WebSphere User Group | WebSphere Integration User Group

A Client Story: PCI Compliance with WebSphere MQ Advanced Message Security

Richard Gamblin
richard.gamblin@uk.ibm.com
WebSphere Technical Software Specialist
IBM System z Software | zChampion

Objectives & assumptions for this PCI/ WMQ AMS Session

- Primary objectives
  - (V. brief) Reminder of the PCI-DSS requirement
  - Introduction to WebSphere MQ Advanced Message Security (WMQ AMS)

- Secondary objectives
  - Consider the implications of PCI & WMQ AMS as part of a File Transfer solution
  - Overview of WebSphere MQ File Transfer Edition

- Some assumptions…
  - Everyone in the room is familiar with WebSphere MQ
  - There are some PCI-DSS / security experts in the room
    (hint: I'm not one of them!)

Agenda for this PCI/ AMS Session

- WebSphere MQ Family Strategy
- Customer story (part 1): Requirements for PCI compliance
  - Overview of Payment Card Industry Data Security Standard (PCI-DSS)
  - Support from existing WMQ security
- WebSphere MQ Advanced Message Security
  - What is it? What does it do?
  - How does it work?
- Customer story (part 2): '*this looks great – can we use it for our files?*'
  - The challenge: how to secure payment card info in file-base traffic
  - A quick overview of WebSphere MQ File Transfer Edition (WMQ FTE)
  - Integrating with WMQ AMS
- Summary & Questions

WebSphere MQ Vision

Universal Messaging Backbone

Skills

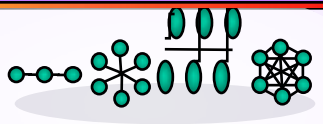
- Languages
  - *COBOL, C/C++, RPC*
  - *Java, JEE, JMS*
  - *.NET, C#, VB, WCF*
  - *AJAX, Perl, Python…*
- Orientations
  - *Service*
  - *Batch*
  - *File*
  - *Message*
  - *Resource…*
- Mindsets
  - *WSDL, XML, WS-**
  - *REST, MEST, KISS*

End-Points

- Vendor Platforms
  - *JEE, .NET, etc*
- Operating Systems
  - *Exploitation & Support*
- Applications
  - *SAP, Siebel, etc…*
- Devices
  - *Mobile, Wireless, PoS, Sensor, Actuator, RFID…*
- Web services
  - *SOAP, WSDL, WS-RM, WS-N…*
- Web 2.0
  - *HTTP, AJAX, REST,…*
- Appliances

Qualities-of-Service

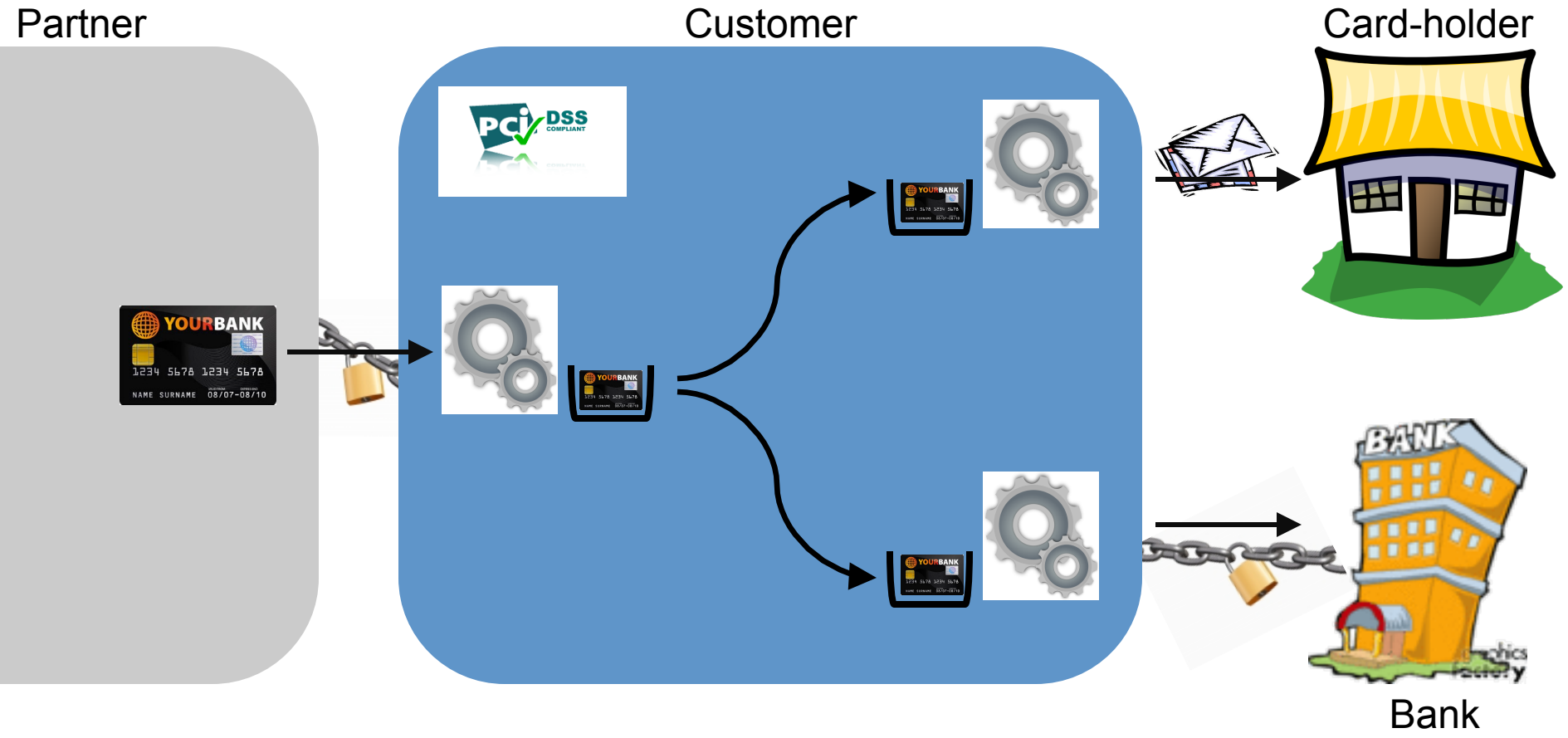
- Transactional
- Guaranteed
- Persistent
- At-Most-Once
- Replay
- At-least-once
- Best-Effort
- Fire-and-Forget
- Request-Reply
- Secure
- Lowest Latency



Delivery Styles

- Client-Server
- Backbone
- Point-to-Point
- Peer-to-Peer
- Publish/Subscribe
- Grid
- Bus
- Multicast
- Unicast

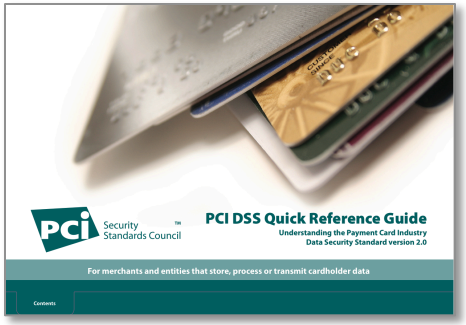
Customer story: requirements for PCI-DSS Compliance



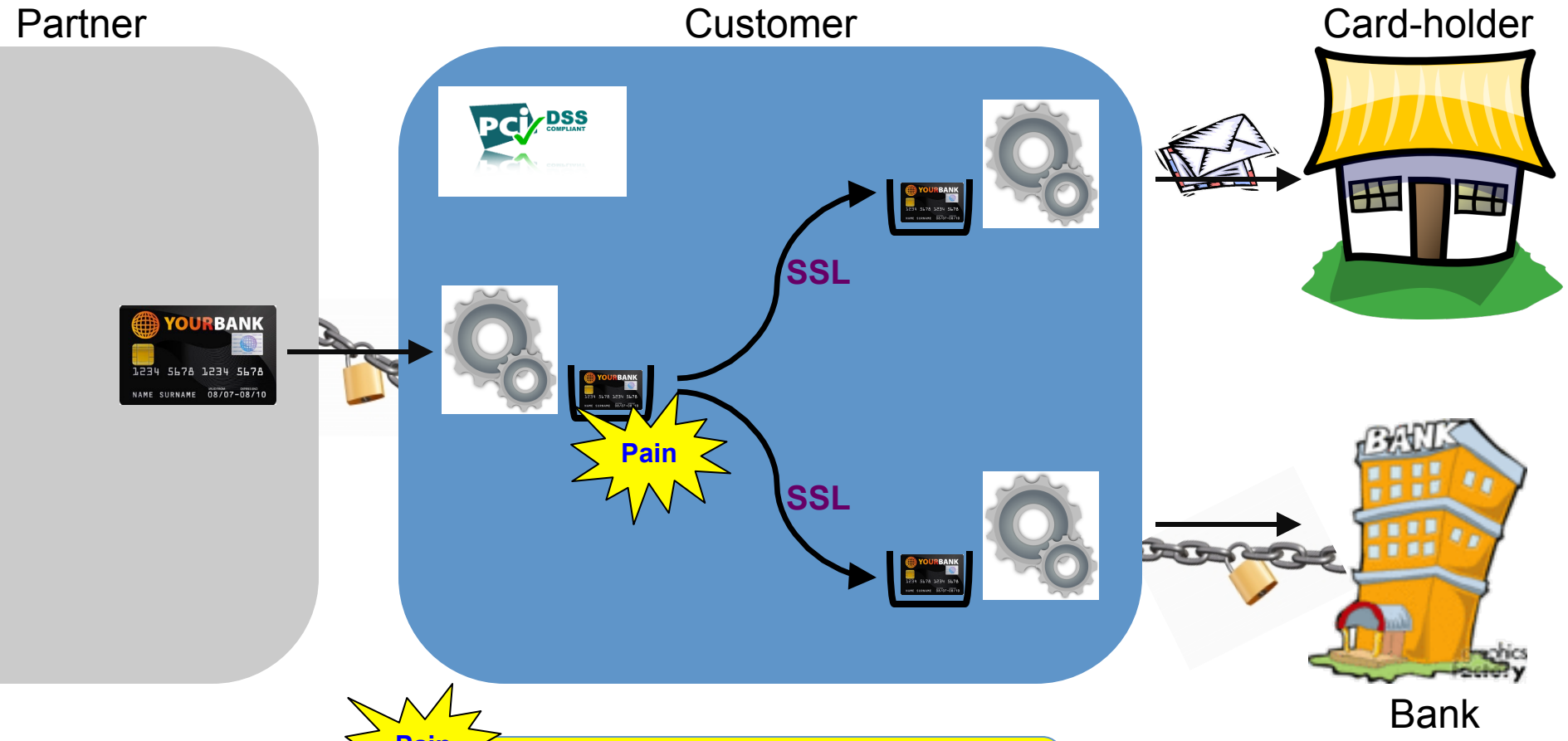
Payment Card Industry Data Security Standard (PCI DSS)

- Payment Card Industry Data Security Standard (PCI DSS) is a global security program that was created to increase confidence in the payment card industry
- All merchants and service providers that store, process, use or transmit payment cardholder data must comply with PCI Data Security Standard (DSS).

