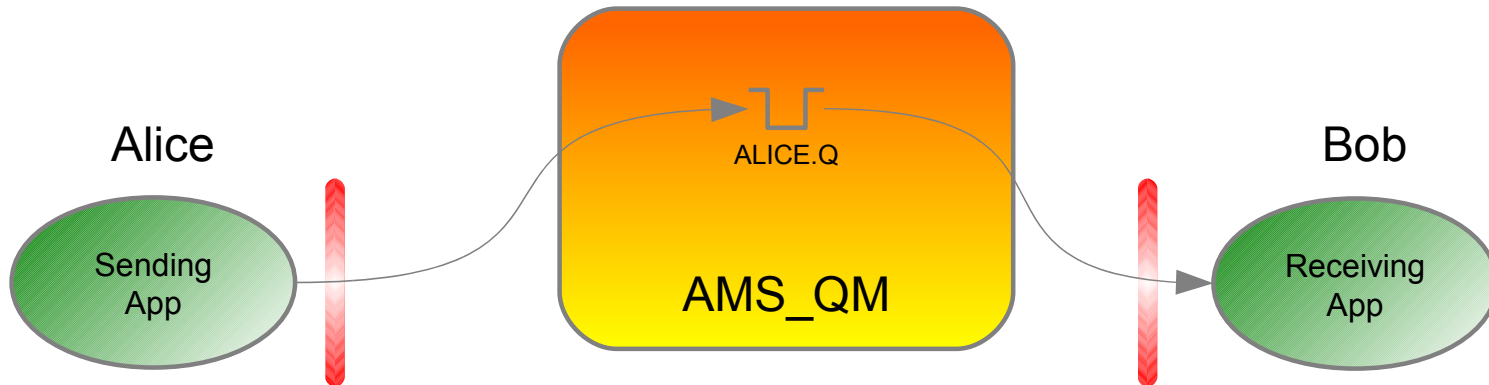
The second dialog is also titled 'Create a message protection policy' and is for setting encryption options:

- Encryption: Set encryption options for the message protection policy
- Message encryption algorithm:
- Messages are only readable if encrypted for one of the permitted message recipients specified below.
- Distinguished names of permitted message recipients:

