For Your Eyes Only – WebSphere MQ Advanced Messaging Security

Craig Both (bothcr@uk.ibm.com)
IBM UK, Hursley

8th August 2012
11509

Agenda

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

Why Message Level Security ?

- 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

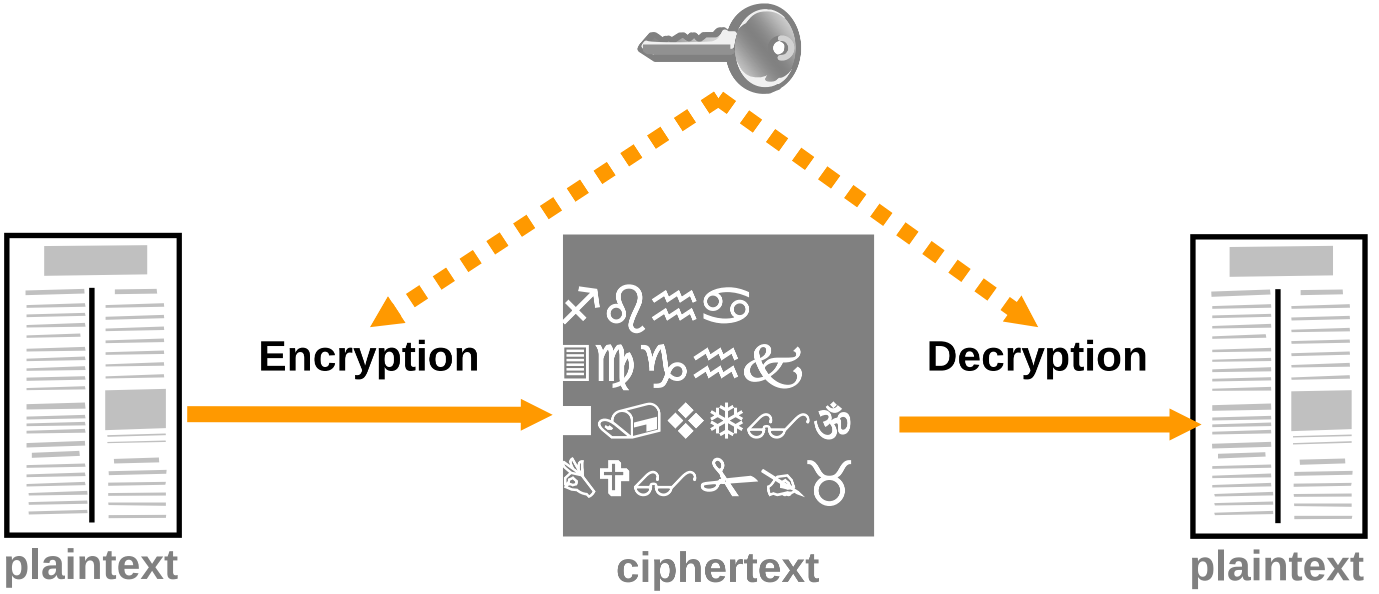
Message Level Protection

- 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

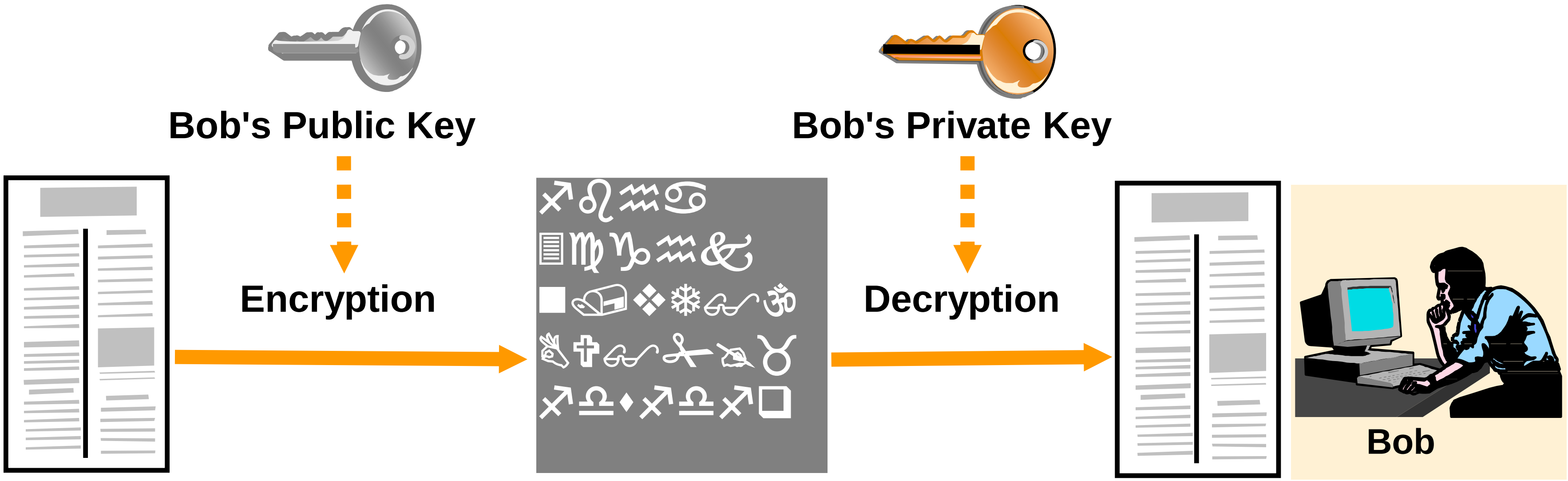
Cryptography

- 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 Crytography



Asymmetric Key Cryptography



Bob's Public Key

Encryption