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel



Customer story: requirements for PCI-DSS Compliance

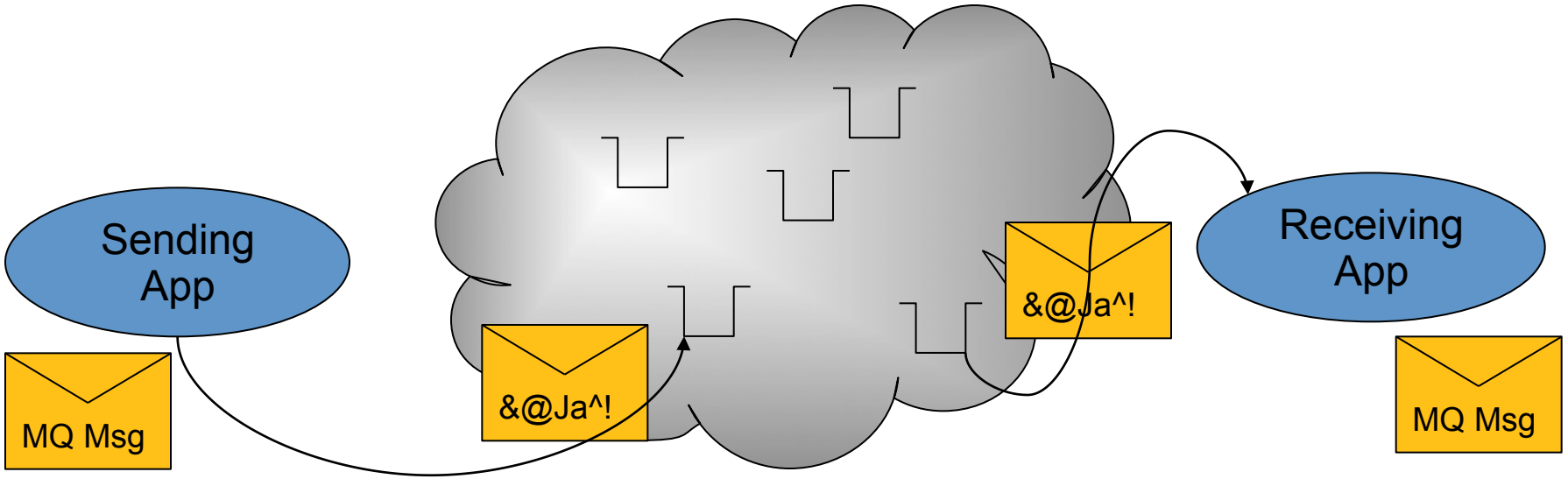


WebSphere MQ Advanced Message Security

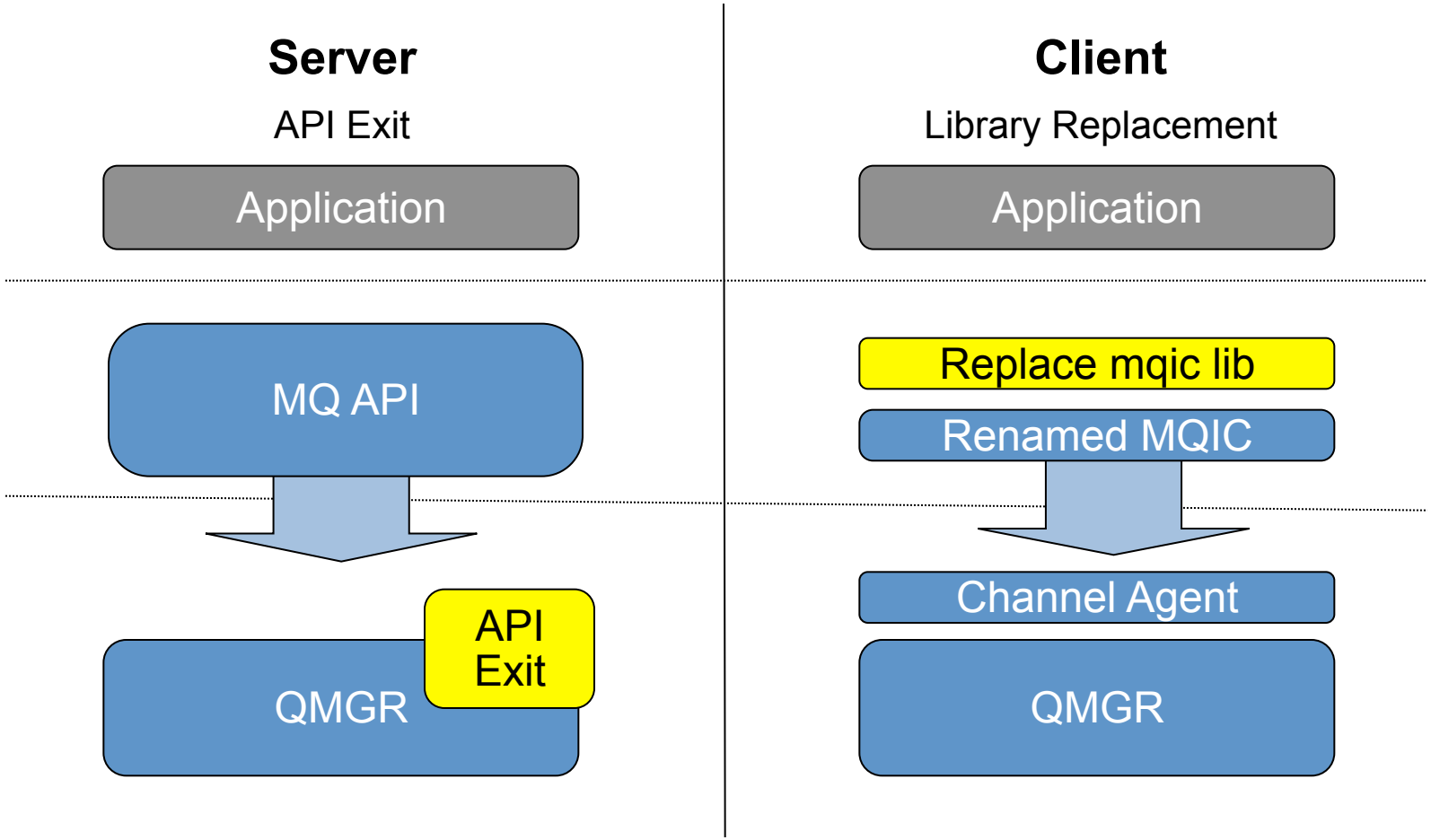
Overview

What is WebSphere MQ Advanced Message Security?

- Adds *message-level* security to existing WebSphere MQ (V6 & V7)
- Protects customer data application-to-application, *at rest on queue* & in transit
- Drops in to existing MQ environments with *no change* to applications
- Simplifies regulatory compliance (PCI, HIPAA, SOX, et al.) for audit & privacy

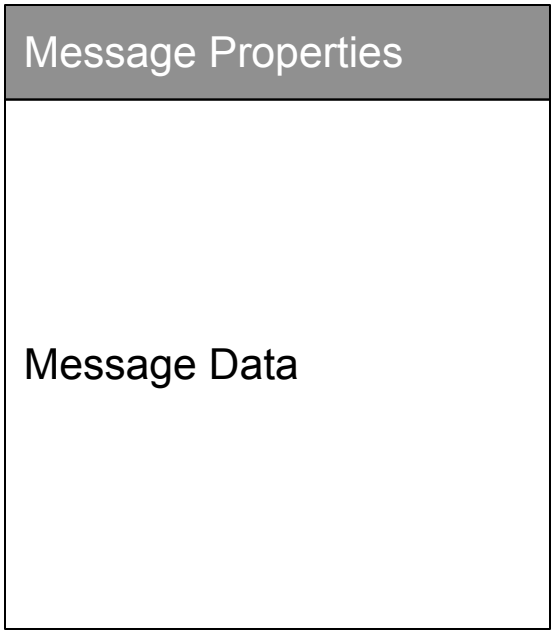


Existing applications use it transparently: no changes!