Securing an MQ Application

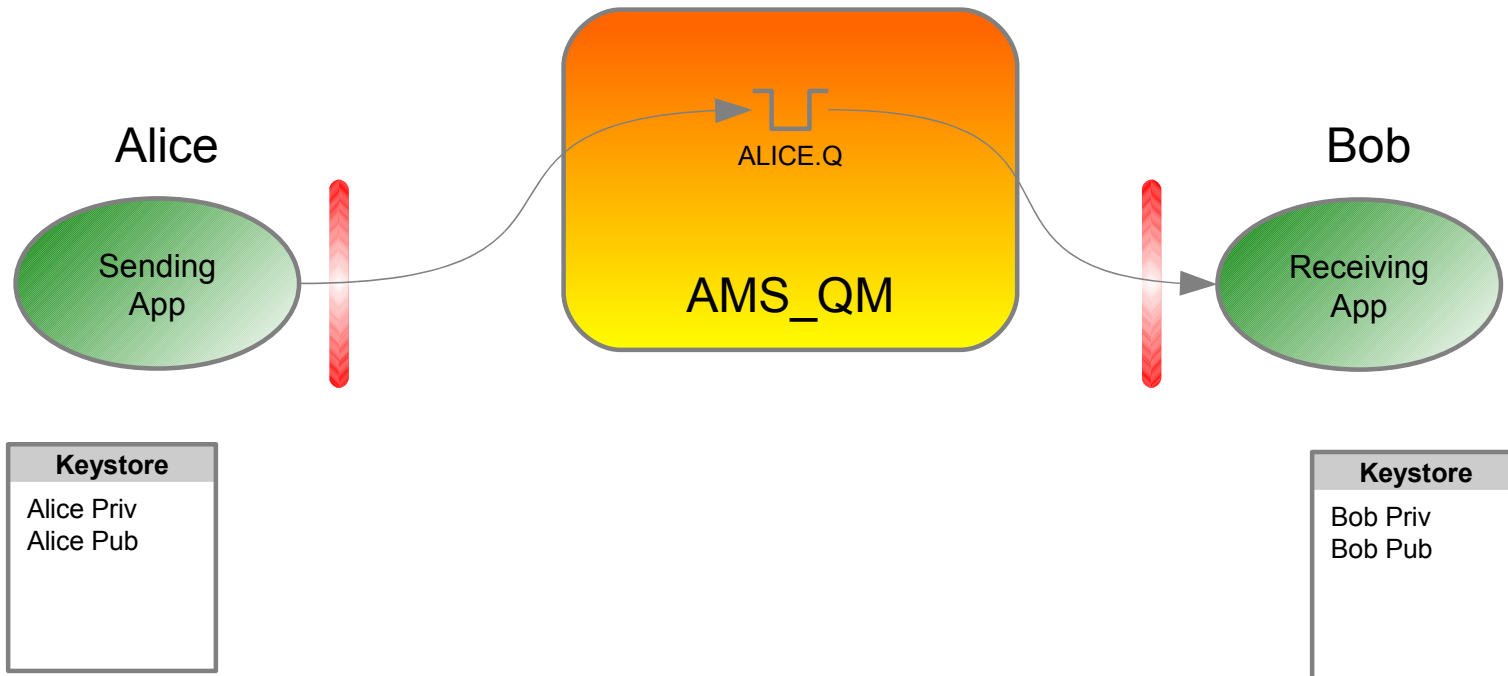


Securing an MQ Application



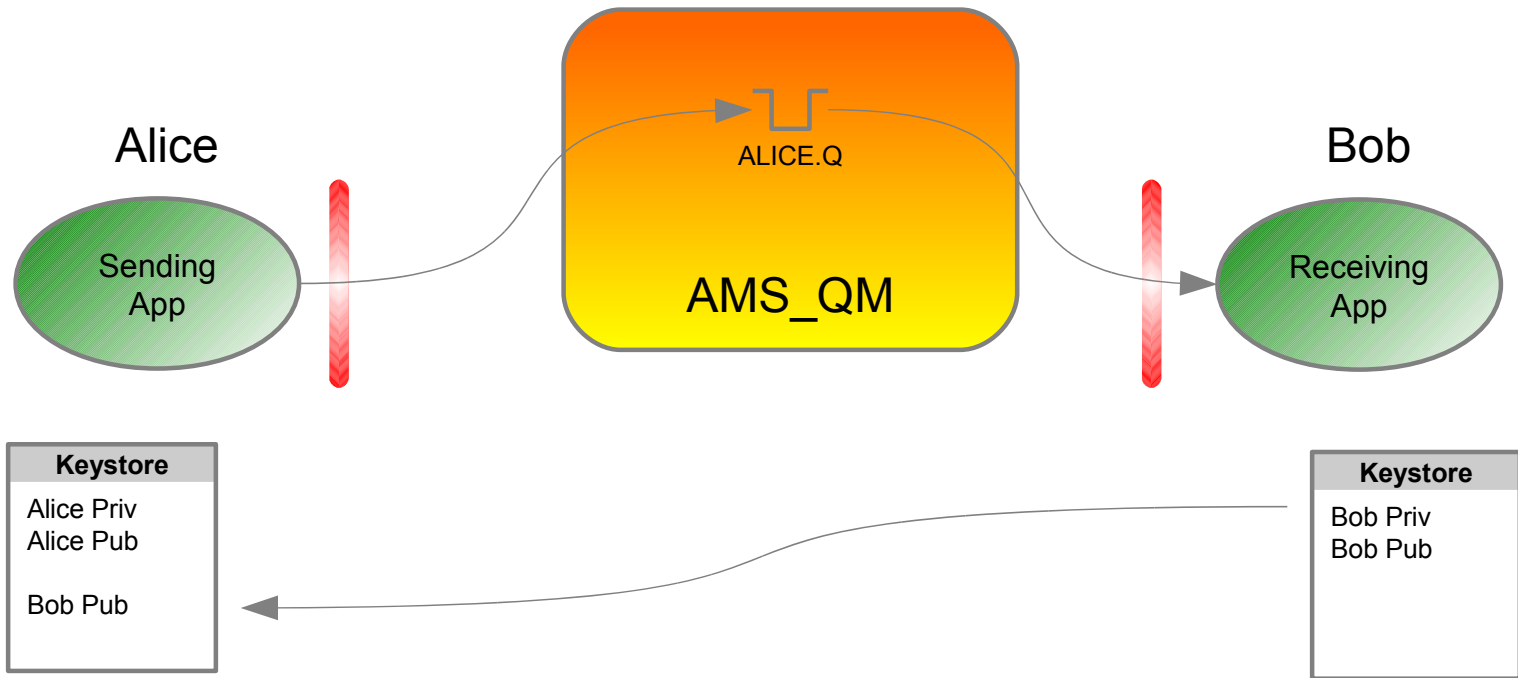