Bob's Private Key

Decryption

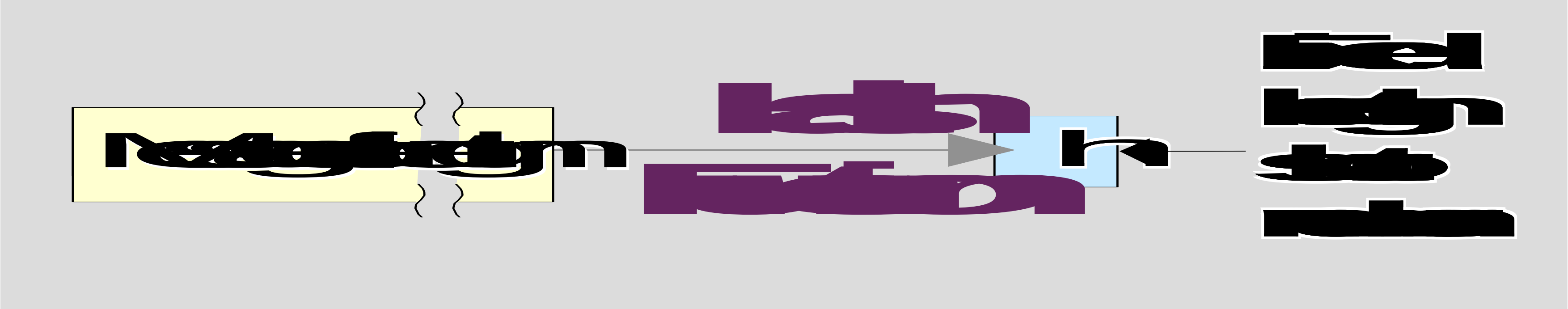
Bob

plaintext

ciphertext

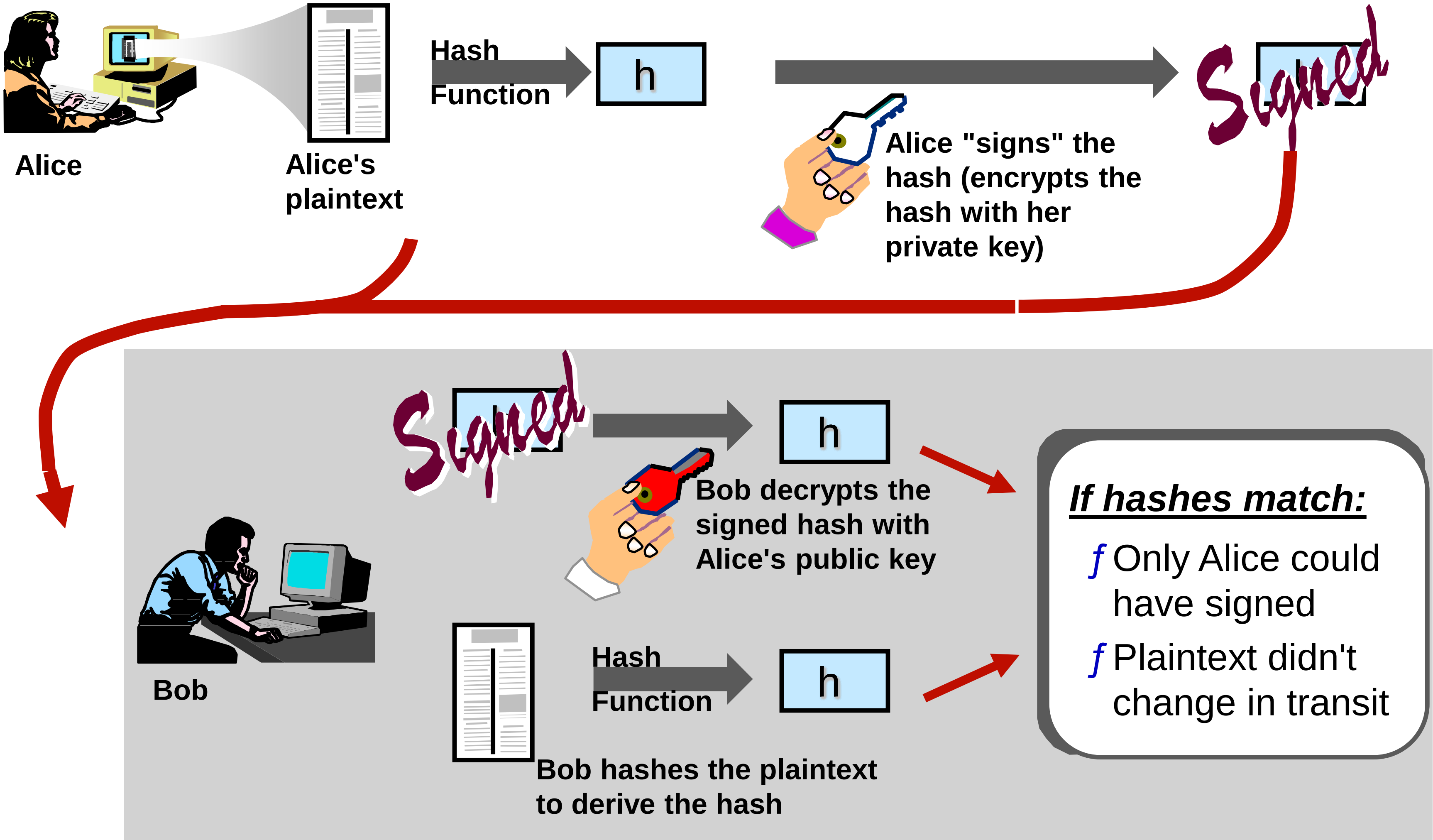
plaintext

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



Alice "signs" the hash (encrypts the hash with her private key)

Bob decrypts the signed hash with Alice's public key

Bob hashes the plaintext to derive the hash

If hashes match:

- Only Alice could have signed
- Plaintext didn't change in transit

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 an additional 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)

