



#SHAREorg



WebSphere MQ Advanced Message Security


Mark Taylor
IBM Hursley




March 2012
Session 10539




Universal Messaging Backbone


Dynamic network that delivers the **data** you require from wherever it resides to wherever you want it in whatever way you want it at whatever time you want it




1. Best Delivery <ul style="list-style-type: none">Choice of serviceResilience, Integrity, SecurityThroughput, LatencyHigh availability	
2. Anything Anywhere <ul style="list-style-type: none">Any skillsAny trafficAny languageAny environmentAny platform	
3. Scale Dynamically <ul style="list-style-type: none">Start smallGrow incrementallyStretch elasticallyScale admin	




Securing the UMB




- Traditionally, WMQ offers:
 - Integration with operating system security e.g. file/directory/user access
 - Object-level access security via the Object Authority Manager
 - Channel encryption
 - Channel authorisation with certificates
- Some applications require higher degrees of security for message data, for example where regulatory compliance rules apply
- Useful to offer an extension to the MQ family offering this capability
 - Aim to be non-invasive to applications
 - Simple to install
 - Straightforward to configure
 - Use industry standards for encryption




Universal Messaging



WMQ Advanced Message Security



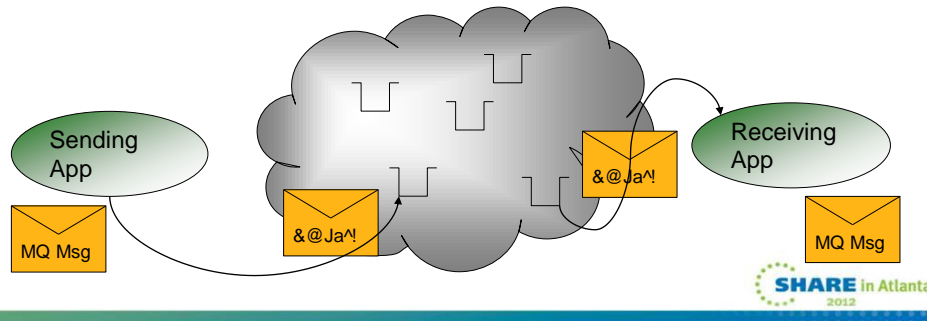
- New product - WMQ Advanced Message Security V7.0.1
 - Available Oct 8, 2010
- Enhances WMQ security processing
 - Provides additional security services over and above base QM
 - Designed to assist with requirements such as PCI DSS compliance
- Application ---> Application protection for point-to-point messaging
 - Sometimes called “end-to-end” or “message-level” protection
- Simplifies regulatory compliance (PCI, HIPAA, etc.) for audit & privacy
- Protects messages even when messages are “at rest”
 - Messages protected from original putter to final getter
 - Messages protected when on a queue and in logs



Message Level Protection



- Enables secure message transfers at application level
- 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 messages, validate the sender
- Assurance that messages can only be viewed by intended recipient(s)
 - When sending confidential information.



Which Messages are Secured



- Not all messages are equal
- May have ...
 - Command and control scenarios
 - Unimportant "status update"
 - Data subject to auditory controls
 - Data subject to standards compliance
 - Credit card data protected by PCI
 - Confidential government data
- Expectation that only limited queues are protected on each qmgr
- System architecture designs need to consider message content



WMQ AMS - Key Features



- Secures sensitive 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
 - Cannot view message contents in logs or queues
- Messages from existing applications are transparently secured
 - No changes needed to existing applications
- Industry standard asymmetric cryptography used to protect messages
 - Uses Public Key Infrastructure (PKI) to protect messages
 - Uses digital certificates (X.509) for applications



WMQ AMS – Simplicity and Integration



- No prereq products
 - Significantly simplified installation and configuration compared to predecessor product
 - Up and running in minutes ...
- Works in conjunction with SSL
 - Can choose to use either or both depending on your requirements
- Works in conjunction with WMQ authorisation model (OAM and SAF)
- No changes required to WMQ applications
 - Works with local applications and clients, including Java
 - Support for WMQ V6 and V7
- No changes required to existing object definitions
- Fine-grained policies to define which queues are protected and how
- Administratively controlled policies
 - Command line
 - MQ Explorer



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
 - CICS Bridge, IMS Bridge, IMS SRB apps are not supported

- Supports MQ6, MQ7, MQ7.1 queue managers (JMS requires V7 jars)