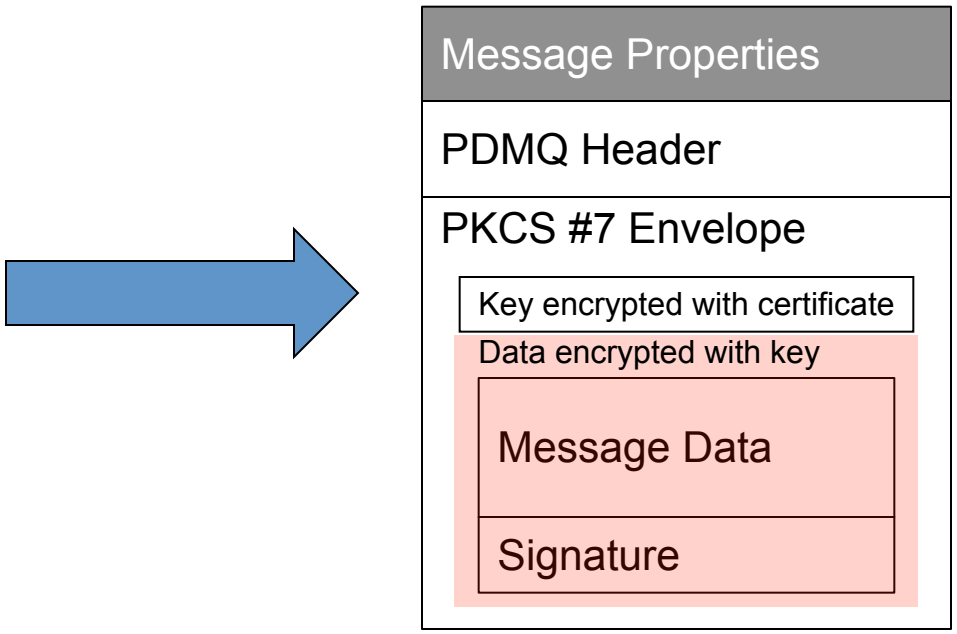


WMQ AMS work places your sensitive data in a secure envelope

Original MQ Message

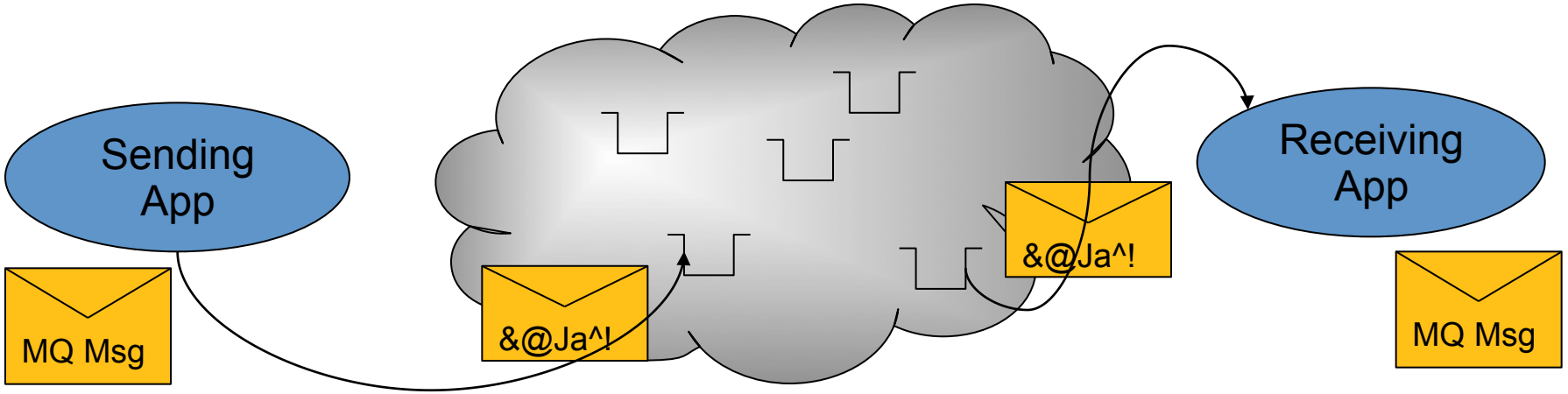


AMS Protected Message



WMQ AMS: enhances existing WMQ network, providing

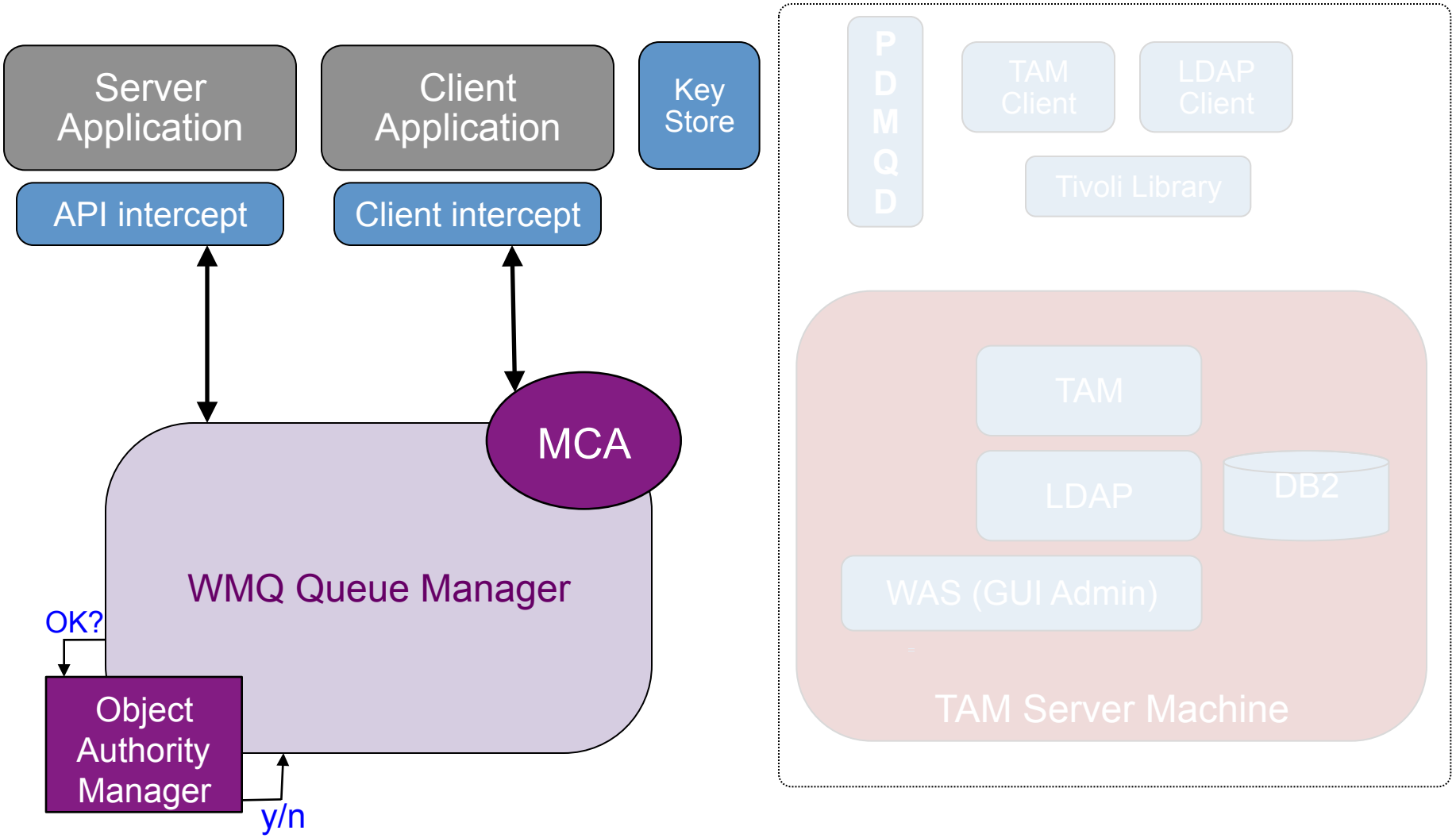
- Application-to-Application secure message transfers
  - Privacy & integrity protected in transit AND at rest in queues (unlike SSL)
- Assurance that messages have not been altered in transit
  - e.g. ensure the payment amount does not change before reaching the receiver
- Assurance that messages originated from the expected source
  - Receiver validate sender's X.509 signature. Rejects rogue messages
- Assurance that messages can only be viewed by intended recipient(s)
  - When sending confidential information, even MQ admin can't see it