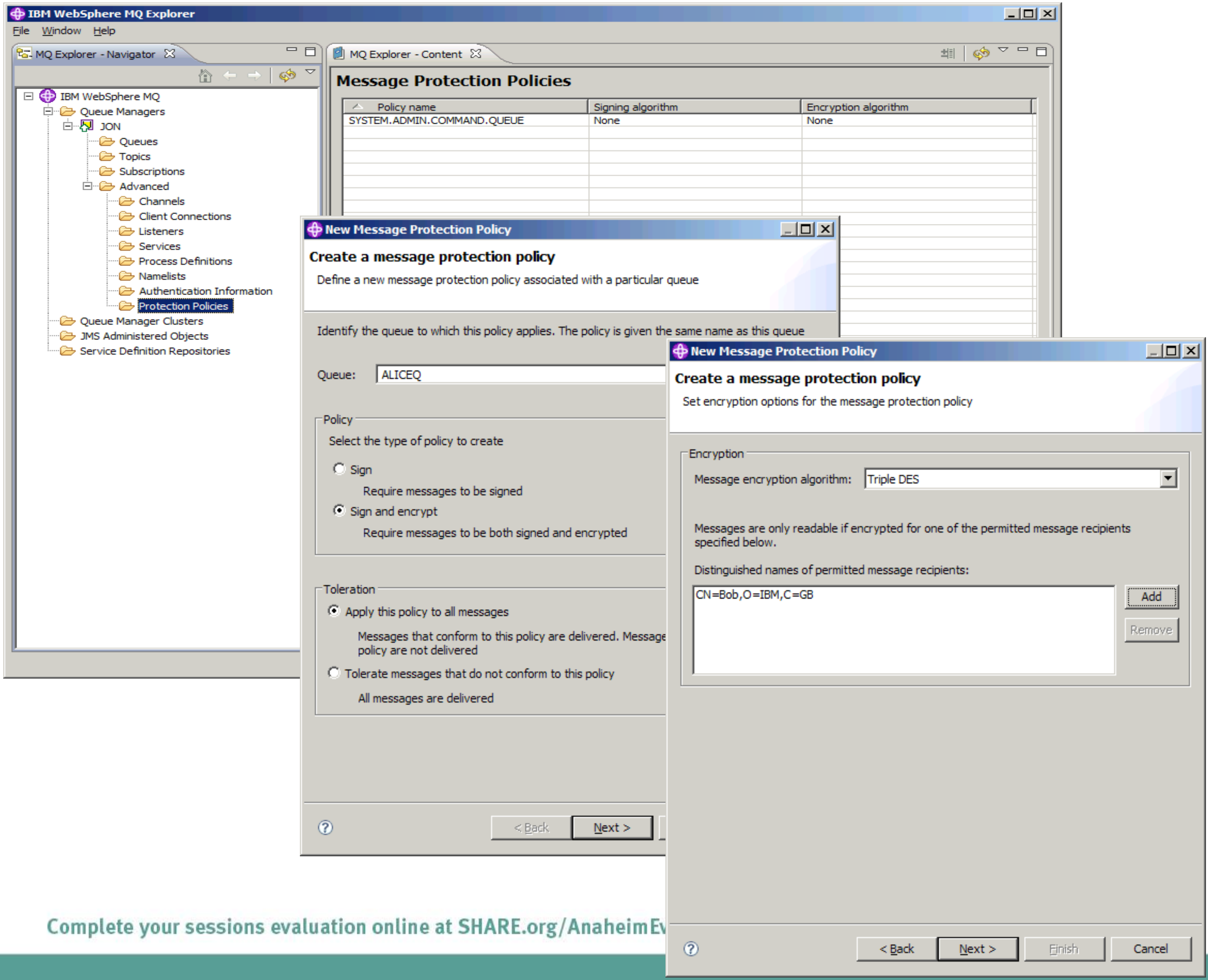
AMS Policies

- 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



Message Protection Policies

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

Create a message protection policy

Define a new message protection policy associated with a particular queue

Identify the queue to which this policy applies. The policy is given the same name as this queue

Queue: ALICEQ

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