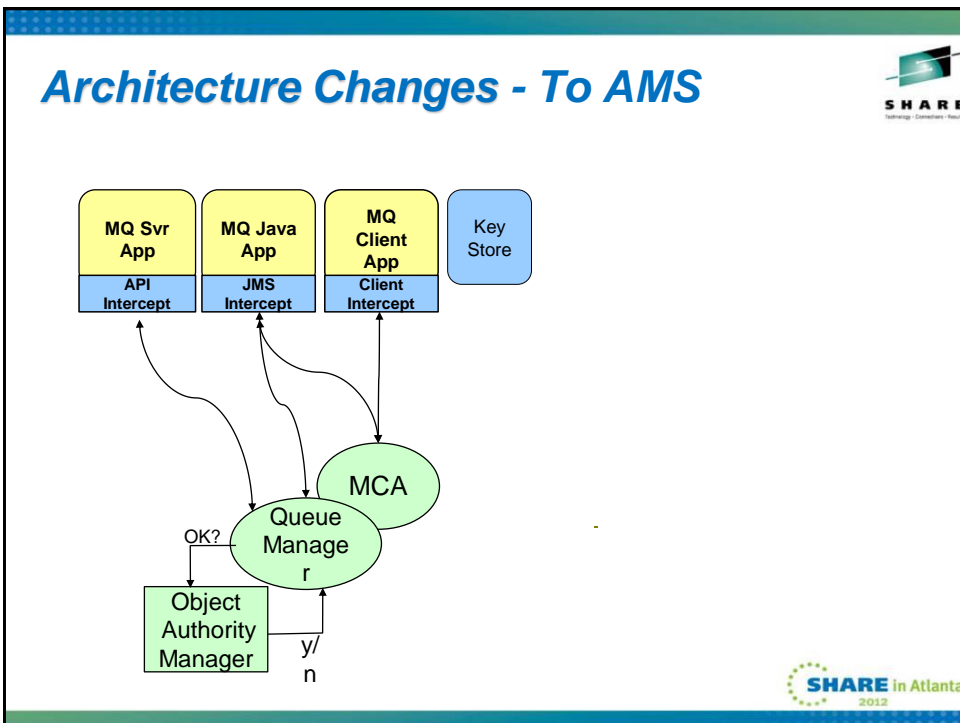
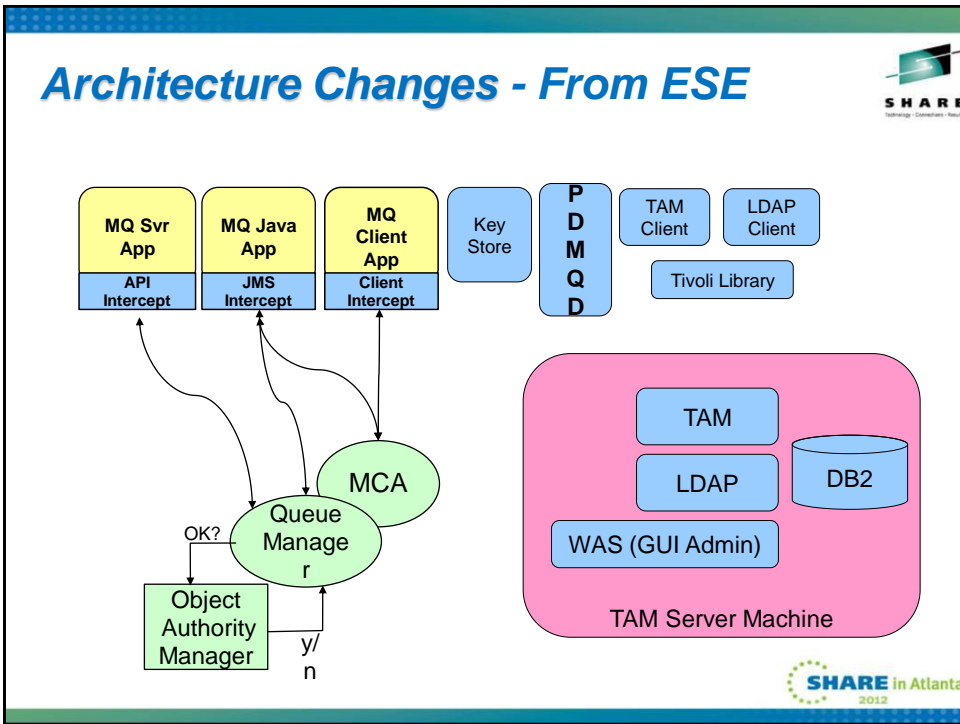
WMQ vs WMQ AMS