WebSphere MQ Advanced Message Security

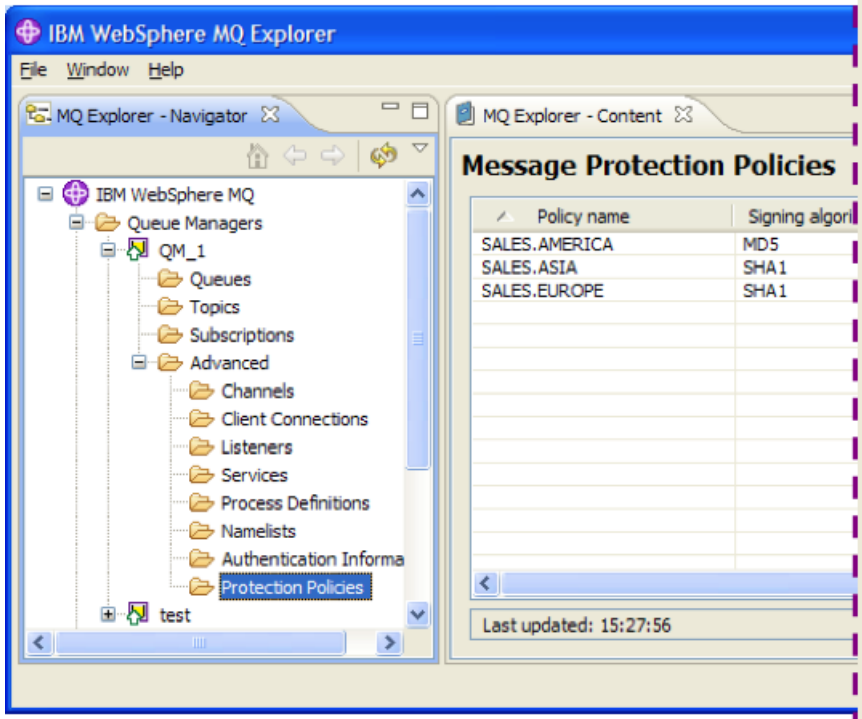
Technical Detail

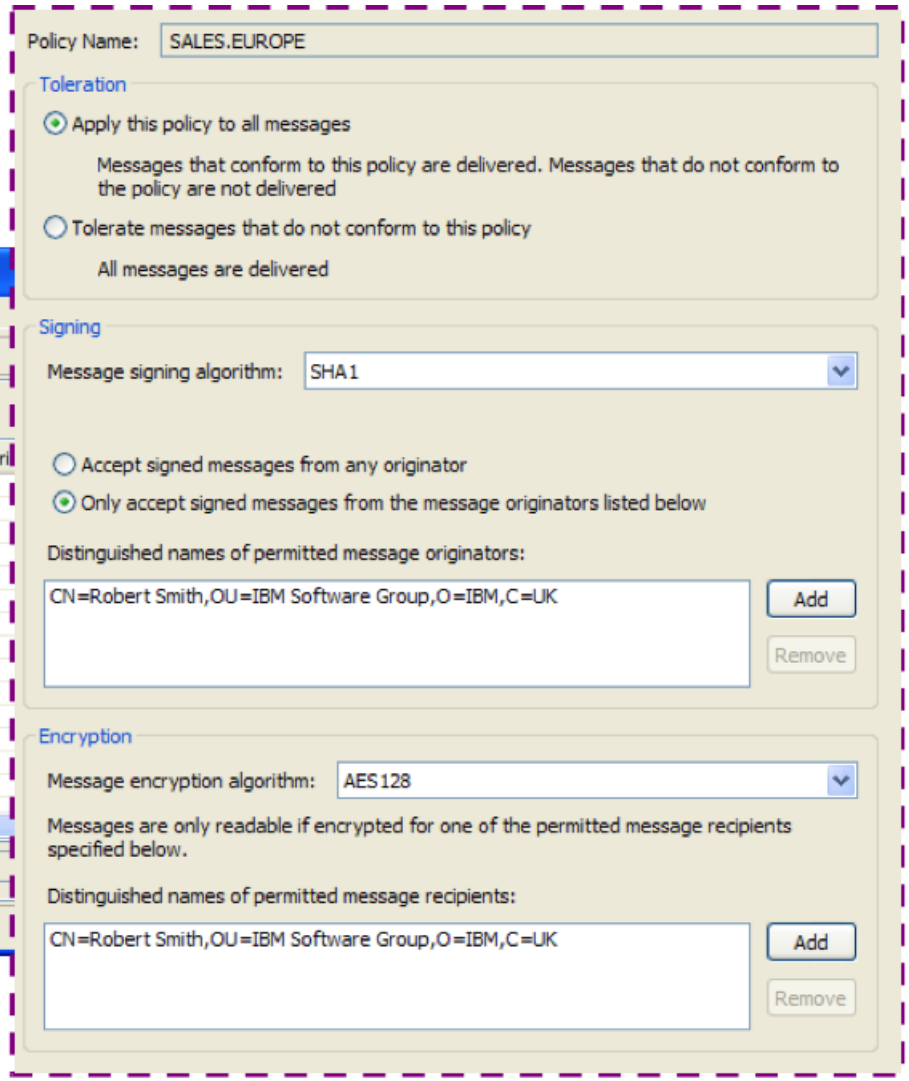
WebSphere MQ ESE Architecture vs. MQ AMS Architecture



Instantly familiar UI & command line: no new tooling to learn

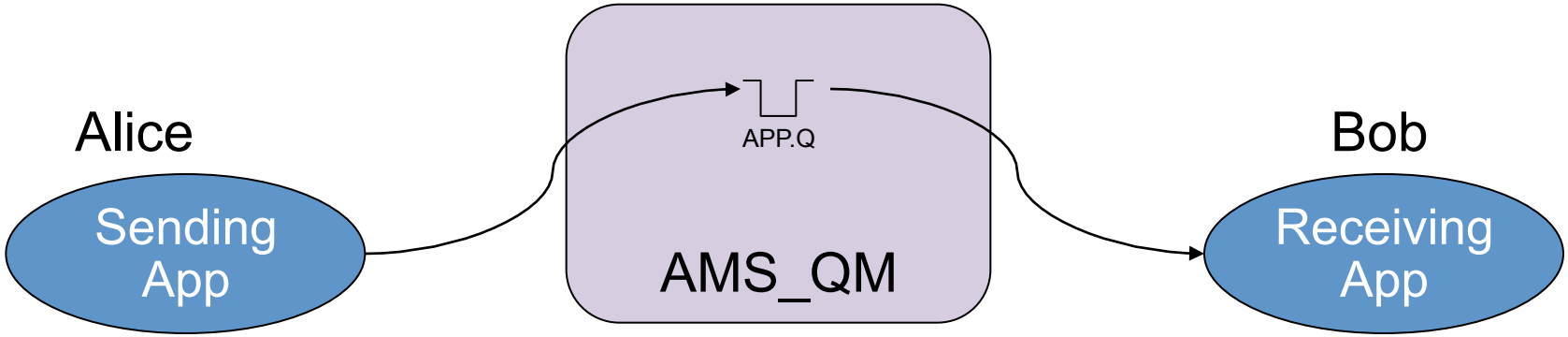
- Examine & manage security policies from the MQ Explorer
- Or from the command line





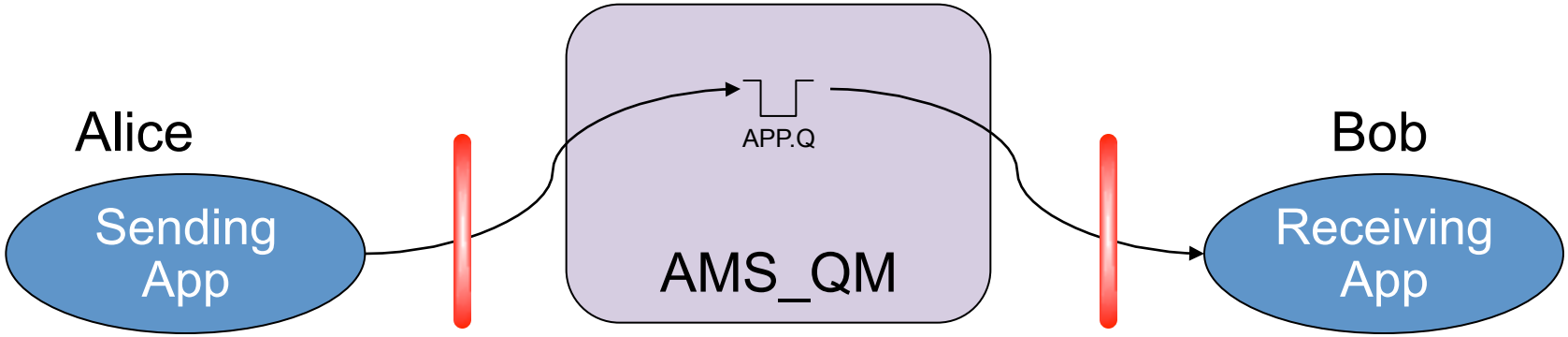
WebSphere MQ AMS Components and deployment example

1) Start with 2 Applications communicating over MQ



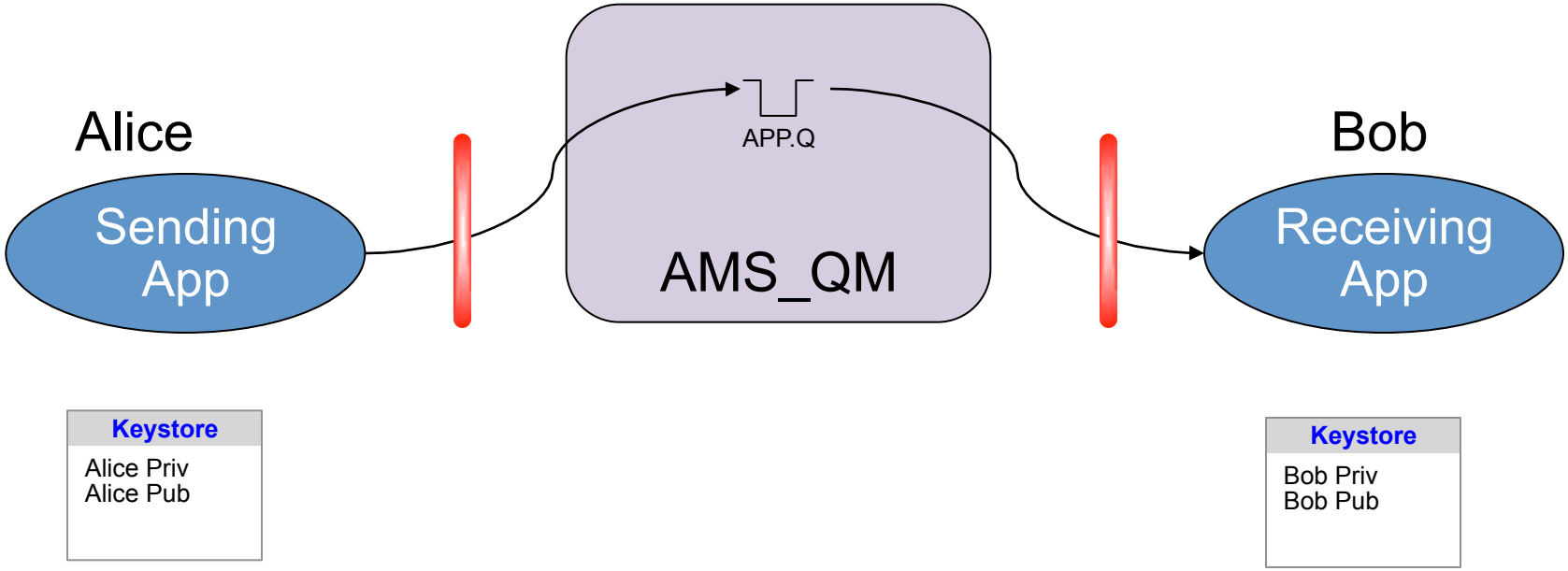
WebSphere MQ AMS Components and deployment example

1) Start with 2 Applications communicating over MQ
2) Install the MQ AMS Interceptor



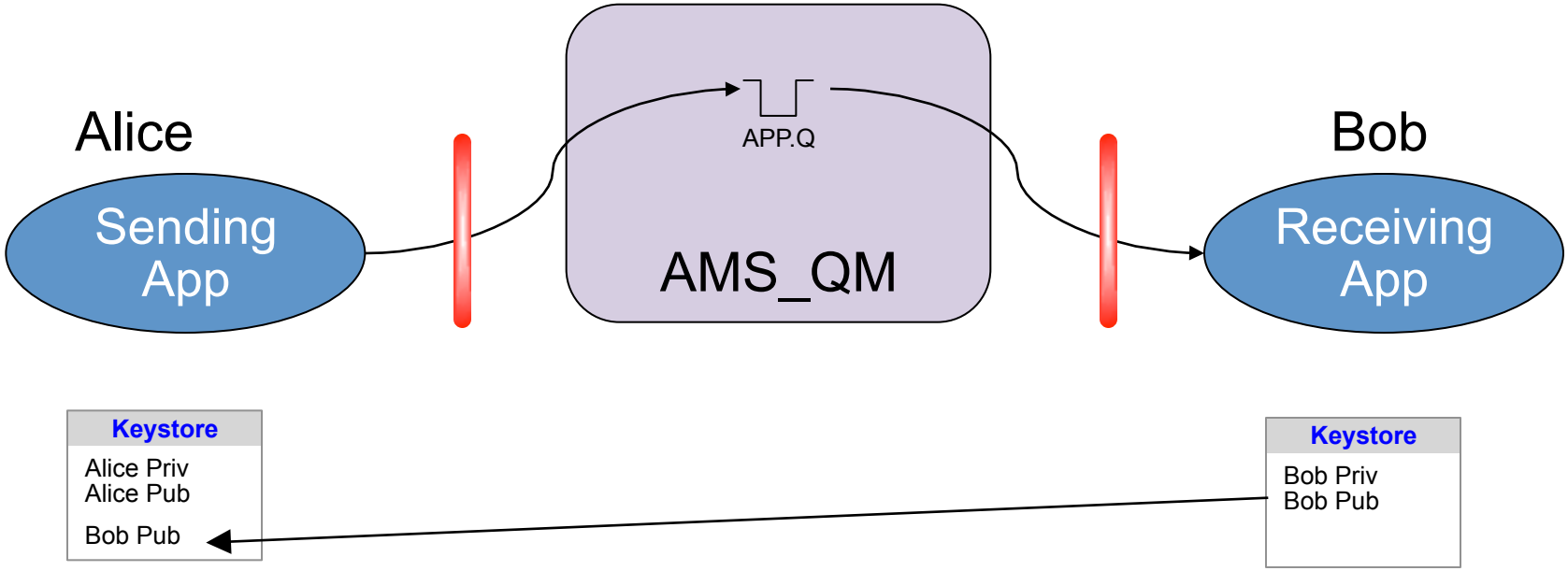
WebSphere MQ AMS Components and deployment example