Toleration

● 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

Create a message protection policy

Set encryption options for the message protection policy

Encryption

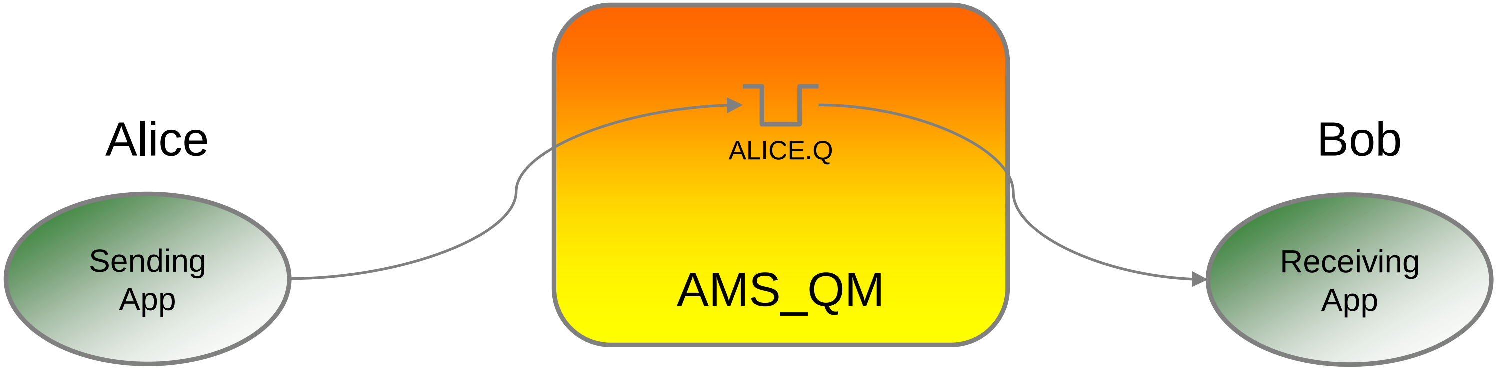
Message encryption algorithm: Triple DES

Messages are only readable if encrypted for one of the permitted message recipients specified below.

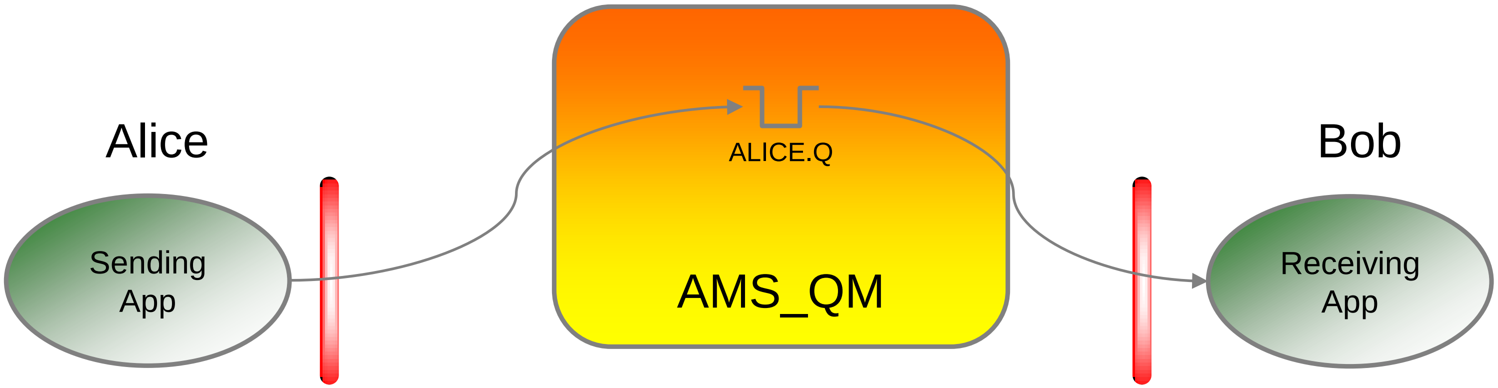
Distinguished names of permitted message recipients:

CN=Bob,O=IBM,C=GB

Securing an MQ Application

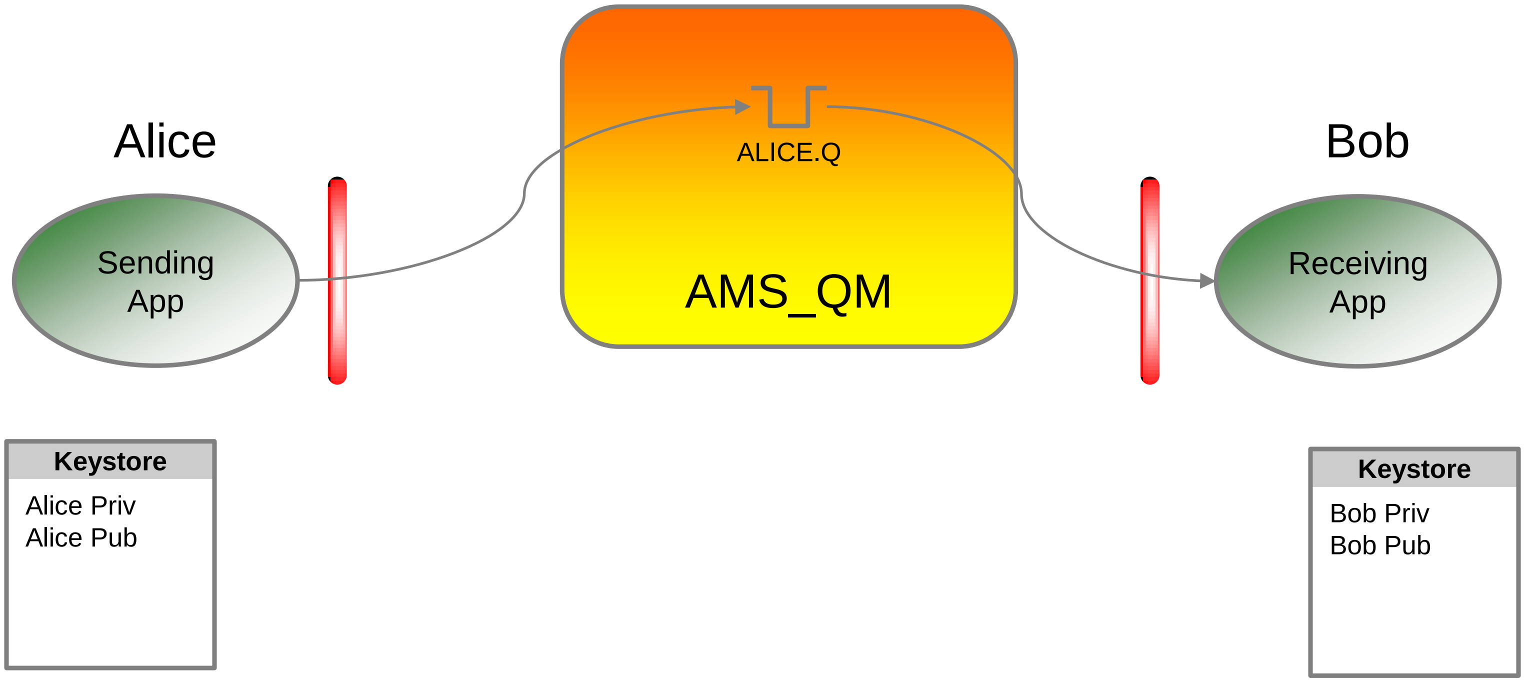


Securing an MQ Application



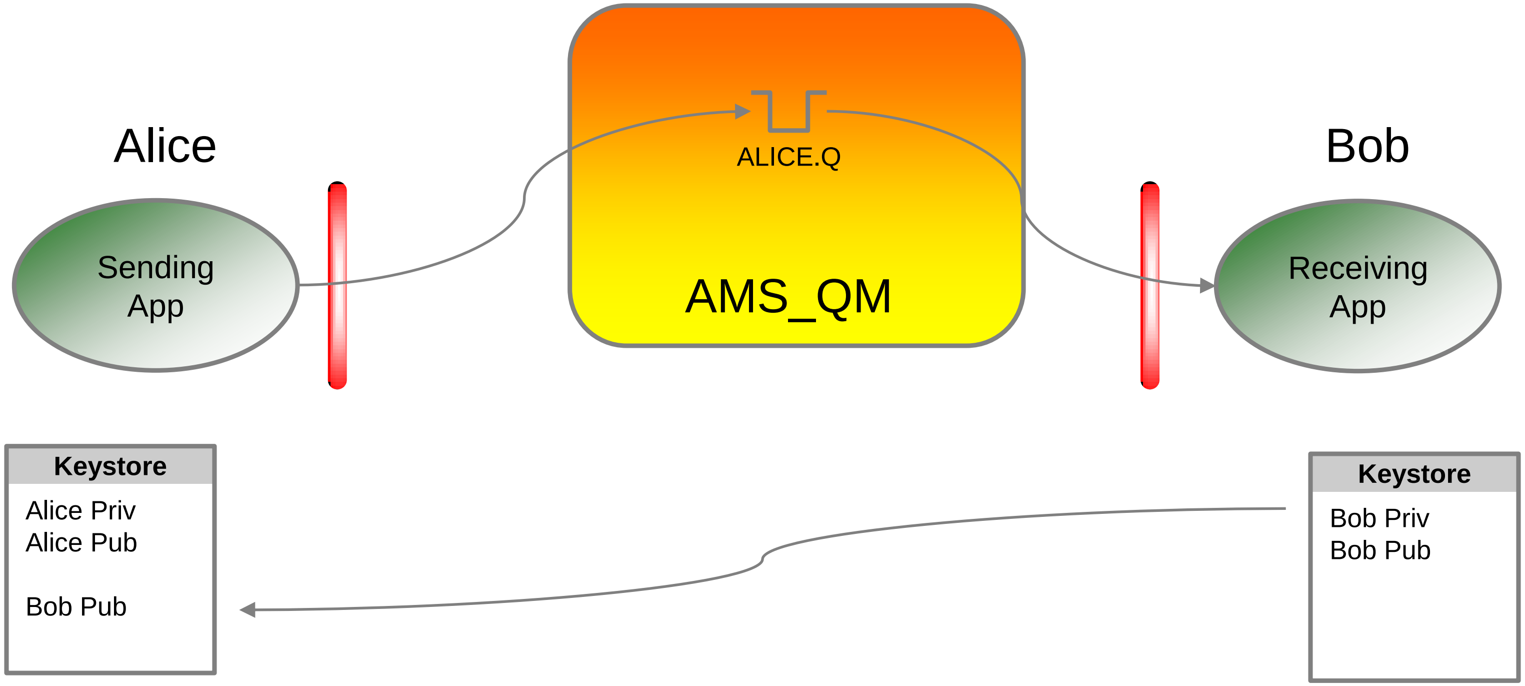