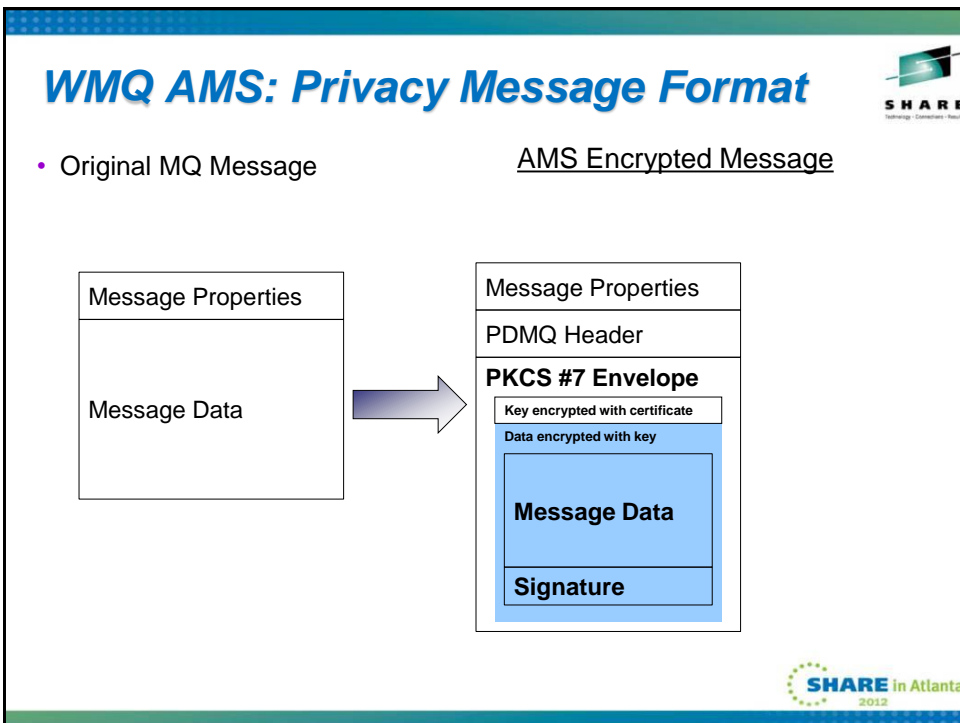
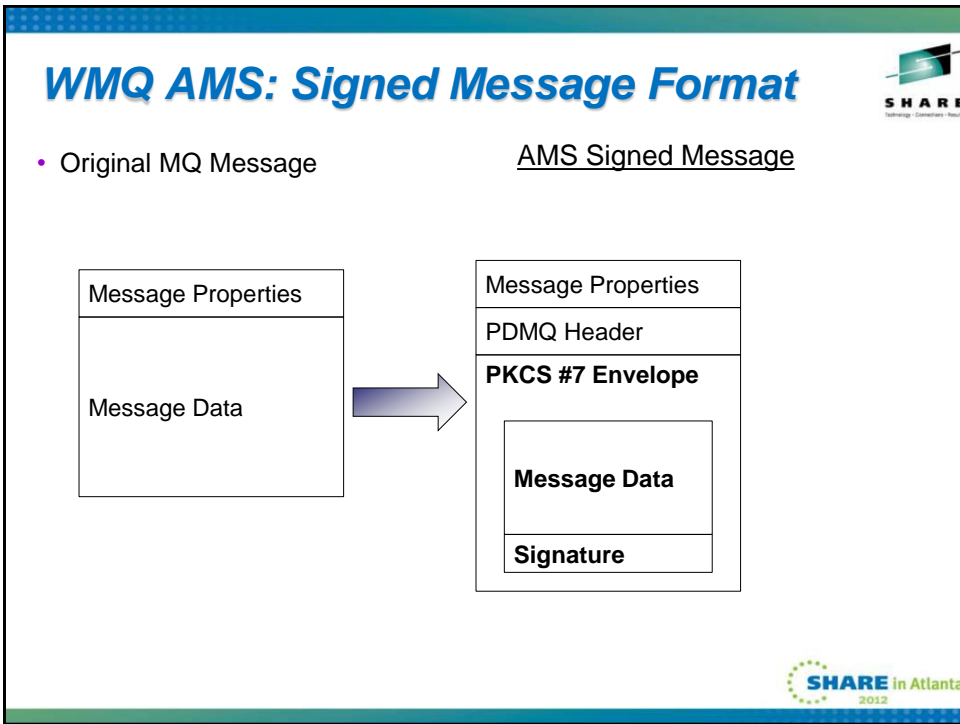