1) Start with 2 Applications communicating over MQ
2) Install the MQ AMS Interceptor
3) Create public / private key pairs



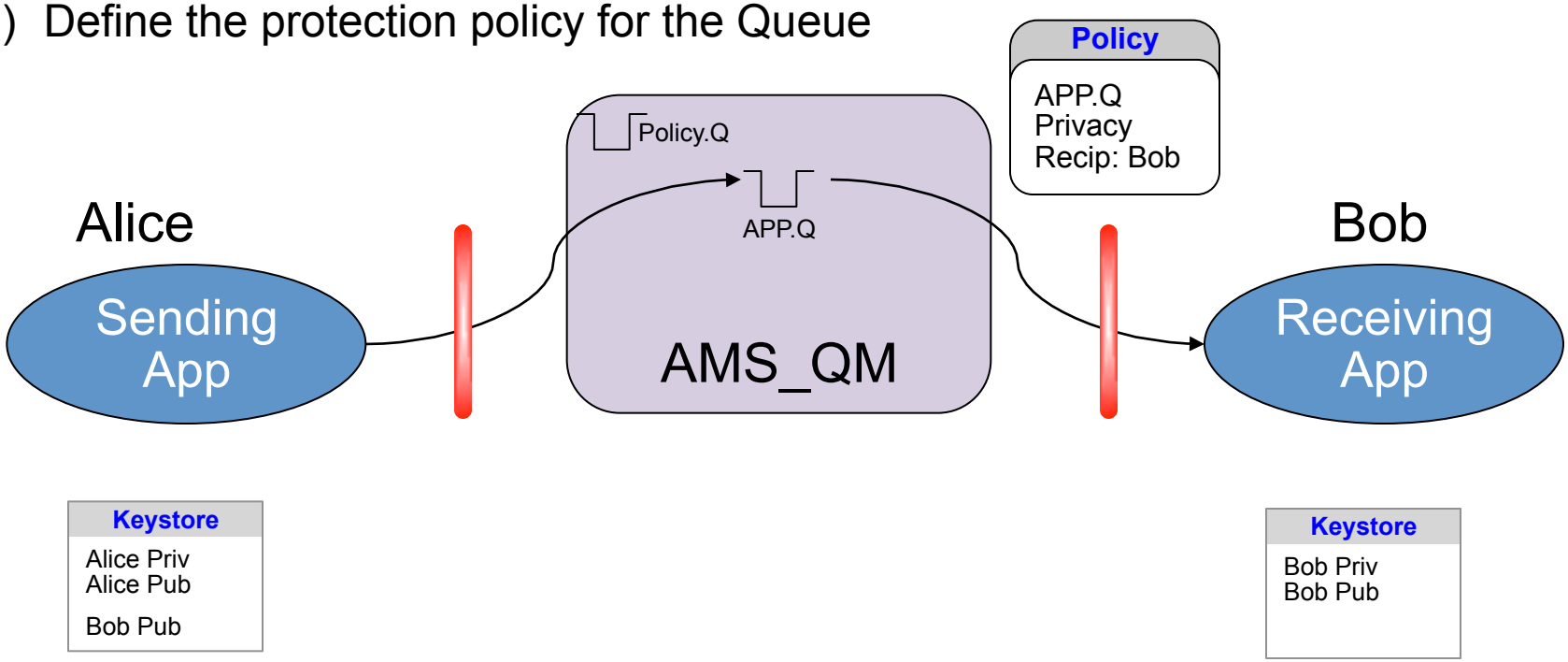
WebSphere MQ AMS Components and deployment example

1) Start with 2 Applications communicating over MQ
2) Install the MQ AMS Interceptor
3) Create public / private key pairs
4) Copy recipient's Public Key



WebSphere MQ AMS Components and deployment example

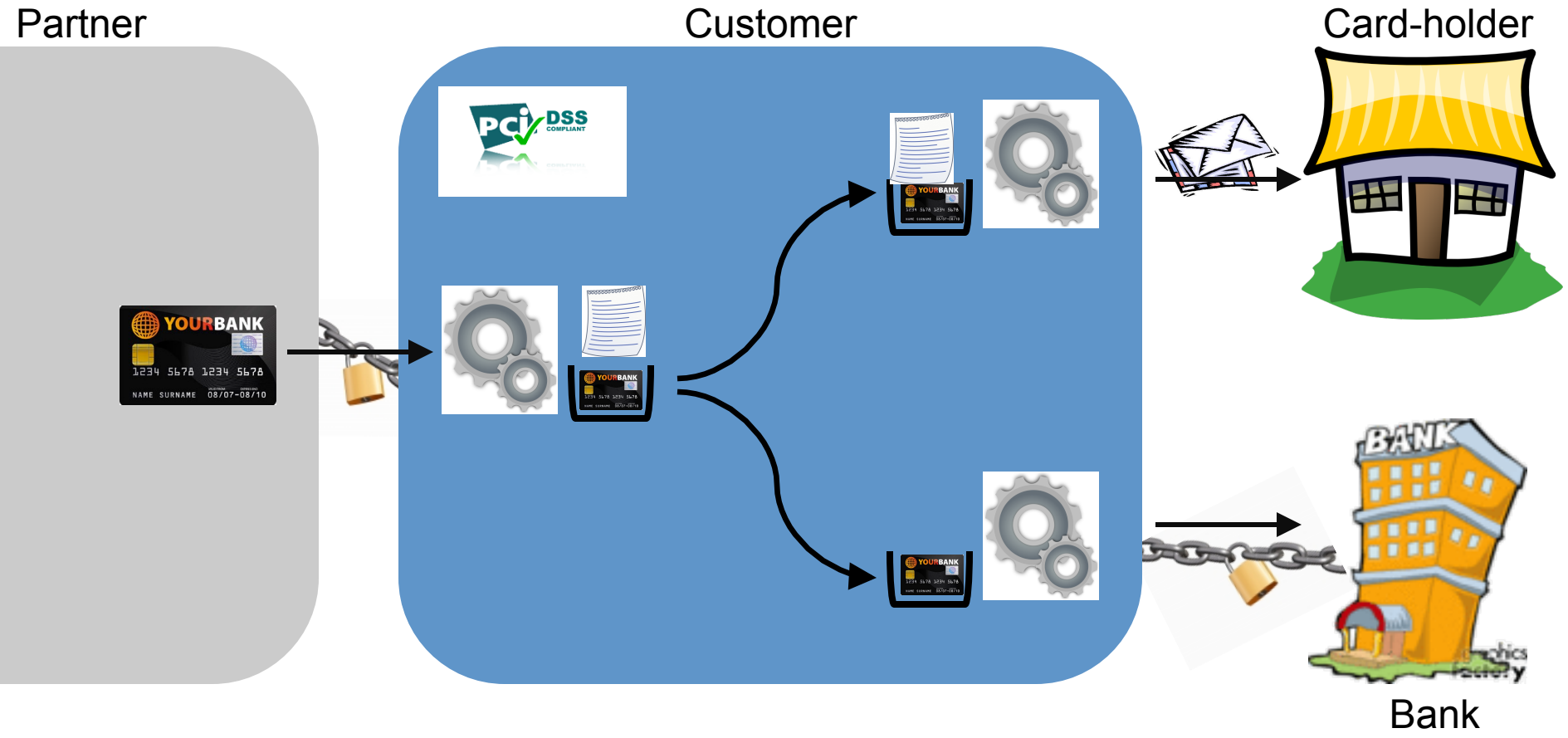
1) Start with 2 Applications communicating over MQ
2) Install the MQ AMS Interceptor
3) Create public / private key pairs
4) Copy recipient's Public Key
5) Define the protection policy for the Queue



Agenda for this PCI/ AMS Session

- Customer story (part 1): Requirements for PCI compliance
  - Reminder of Payment Card Industry Data Security Standard
  - Existing WMQ security
- WebSphere MQ Advanced Message Security
  - Why have it? …and what does it do?
  - How does it work?
- Customer story (part 2): '*this looks great – can we use it for our files?*'
  - The challenge: how to secure payment card info in file-base traffic
  - A quick overview of WebSphere MQ File Transfer Edition (WMQ FTE)
  - Integrating with WMQ AMS
- Summary & Questions

Customer story: requirements for PCI-DSS Compliance



WebSphere MQ File Transfer Edition: a quick overview

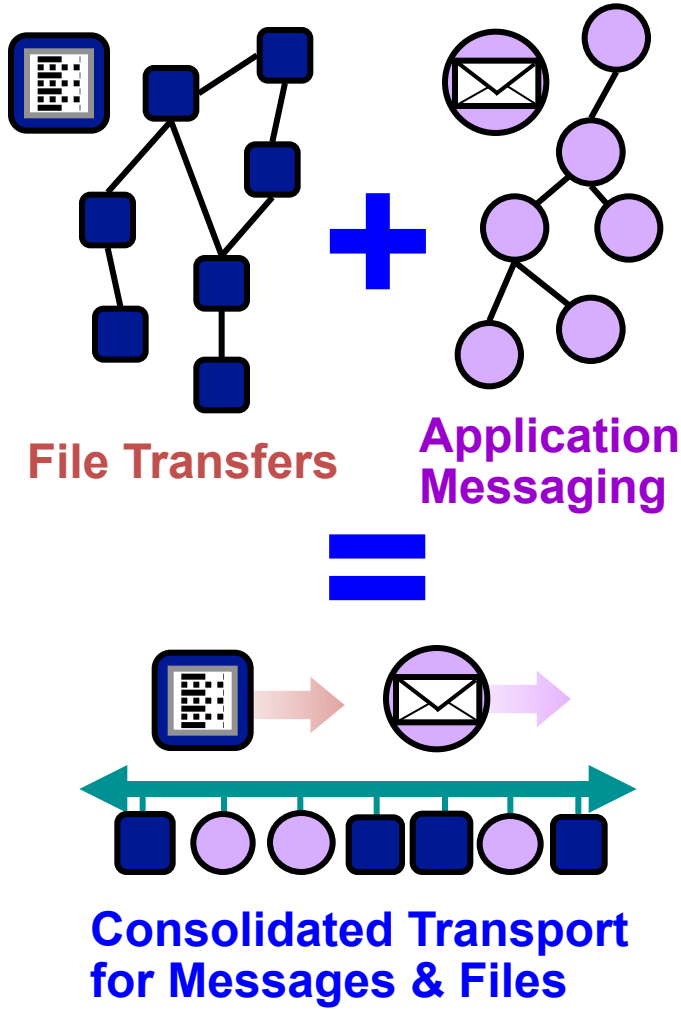
Traditional approaches to file transfer result in parallel infrastructures