1.Install AMS Interceptor

Securing an MQ Application



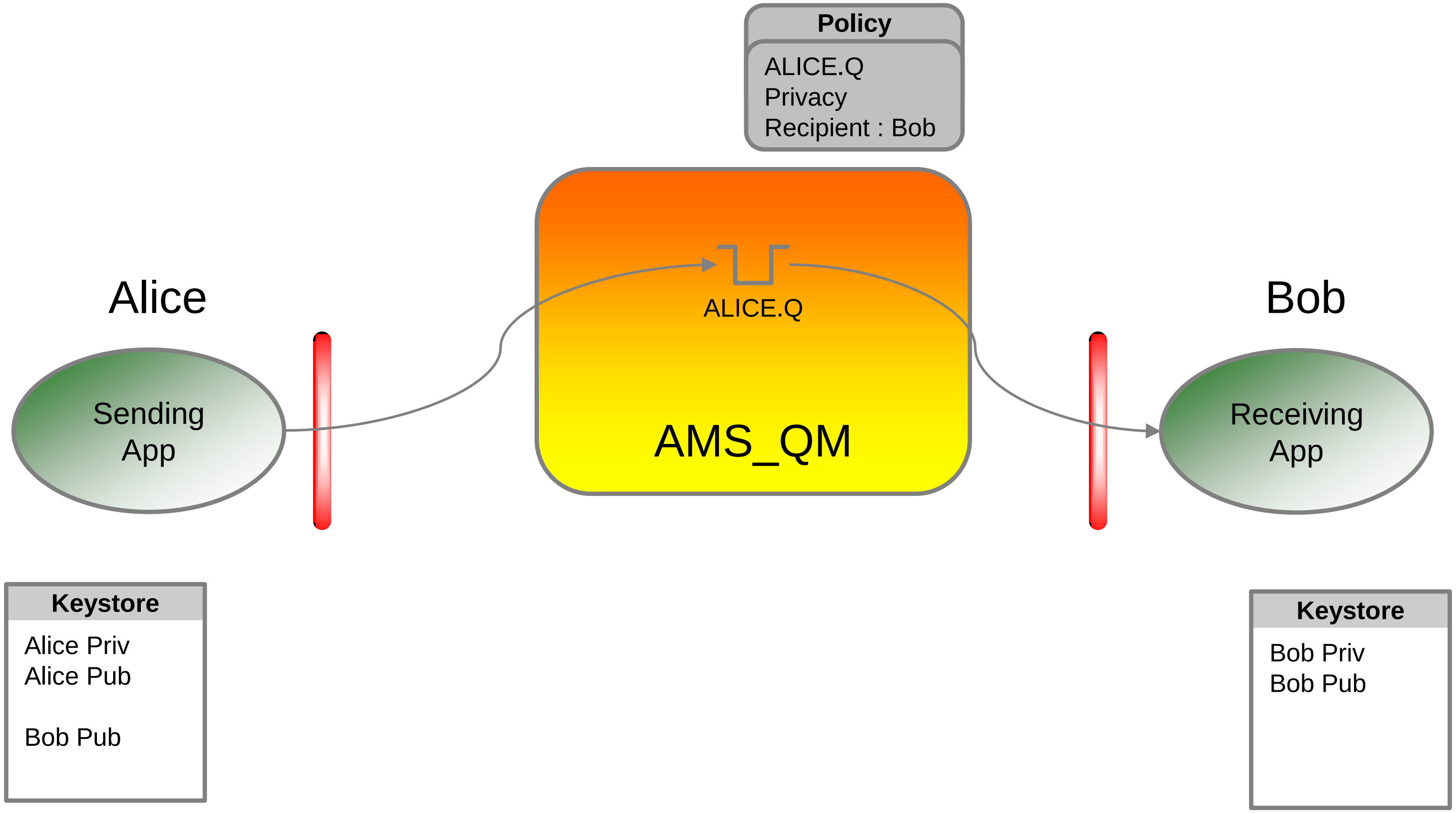
1. Install AMS Interceptor
2. Create public / private key pairs