- WebSphere MQ
 - Authentication (OS for local apps or peer authenticated SSL for client apps)
 - Authorisation (OAM on distributed, SAF on z/OS)
 - Auditing (event messages)
 - Integrity (SSL for channels)
 - Privacy (SSL for channels)

- WebSphere MQ AMS
 - As above, additionally:
 - Integrity (Digital signature of message content)
 - Privacy (Message content encryption)







A Protected Message

Message 1 - Properties

General
Report
Context
Identifiers
Segmentation
Data

Data length: 1270

Format:

Coded character set identifier: 437

Encoding: 546

Message data: PDMQ

Message data bytes:

```

00000 50 44 4D 51 02 00 00--68 00 00 68 00 00 00 |PDMQ...h...h...
00010 08 00 00 00 B5 01 00 00--26 00 00 00 00 00 00 |...|...6...
00020 4D 51 53 54 52 20 20--00 00 00 00 00 00 00 00 |MQSTR...
00030 00 00 00 00 00 00 00 00--00 00 00 00 00 00 00 |...
00040 00 00 00 00 00 00 00 00--00 00 00 00 00 00 00 |...
00050 00 00 00 00 00 00 00 00--00 00 00 00 00 00 00 |...
00060 00 00 00 00 00 00 00 00--30 82 04 8A 06 09 2A 86 |...|...0...
00070 48 86 F7 0D 01 07 03 AD--82 04 78 30 82 04 77 02 |H...|...A...|...|...
00080 01 00 31 81 CF 30 81 C0--02 01 00 30 35 30 29 31 |...|...40...|...|...050|...
00090 08 30 09 06 03 55 04 06--13 02 55 53 31 0C 30 0A |...|...U...|...US10|...
000A0 06 03 55 04 0A 13 03 49--42 4D 31 0C 30 0A 06 03 |...|...|...IBM100...
000B0 55 04 03 13 03 62 6F 62--02 08 AD AD 1B 87 B3 0D |...|...bob...|...|...
000C0 4E 66 30 0D 06 09 2A 86--48 86 F7 0D 01 01 01 05 |Nf0D...
000D0 00 04 81 80 71 1D 54 1A--A7 F2 67 98 7D 70 EE 5B |...|...gDT...2g...|...p...
000E0 22 12 FB FF 40 0C DA 32--9F 4F 3D 6C 04 3B DF C3 |...|...V...|...2...|...|...
000F0 96 CC FA A5 24 71 F4 07--A3 80 B2 A1 B4 C1 1E B4 |...|...Nsq...|...|...|...
00100 03 4F 4D 99 8F F3 38 38--60 A5 D7 C7 8E EE F9 BA |...|...OM...|...|...e...|...
00110 94 DA CD 90 B2 91 B5 7A--73 C3 C0 34 5B 92 E6 6E |...|...|...|...|...|...|...
00120 3E AD E0 51 1B 81 FD 9F--06 06 82 85 F6 06 D9 66 |...|...|...|...|...|...|...
00130 25 AA 66 95 F1 DC A5 91--B7 0F 5B 6B 7E DE D3 |...|...|...|...|...|...|...
00140 BA 55 25 38 BD 20 DE F2--30 B7 D9 DC 5A 36 76 40 |...|...|...|...|...|...|...
00150 D5 53 BE CD 30 82 03 9E--06 09 2A 86 48 86 F7 0D |...|...|...|...|...|...|...
00160 01 07 02 30 1D 06 09 60--86 48 01 65 03 04 01 2A |...|...|...|...|...|...|...
00170 04 10 84 F4 74 FE 78 40--80 02 47 09 46 5D A2 86 |...|...|...|...|...|...|...

```

Message data is encrypted in TEST.Q. AMS has added the header PDMQ, which includes Alice's pub key and dig cert.