- One for files – typically built on FTP
- One for application messaging – based on WebSphere MQ, or similar

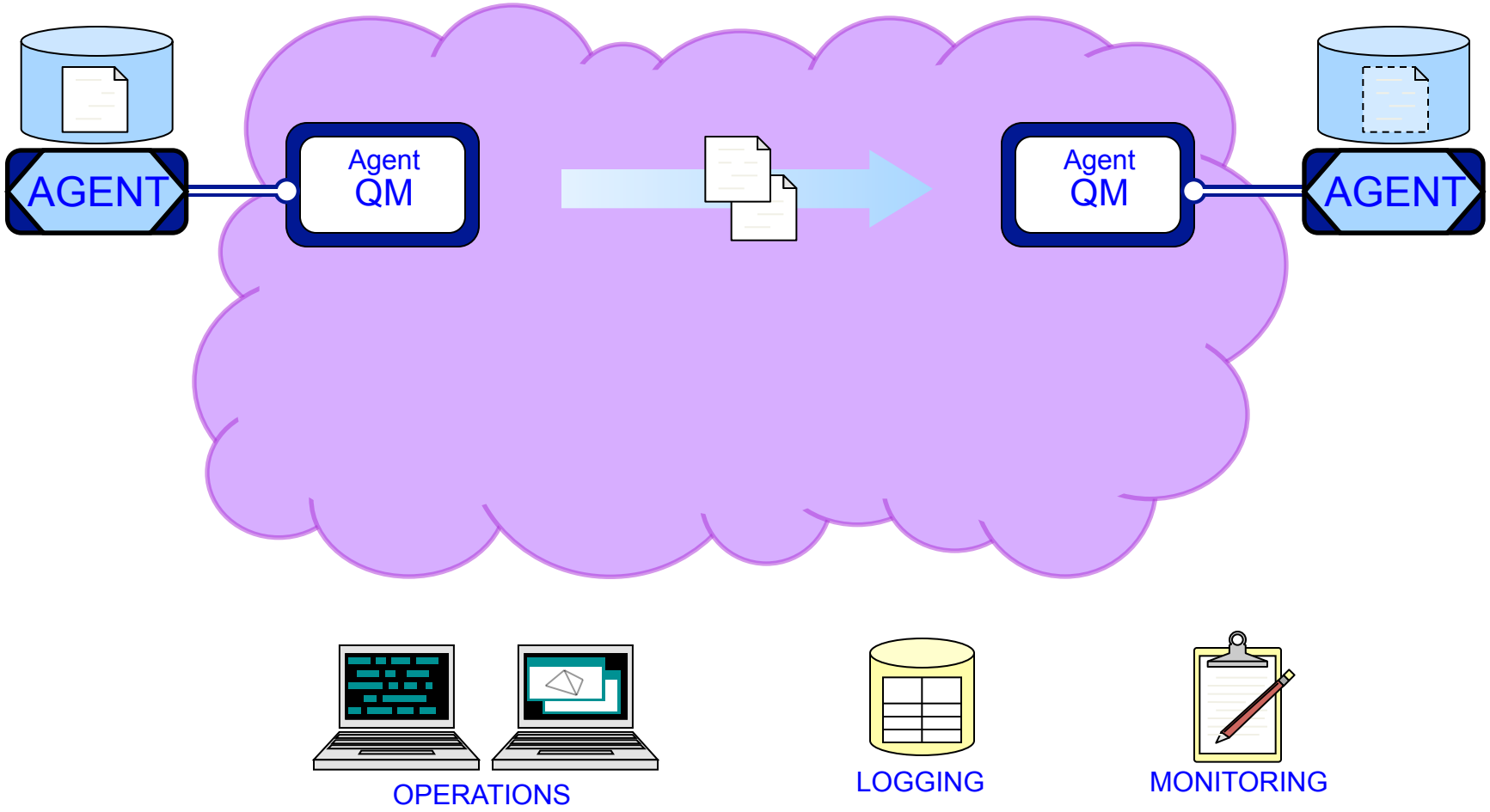
High degree of duplication in creating and maintaining the two infrastructures

Consolidating messaging and file transports yields:

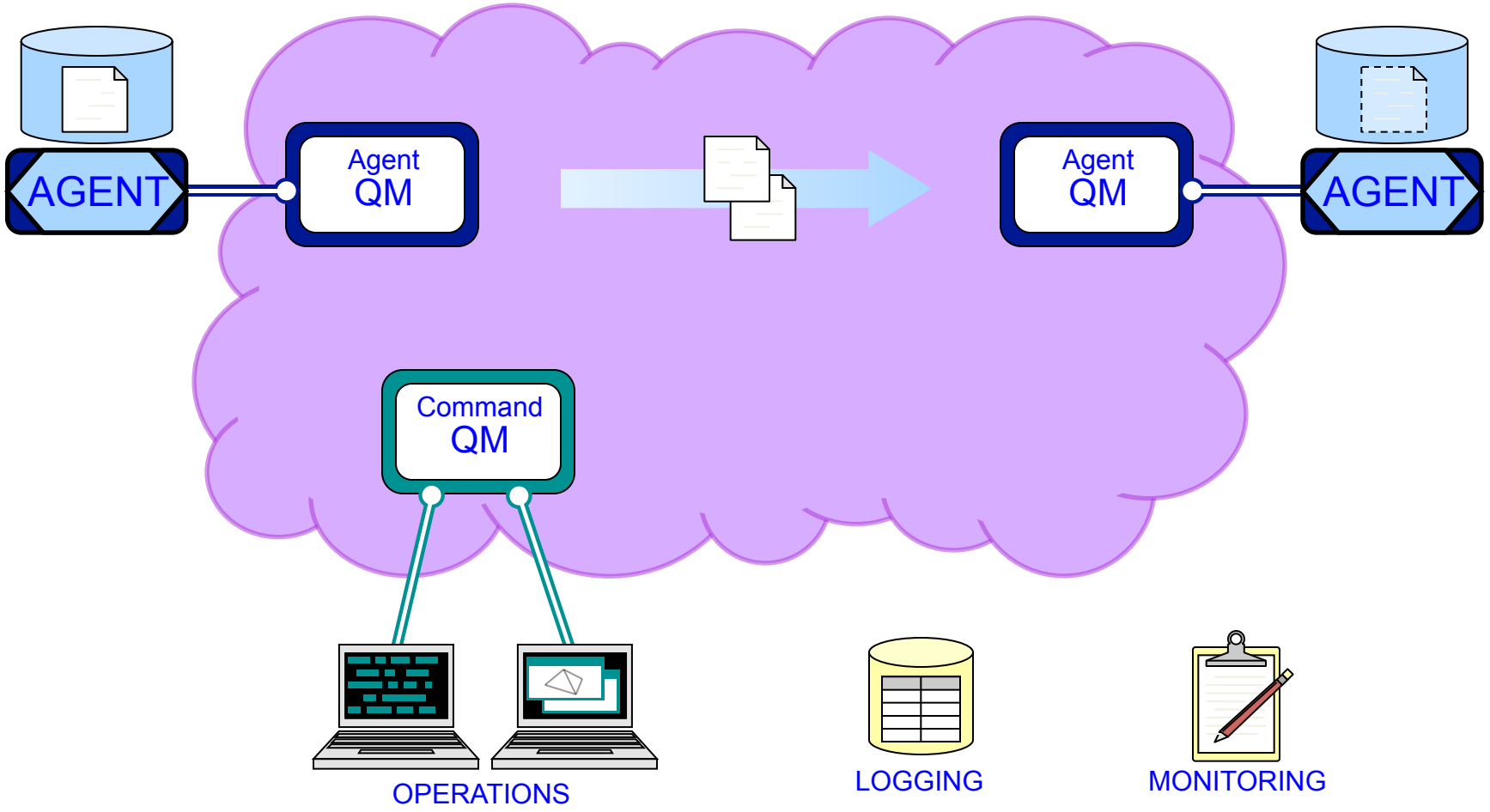
- Operational savings and simplification
- Reduced administration effort
- Reduced skills requirements and maintenance