Securing an MQ Application



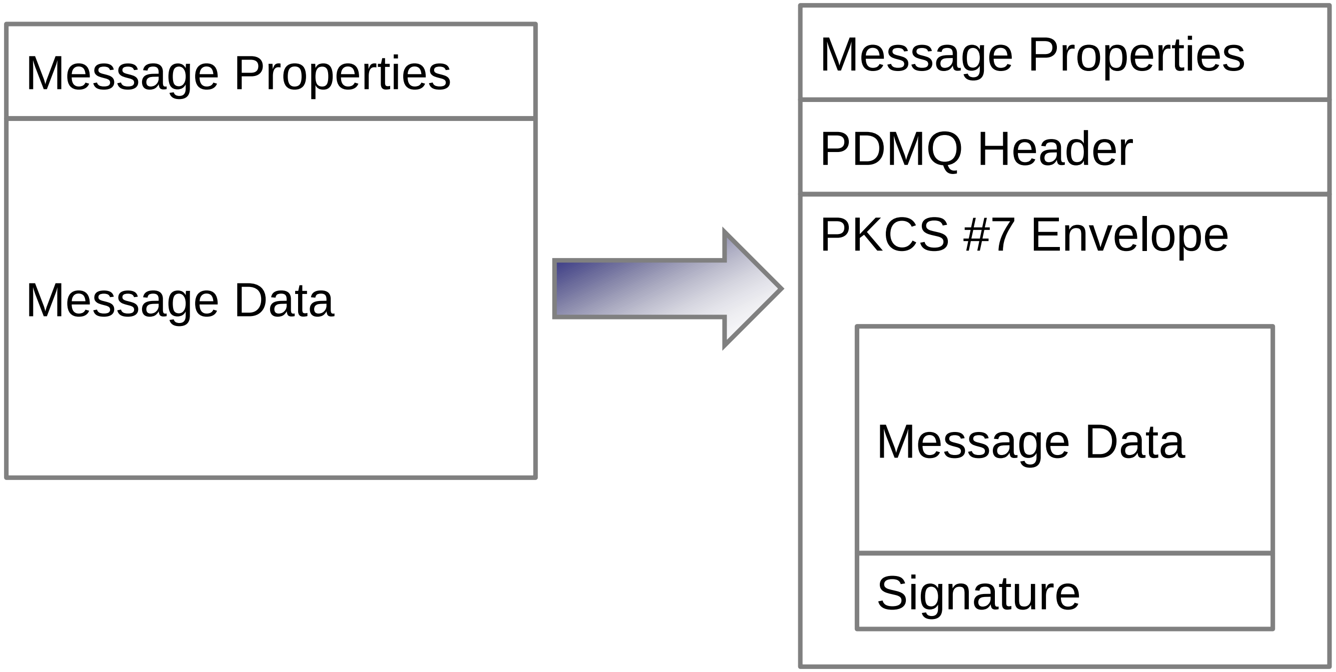
1. Install AMS Interceptor
2. Create public / private key pairs
3. Copy recipient's public key