SHARE in Atlanta 2012

Protected Messages

- New message size is approximately ...
 - 1280 + Original Length + (200*Recipient Count) bytes
- May affect max lengths configured on queues and channels
- Data conversion done by queue manager after protection removed
- Bad messages sent to SYSTEM.PROTECTION.ERROR.QUEUE
 - Sender did not have the authority to write to the queue
 - Sender's certificate was not valid
 - AMS was unable to decrypt the message
 - A policy mismatch occurred. For example, the sender used integrity instead of the expected quality of protection of privacy, or used the wrong algorithm
 - The message was sent without expected AMS protection
- Messages moved here have a DLH attached
 - So standard dead-letter handlers can process them

SHARE in Atlanta 2012

Message Protection Policies - Overview



- Created or updated or removed by command 'setmqsp1'
 - Or by AMS plug-in for MQ Explorer (GUI)
- Policies are stored on queue SYSTEM.PROTECTION.POLICY.QUEUE
- Each protected queue can have only one associated policy
- Display policies with command 'dspmqsp1'
 - Can be displayed in "setmqsp1" format for easy backup/restore
- Applied based on queue name as opened by application
 - can deal with alias and remote queues



Message Protection Policies - Detail



- 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
- If encryption set to NONE, then only signing is done
- Toleration flag (-t) assists with phased introduction of AMS

```
setmqsp1
-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>
-t <0|1>
```



Message Protection Policies - 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 sends messages to SYSTEM.PROTECTION.ERROR.QUEUE

```
setmqsp1
-m QM
-p Q.PRIVACY
-s SHA1
-e AES128
-r 'CN=pdmqss,O=tivoli,C=US'
-r 'CN=Vicente
  Suarez,OU=ISSW,O=IBM,
  L=Hursley,C=GB'
```



Publish/Subscribe with AMS



- AMS does not directly support MQv7 publish/subscribe features
- Main reason for this is the decoupling of publisher from subscriber
 - The publisher does not know who the recipients are going to be
 - Dynamic changes to subscription list
 - Only the queue manager knows – and does not have access to publisher's certificates
- However, a degree of support is possible
 - Use QALIAS to point to a TOPIC
 - Set a policy on the QALIAS that lists all authorised subscribers
 - More like a distribution list but OK for some scenarios
- Question: what would user requirements be for greater pub/sub?
 - Signed messages only?
 - Using qmgr credentials sometimes, but not publisher?
 - How dynamic?



Administration: MQ Explorer Plug-in

IBM WebSphere MQ Explorer

MQ Explorer - Navigator

MQ Explorer - Content

Message Protection

Policy name

- SALES.AMERICA
- SALES.ASIA
- SALES.EUROPE

Last updated: 15:27:56

SALES.EUROPE

General

Apply this policy to all messages

Messages that conform to this policy are delivered. Messages that do not conform to the policy are not delivered

Tolerate messages that do not conform to this policy

All messages are delivered

Signing

Message signing algorithm: SHA1

Accept signed messages from any originator

Only accept signed messages from the message originators listed below

Distinguished names of permitted message originators:

CN=Robert Smith,OU=IBM Software Group,O=IBM,C=UK

Remove

Encryption

Message encryption algorithm: AES 128

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

Distinguished names of permitted message recipients:

CN=Robert Smith,OU=IBM Software Group,O=IBM,C=UK

Add

Remove

Apply

OK Cancel

Callouts:

- Double click policy to view properties
- Right click node to create a new policy
- Tolerance mode allows messages not conforming to policy
- Name of policy is not editable once created
- Removes the selected DN's from the list on left
- Pops up a dialog asking the user to supply a DN
- If an encryption policy is specified, message will be encrypted and at least one DN must be entered

SHARE in Atlanta 2012

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 must also contain trusted certificates to validate message signers or to obtain the public keys of encrypted message recipients
- Several types of keystore are supported: CMS, JKS and JCEKS.