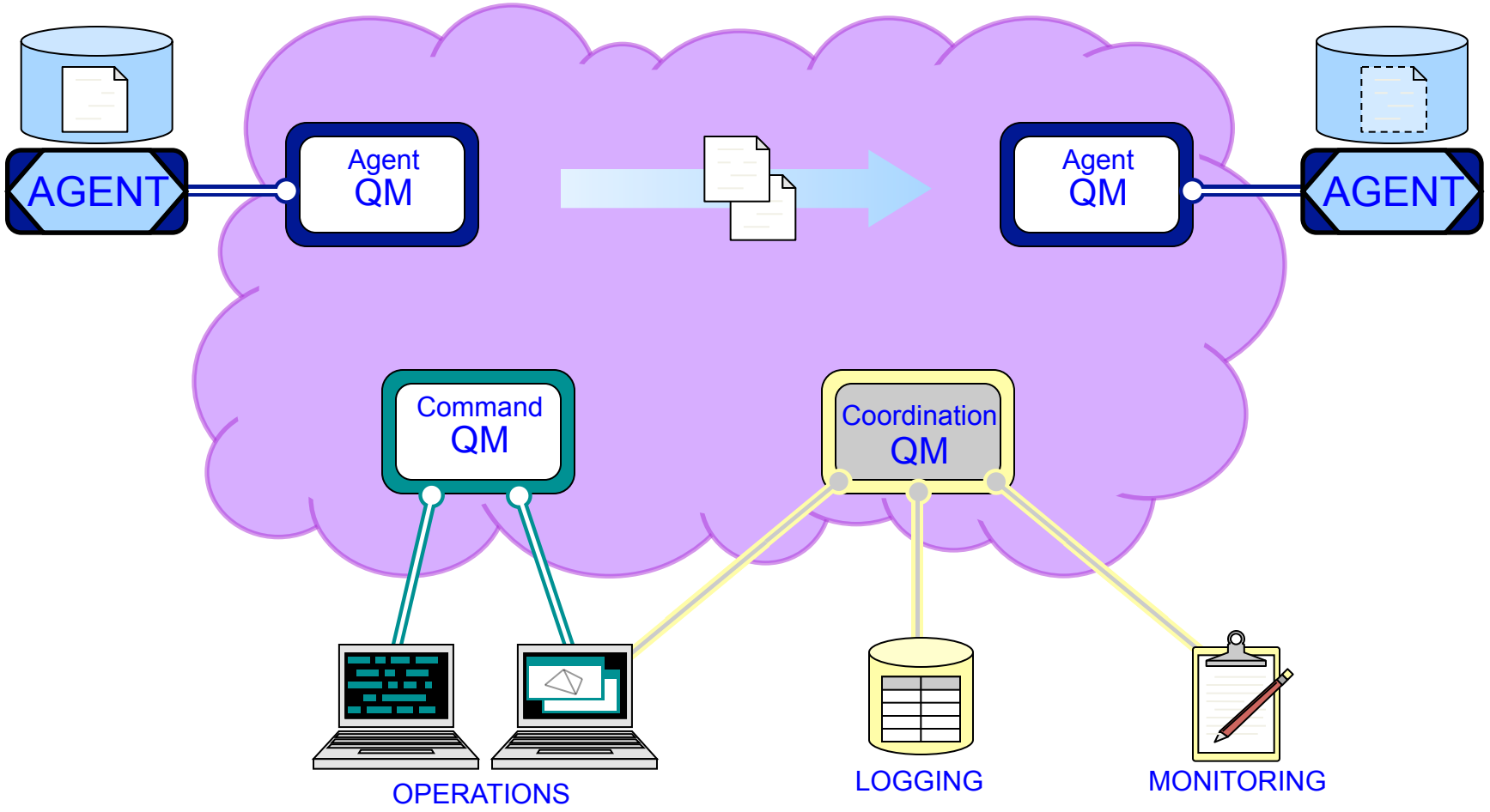
WebSphere MQ File Transfer Edition: Components (Agents)



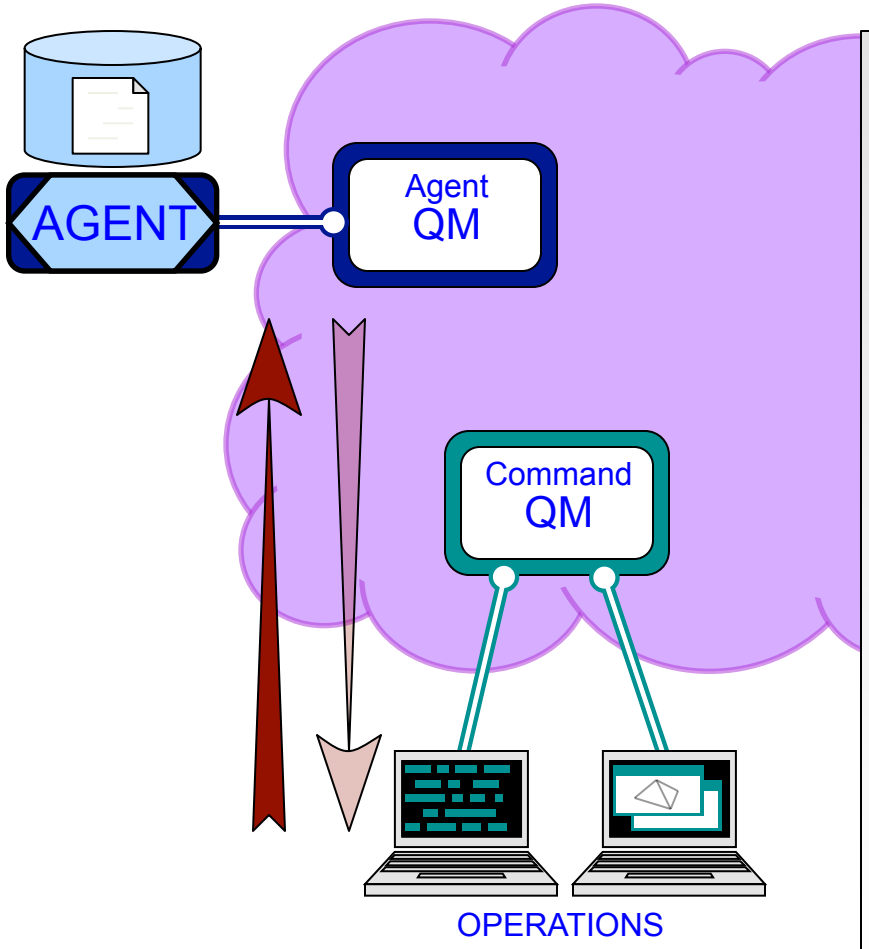
WebSphere MQ File Transfer Edition: Components (Commands)



WebSphere MQ File Transfer Edition: Components (Coordination)

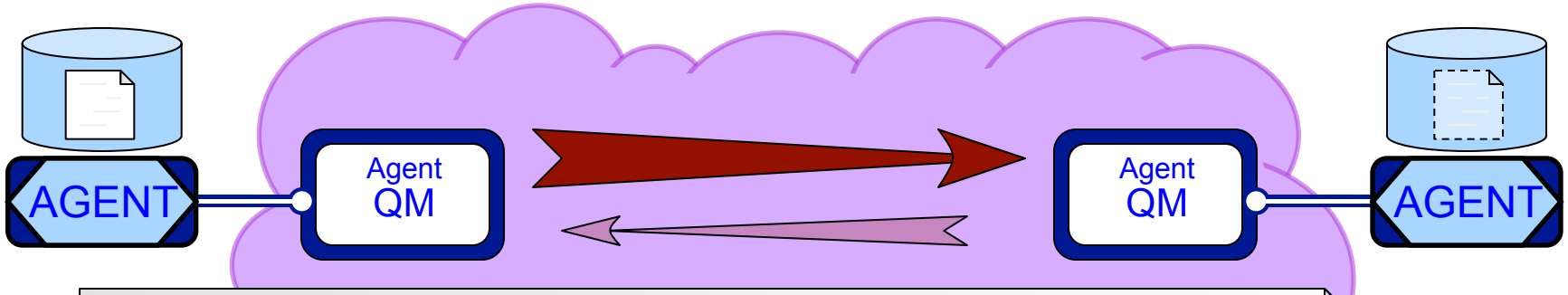


WebSphere MQ File Transfer Edition: Issuing commands



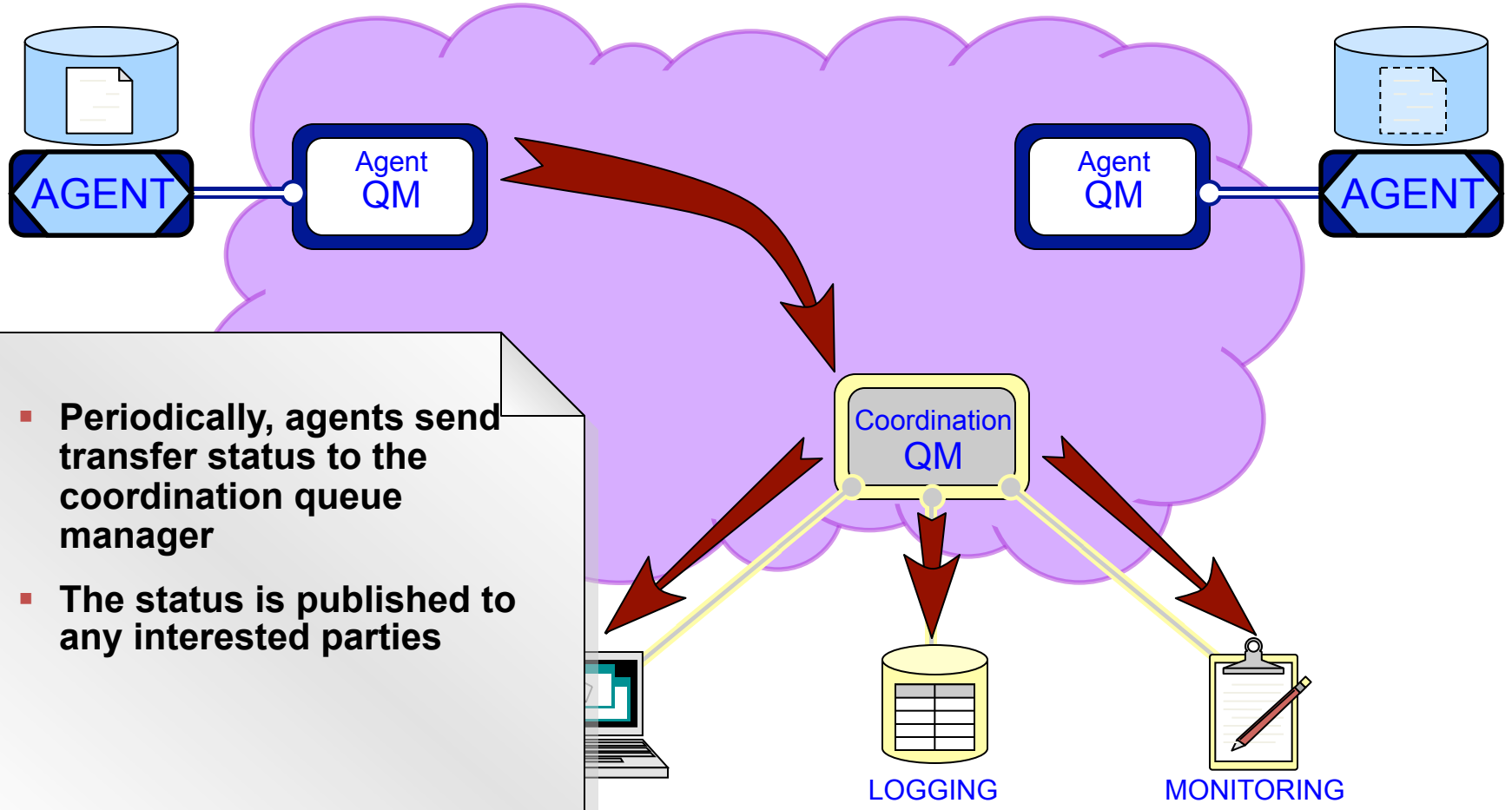
- **A new transfer is started by sending an MQ message to an agent**
  - The message may be routed via a *command queue manager*
- **The MQ message:**
  - Describes which files to transfer
  - Specifies the agent to which the files will be transferred
- **The agent responds by starting to transfer files, as instructed in the MQ message**
- **The agent can, optionally, reply**