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

Message Properties

Message Data

AMS Signed Message

Message Properties

PDMQ Header

PKCS #7 Envelope

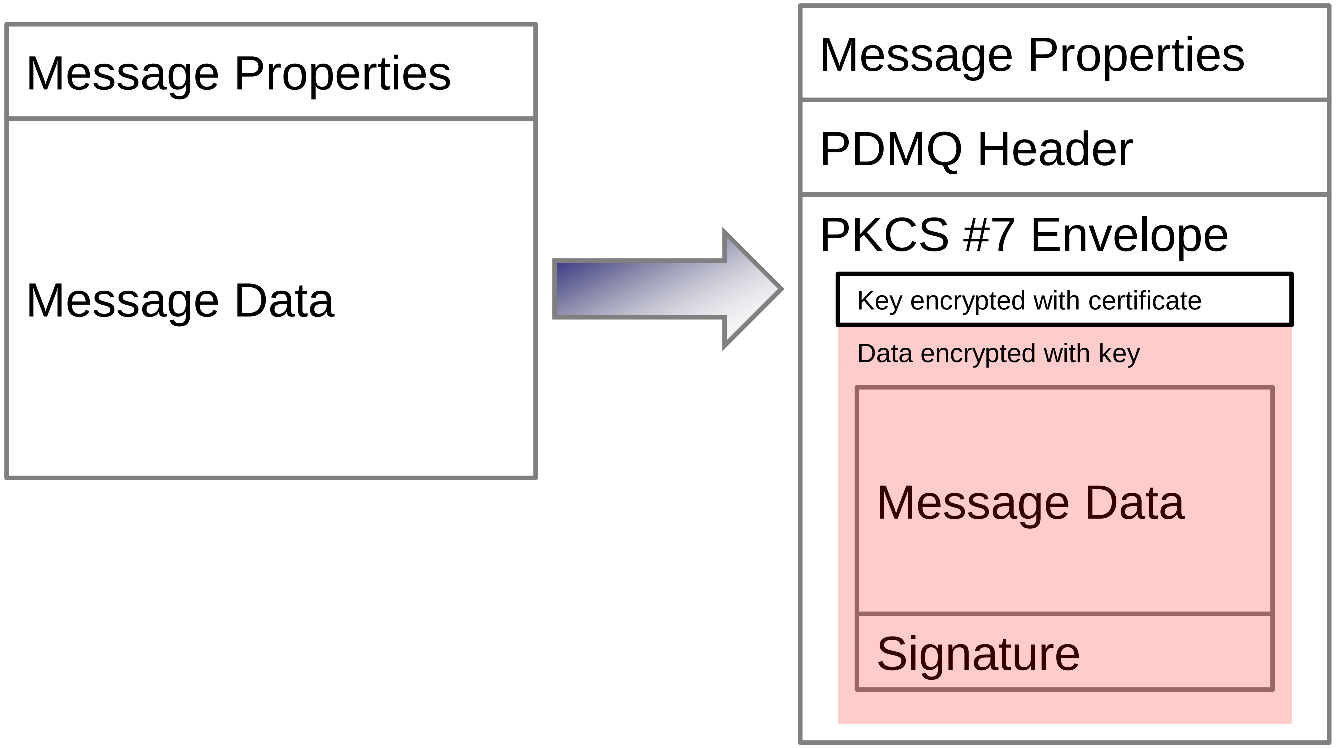
Message Data

Signature

WebSphere MQ AMS : Privacy Message Format

Original MQ Message

AMS Encrypted Message



Message Properties

Message Data

Message Properties

PDMQ Header

PKCS #7 Envelope

Key encrypted with certificate

Data encrypted with key

Message Data

Signature

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

- Quick Start guides (for 7.5)
  - http://pic.dhe.ibm.com/infocenter/wmqv7/v7r5/index.jsp?topic=%2Fcom.ibm.mq.doc%2Fas10170_.htm

WebSphere MQ AMS - The rest of the week ……

	Monday	Tuesday	Wednesday	Thursday	Friday
08:00					Free MQ! - MQ Clients and what you can do with them
09:30	Clustering – the easier way to connect your Queue Managers	MQ on z/OS – vivisection	The Dark Side of Monitoring MQ - SMF 115 and 116 record reading and interpretation		
11:00		Diagnosing problems for Message Broker	Lock it down - WebSphere MQ Security	Using IBM WebSphere Application Server and IBM WebSphere MQ Together	Spreading the message – MQ pubsub
12:15	Highly Available Messaging - Rock solid MQ	Putting the web into WebSphere MQ: A look at Web 2.0 technologies	The Doctor is In and Lots of Help with the MQ family - Hands-on Lab		
01:30	WebSphere MQ 101: Introduction to the world's leading messaging provider	What’s new in the WebSphere MQ Product Family	Extending IBM WebSphere MQ and WebSphere Message Broker to the Cloud	MQ Performance and Tuning on distributed including internals	
03:00	First steps with WebSphere Message Broker: Application integration for the messy	What's new in Message Broker V8.0	Under the hood of Message Broker on z/OS - WLM, SMF and more	The Do’s and Don’ts of z/OS Queue Manager Performance	
04:30	The MQ API for Dummies - the Basics	What the **** is going on in my Queue Manager!?	Diagnosing problems for MQ	Shared Q using Shared Message Data Sets	
06:00			For your eyes only - WebSphere MQ Advanced Message Security	MQ Q-Box - Open Microphone to ask the experts questions	