SHARE in Atlanta 2012

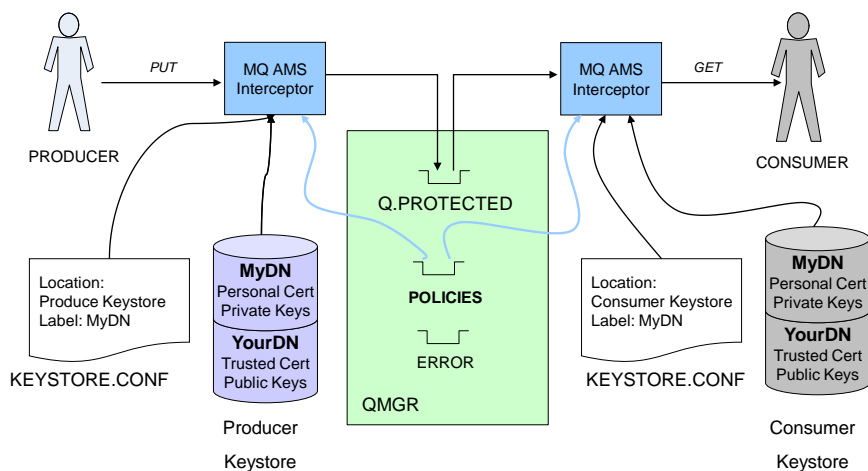
AMS Configuration Files

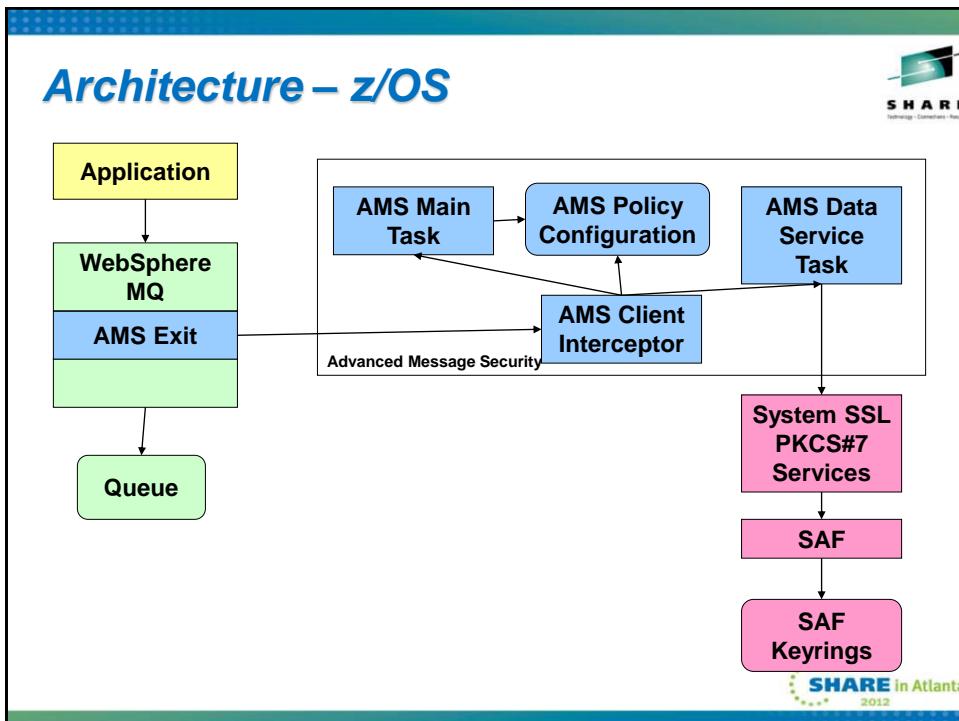


- Each user of AMS requires a configuration file.
 - Type of keystore: CMS (for C programs) and JKS, JCEKS (for Java)
 - Location of the keystore
 - Label of the personal certificate
 - Passwords to access keystore and private keys
 - Password can be encrypted in the configuration file
- Configuration file located using one of the following methods:
 - Environment variable MQS_KEYSTORE_CONF=<path to conf file>
 - MQS_KEYSTORE_CONF=C:\Documents and Settings\Bob\AMS\keystore.conf
 - Checking default locations and file names
 - Platform dependent. For example in UNIX: "\$HOME/.mqs/keystore.conf"
- Configuration file should be secured with OS permissions
- Also a configuration file ("routing file") for logging and tracing