1. Install AMS Interceptor

Securing an MQ Application



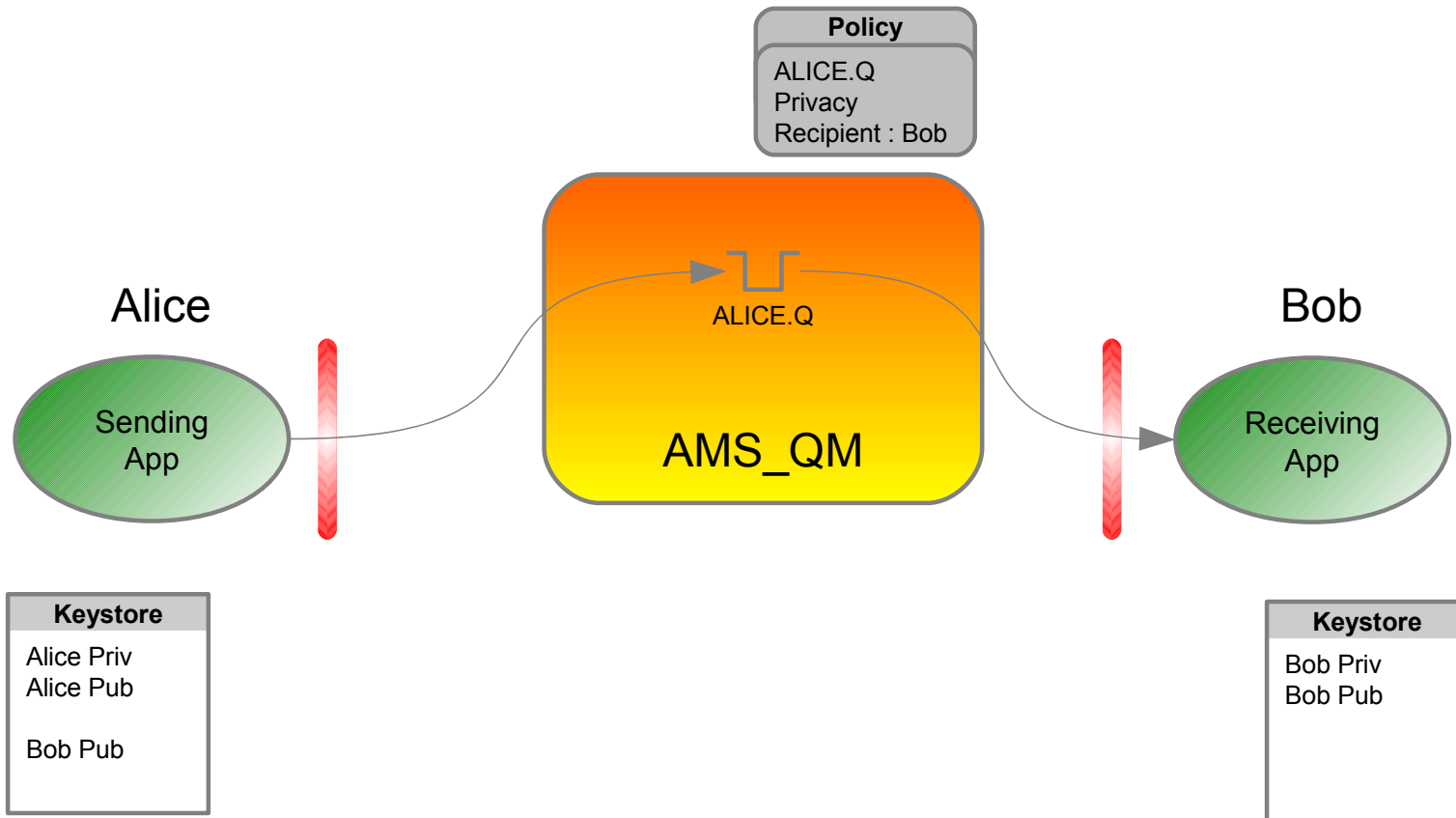
1. Install AMS Interceptor
2. Create public / private key pairs