WebSphere MQ File Transfer Edition: Transferring file data



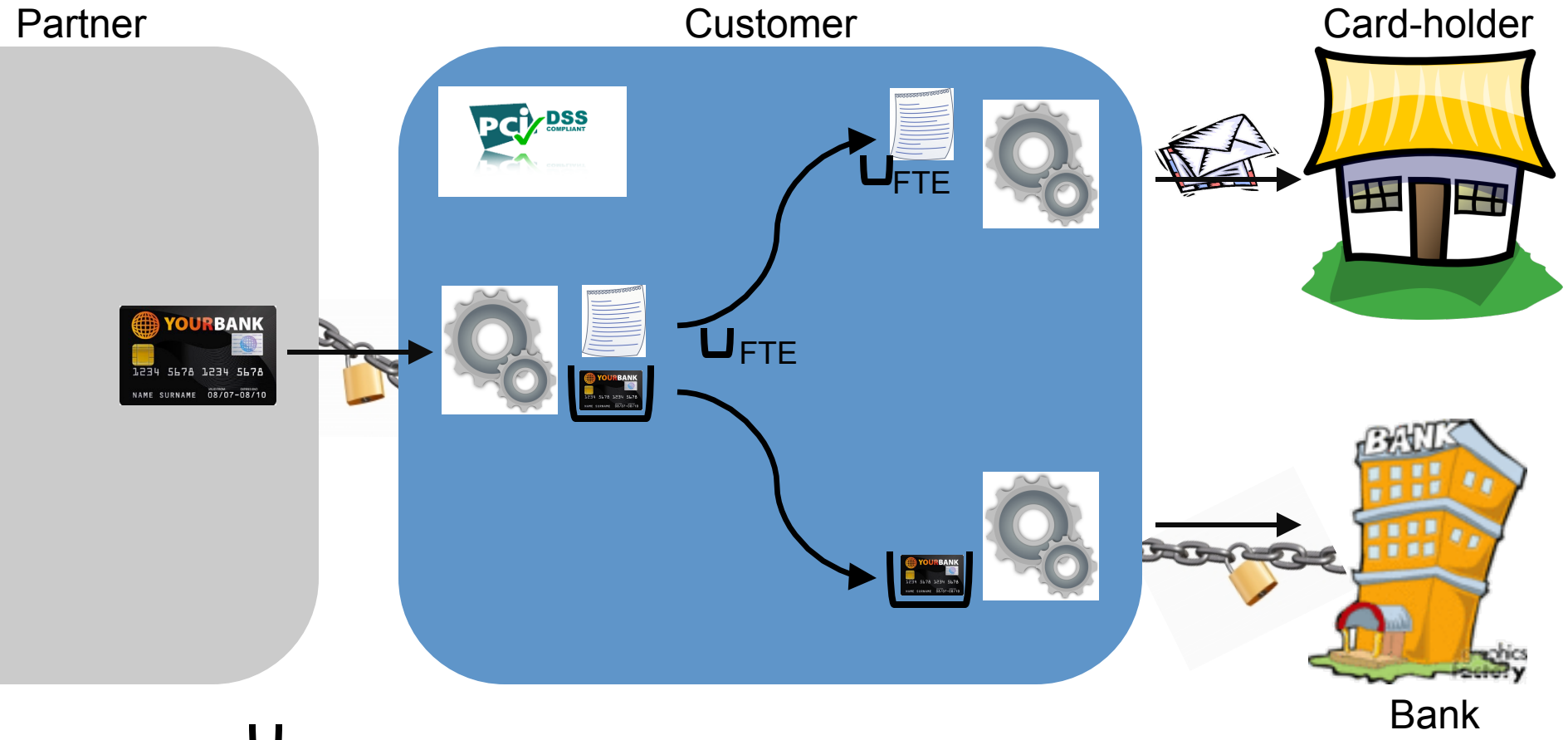
- **Agents transfer file data as MQ messages**
  - File data sent as MQ non-persistent messages
  - Allows prioritization with existing messaging workloads
  - Protocol used accounts for non-delivery and re-ordering
- **Transfers are paced**
  - This avoids a backlog of messages building up
- **Transfers automatically check-point:**
  - If any part of the infrastructure suffers an outage, transfers automatically re-start from the last check-point

WebSphere MQ File Transfer Edition: Tracking progress



- **Periodically, agents send transfer status to the coordination queue manager**
- **The status is published to any interested parties**

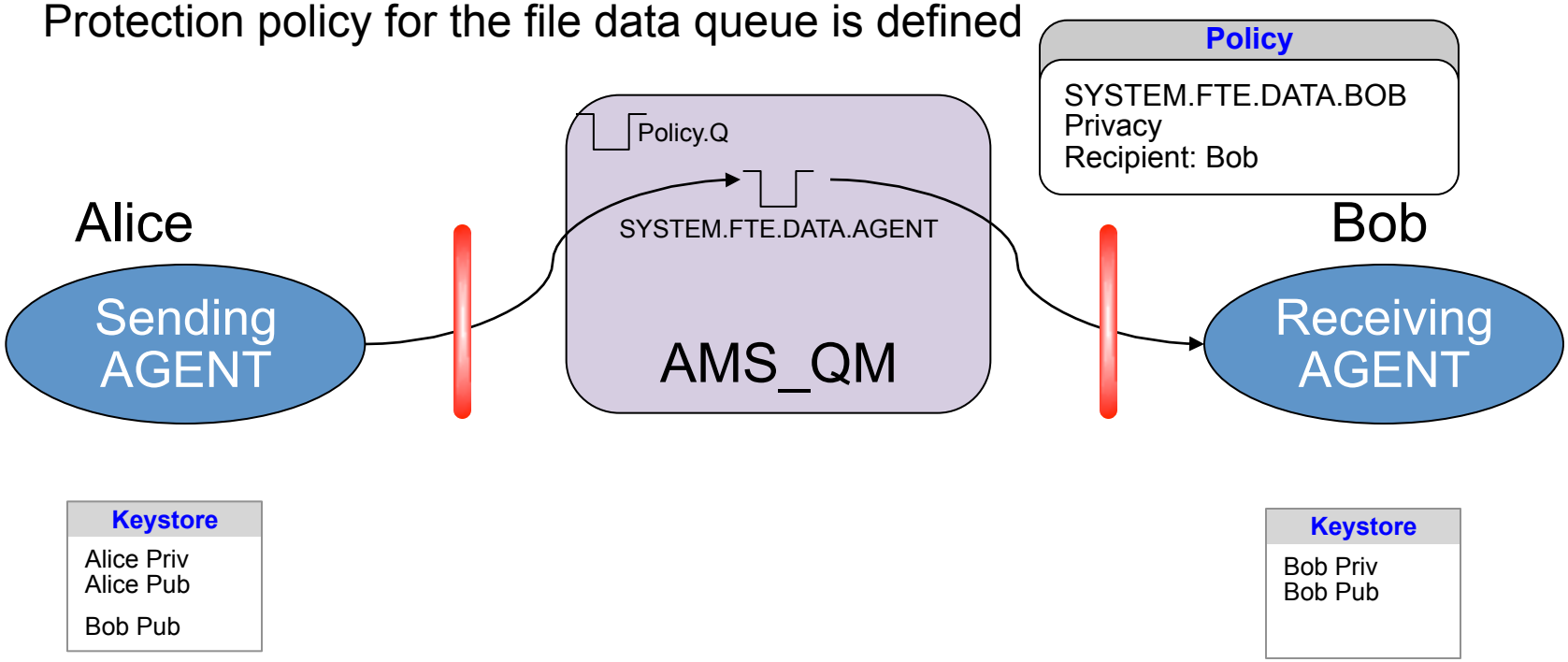
Customer story: integrating FTE with WMQ AMS



- Since FTE transfers the data over MQ, the FTE agents can be treated as the application interfacing with WMQ AMS

Example: WebSphere MQ AMS with WebSphere MQ FTE

- 2 MQ FTE agents transferring data
- MQ AMS Interceptor is in place
- The public / private key pairs are in place
- AGENT Bob's Public Key is available to AGENT Alice
- Protection policy for the file data queue is defined



WebSphere MQ AMS & PCI Summary

- PCI-DSS compliance is a key requirement for any organisation holding payment card information

- WMQ AMS extends core WMQ Security
  - Provides end-to-end integrity of MQ messages (digital signing)
  - Provides end-to-end privacy of MQ messages (encryption)
  - Supports PCI requirement for encryption during data-at-rest in MQ queues

- No alterations needed to support existing applications
  - Supporting existing and new workloads, such as WMQ FTE

Useful references

- WebSphere MQ Advanced Message Security website

http://www-01.ibm.com/software/integration/wmq/advanced-message-security/

- WebSphere MQ Advanced Message Security InfoCenter

http://publib.boulder.ibm.com/infocenter/mqams/v7r0m1/index.jsp

- developerWorks: End-to-end encryption with WMQ Advanced Message Security

http://www.ibm.com/developerworks/websphere/techjournal/1011_mismes/1011_mismes.html

- developerWorks: WMQ, PCI DSS and security standards

http://www.ibm.com/developerworks/websphere/techjournal/0806_mismes/0806_mismes.html

- WMQ AMS with WMQ File Transfer Edition

http://publib.boulder.ibm.com/infocenter/mqams/v7r0m1/topic/com.ibm.mqese.doc/overview/overview_AMS_FTE.htm

WebSphere MQ Advanced Message Security

Additional Material

Key stores & 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.

Signature Algorithm

- MD5
- SHA1

Encryption Algorithm

- RC2
- DES
- 3DES
- AES128
- AES256