Architecture - Distributed Platforms

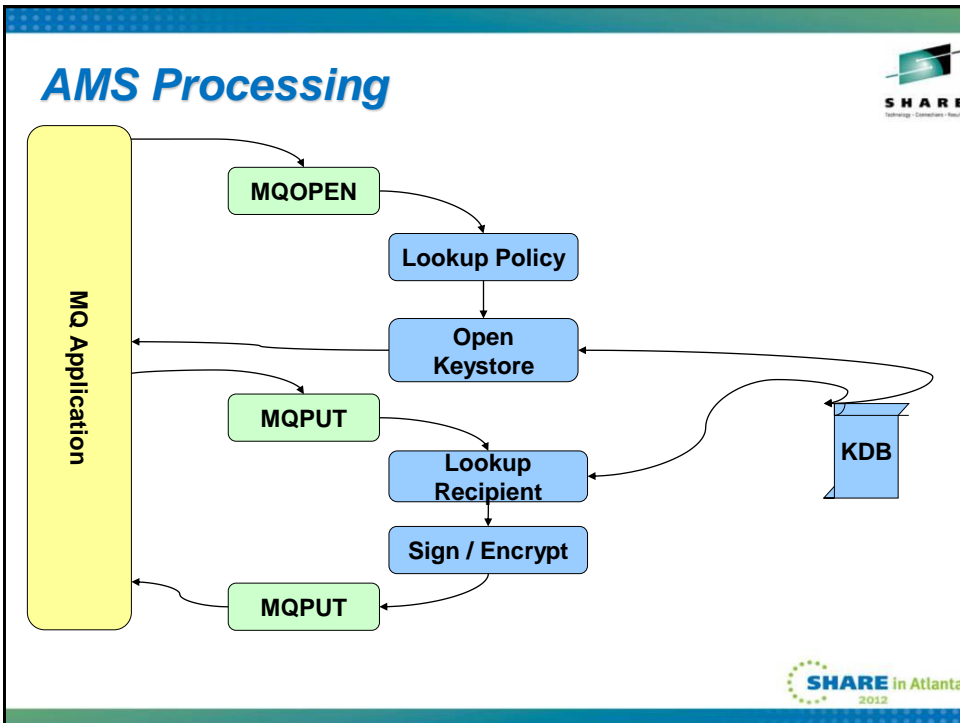
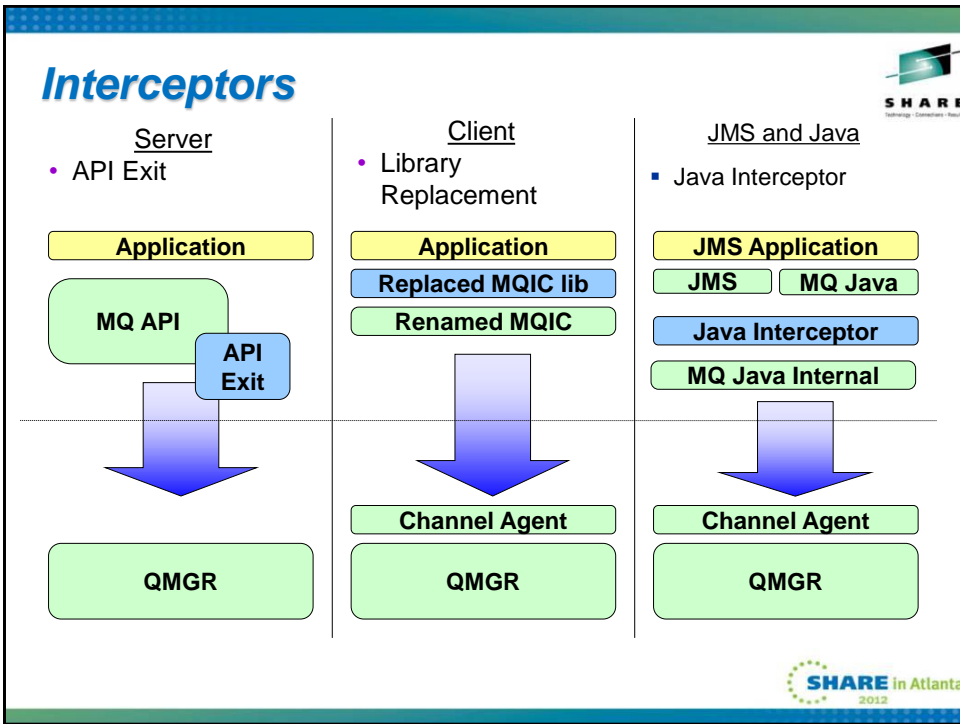




AMS Interceptors

- 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
 - Server interceptor for local (bindings mode) MQI API and Java applications.
 - Implemented as queue manager API exit.
 - MQI API client interceptor for remote (client mode) MQ API applications.
 - MQ AMS interceptor imbedded in MQ client code.
 - 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.
- Scripts provided to install and configure these interceptors
 - For example, update qm.ini for the API Exit

Logos for SHARE and SHARE in Atlanta 2012 are visible in the top right and bottom right corners of the slide.