Securing an MQ Application



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

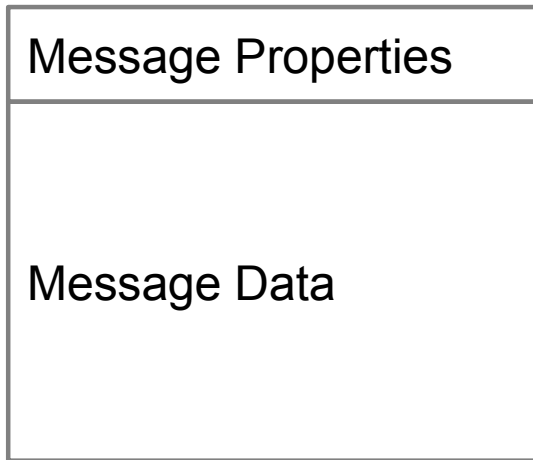
Securing an MQ Application



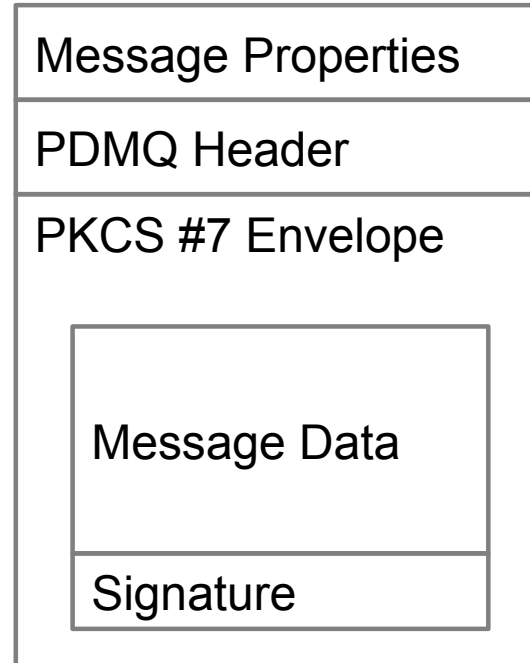
1. Install AMS Interceptor
2. Create public / private key pairs
3. Copy recipient's public key
4. Define protection policy for the queue

WebSphere MQ AMS : Integrity Message Format

Original MQ Message



AMS Signed Message

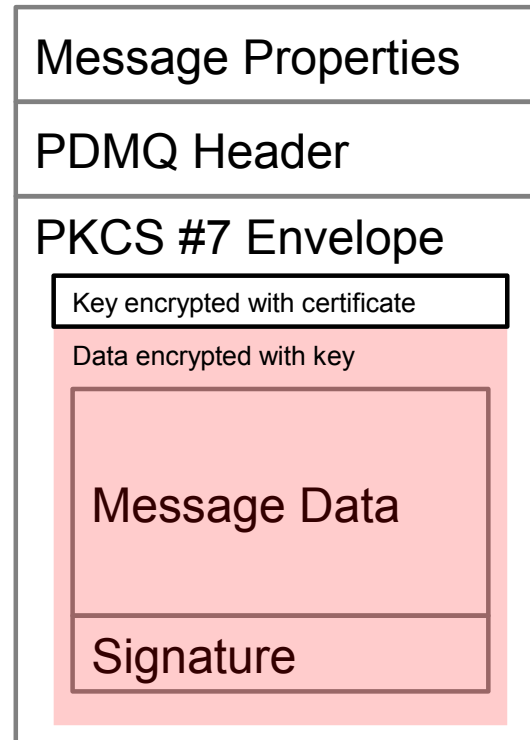


WebSphere MQ AMS : Privacy Message Format

Original MQ Message



AMS Encrypted Message



Availability

- MQ AMS dates :
 - Released : 8th Oct 2010
 - 7.0.1.1 Released : 14th April 2011
 - Added support for crypto hardware to store keys
 - 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)

Summary

- AMS provides message level security
 - Complements base MQ security, not a replacement
 - Can be applied selectively at a queue level
 - Each message protected with asymmetric key cryptography
- Application to application, end to end security
 - No code changes required
 - Well suited to point to point applications

The rest of the week

	Monday	Tuesday	Wednesday	Thursday	Friday
08:00			More than a buzzword: Extending the reach of your MQ messaging with Web 2.0	Batch, local, remote, and traditional MVS - file processing in Message Broker	Lyn's Story Time - Avoiding the MQ Problems Others have Hit
09:30		WebSphere MQ 101: Introduction to the world's leading messaging provider	The Do's and Don'ts of Queue Manager Performance	So, what else can I do? - MQ API beyond the basics	MQ Project Planning Session
11:00		MQ Publish/Subscribe	The Do's and Don'ts of Message Broker Performance	Diagnosing problems for Message Broker	What's new for the MQ Family and Message Broker
12:15	MQ Freebies! Top 5 SupportPacs	The doctor is in. Hands-on lab and lots of help with the MQ family		Using the WMQ V7 Verbs in CICS Programs	
01:30	Diagnosing problems for MQ	WebSphere Message Broker 101: The Swiss army knife for application integration	The Dark Side of Monitoring MQ - SMF 115 and 116 record reading and interpretation	Getting your MQ JMS applications running, with or without WAS	
03:00	Keeping your eye on it all - Queue Manager Monitoring & Auditing	The MQ API for dummies - the basics	Under the hood of Message Broker on z/OS - WLM, SMF and more	Message Broker Patterns - Generate applications in an instant	
04:30	Message Broker administration for dummies	All About WebSphere MQ File Transfer Edition	For your eyes only - WebSphere MQ Advanced Message Security	Keeping your MQ service up and running - Queue Manager clustering	
06:00			Free MQ! - MQ Clients and what you can do with them	MQ Q-Box - Open Microphone to ask the experts questions	

Questions & Answers

Please fill out your evaluation forms
Session # 9417