WMQ AMS Deployment

The diagram illustrates the deployment of WebSphere Message Queues (WMQ) with Advanced Message Security (AMS). It shows two parties, Alice and Bob, separated by a network barrier. Alice has a 'Sending App' and Bob has a 'Receiving App'. They are connected via a central 'AMS_QM' queue. A specific queue 'APP.Q' is shown within the AMS_QM. A policy is defined for 'APP.Q' with the privacy recipient set to 'Bob'. Both Alice and Bob have their own 'Keystore' files. Alice's keystore contains 'Alice Priv', 'Alice Pub', and 'Bob Pub'. Bob's keystore contains 'Bob Priv' and 'Bob Pub'. Arrows indicate the flow of data from Alice's app to the queue and then to Bob's app, and the flow of keys from both keystore files to the queue.

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

SHARE
Technology · Connected · Ready

SHARE in Atlanta
2012

WebSphere MQ AMS and FTE

The diagram illustrates the deployment of WebSphere Message Queues (WMQ) with Advanced Message Security (AMS) and Full Text Encryption (FTE). It shows two parties, Alice and Bob, separated by a network barrier. Alice has a 'Sending AGENT' and Bob has a 'Receiving AGENT'. They are connected via a central 'AMS_QM' queue. A specific queue 'SYSTEM.DATA.FTE.BOB' is shown within the AMS_QM. A policy is defined for 'SYSTEM.DATA.FTE.BOB' with the privacy recipient set to 'Bob'. Both Alice and Bob have their own 'Keystore' files. Alice's keystore contains 'Alice Priv', 'Alice Pub', and 'Bob Pub'. Bob's keystore contains 'Bob Priv' and 'Bob Pub'. Arrows indicate the flow of data from Alice's agent to the queue and then to Bob's agent, and the flow of keys from both keystore files to the queue.

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

SHARE
Technology · Connected · Ready

SHARE in Atlanta
2012

Using Message Broker with AMS



- Remember that messages can only be read by authorised applications
- If MB used purely as a router, then it does not need to decrypt messages
 - Can do true end-to-end protection
 - MQ Input and Output queues do not need policy settings
- If MB does work based on message content, or changes content, then it has to be considered an endpoint for AMS
 - "End-to-middle" protection
 - Still achieves goal of no unprotected message data on queues or in logs
- Many MB scenarios only have MQ on one side of a flow
 - Security for other protocols can be done by MB eg WS-Security



Responding to Regulatory Compliance



<p><i>Large Food & Drug Retailer in North America</i></p>	<ul style="list-style-type: none"> ➢ Company had exposure to loss of customer personal healthcare information and personal credit card data ➢ A level 1 retailer with large volumes of personal data to deal with the need to secure their systems across multi-channels
---------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Solution:

- Implementing WMQ AMS for encryption of data at rest in queues.
- WebSphere DataPower XS40 for firewall and data encryption for data in motion.

Solution Benefit:

- No need to modify applications, able to leave existing systems intact and add security updates quickly at the same time as continuing normal operation.
- By encrypting the data and limiting access to the applications the possibility of personal data being stolen and will be minimized.



V7.0.1.2 Enhancements



- Available January 2012
- Supports WMQ V7.1
 - Extends WMQ V7.1 Application Activity Trace to show applied AMS policy
- Supports SHA-2 Digest algorithms
- Provides Command and Configuration Events for Policy changes
 - Audit trail of who has changed configuration



SOA Sandbox for AMS discovery



- Try AMS and see what it can do for you
 - <http://www.ibm.com/developerworks/downloads/soasandbox/mqsecurity.html>
- SOA Sandbox main page for offerings designed to give you hands-on experience of various IBM products without having to install them
 - <http://www.ibm.com/developerworks/downloads/soasandbox/.html>



Summary



- WebSphere MQ Advanced Message Security V7.0.1
- Simplifies regulatory compliance
- Provides additional security over and above base MQ
- Complements (does not replace) existing MQ security
- Works with all levels of MQ in service (MQ 6 & 7)
- Does not require application changes
- Policies applied on individual queues

