Securing IBM MQ for GDPR and Regulatory Compliance

Gwydion Tudur (gtudur1@uk.ibm.com)
IBM MQ

November 2018
Session JM




Notices and disclaimers

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM’s products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.** The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

Notices and disclaimers continued

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation.

Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations.

The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about IBM's own GDPR readiness journey and our GDPR capabilities and offerings here: https://ibm.com/gdpr

Introduction

- In May 2016, the European Parliament published the General Data Protection Regulation, which is compulsory in each member state starting 25 May 2018.
- The intention is a stronger data protection for individuals within the EU, and a unified regulation of the export of personal data outside the EU.
- In this session we discuss considerations for configuring MQ to help with GDPR readiness.

Why is GDPR important?

Applies to any organization anywhere in the world that handles personal data of EU data subjects

Widened definition of personal data, with new and enhanced rights for individuals

New obligations for processors, including compulsory data breach notification

Potential for significant financial penalties for non-compliance

Personal data

Individual rights:

- ✓ Right to be informed about collection and use
- ✓ Right to access their personal data
- ✓ Right to have inaccurate data corrected
- ✓ Right to have personal data erased
- ✓ Right to restrict use of personal data
- ✓ Right to move, copy or transfer personal data
- ✓ Right to object
- ✓ Rights related to automated decision making and profiling

Personal data shall be:

- ✓ Processed lawfully, fairly and transparently
- ✓ Collected for specified, explicit and legitimate purposes
- ✓ Adequate, relevant and limited to what is necessary
- ✓ Accurate, and where necessary, kept up to date
- ✓ Kept for no longer than necessary
- ✓ Processed securely, including protection against unauthorized or unlawful access, accidental loss, destruction or damage

How does GDPR relate to messaging and IBM MQ?

Personal data must be securely processed throughout its lifecycle

→ Both at rest and in-flight

IBM MQ enables applications to asynchronously exchange application data using a range of APIs, protocols and bridges

→ This data might be subject to GDPR

→ Message data might be persisted in queue files (page sets, SMDS or Coupling Facility on z/OS), logs and archives

IBM MQ processes…

Authentication credentials

Technically identifiable personal information (when linked to an individual) – e.g. IP address

Application provided data might also be captured in files collected for problem determination.

Error logs, trace files, FFSTs

Address space and CF dumps on z/OS

Examples of personal data that might be exchanged using MQ

- Employees of the customer (payroll, HR)
- Customer's clients (sales leads, CRM)
- Sensitive personal data (HL7 health data)

Data collection

Consider the types of personal data, which in your circumstances, are passing through IBM MQ.

How does data arrive in to your queue managers?

Is the data signed and/or encrypted?

From where/whom is the data sent?

How is data sent out from your queue managers?

Is the data signed and/or encrypted?

Is the data leaving your organization?

How is data stored as it passes through the queue manager?

Any message can be written to stateful media, even if it is non-persistent

How might the data be exposed in MQ?

How are credentials collected and stored, where needed by MQ to access third-party applications?

Where possible, avoid using personal credentials for IBM MQ authentication

Data storage

IBM MQ might persist message data to stateful media, perhaps multiple times, for example:

- Queues
- Recovery logs

Consider how messages flow between queues and queue managers in your messaging infrastructure

- Message data might be persisted at each stage of the message flow

Consider the following types of queues:

- ✓ Application queues
  Store application message data
- ✓ File transfer agent queues
  Store file data while in transit, and a record of those transfers
- ✓ Transmission queues
  Temporarily store messages in transit
- ✓ Dead-letter queues and the AMS error queue
  Store messages that cannot be delivered to their destination, or AMS deems non-compliant
- ✓ Backout queues
  Store messages repeatedly backed out to allow other messages to be processed (e.g. JMS/XMS poison message)
- ✓ Retained publications
  Allow subscribing applications to recall the message data for a previous publication

Data storage

IBM MQ might indirectly persist application message data when some product capabilities are used.

Users might wish to consider these use cases when ensuring compliance with GDPR.

Trace route messaging

Records the route a message takes between applications

Event messages might include technically identifiable personal information, such as IP addresses

Application activity trace

Records messaging API activities of applications and channels

Can include application provided message data

Service trace

Records internal code paths through which message data flows

Can record message data in trace records on disk or in dumps

Queue manager events

Might include personal data, such as in authority, command and configuration events

Protecting data storage

Consider the following actions to protect copies of application message data in IBM MQ.

- ✓ Restrict operating system access to MQ data
  Restrict membership of the mqm group on distributed
  Restrict access to queue manager datasets, the CF and dumps on z/OS (plus DB2 if used to offload messages)
- ✓ Restrict application access to MQ data
  Avoid unnecessary sharing of queues and topics
  Restrict access to queues and topics
- ✓ Use IBM MQ Advanced Message Security
  Provides end-to-end signing and/or encryption of message data
- ✓ Protect trace and FFST data
  Use disk/volume encryption to protect the content of the directory used to store trace logs
  Consider deleting trace data once uploaded to IBM
- ✓ Protect backups
  Encrypt and restrict access to queue manager backups

Data access

IBM MQ can be accessed through local and remote product interfaces, including:

- IBM MQ Console
- IBM MQ REST API
- MQI, JMS, XMS
- MQSC, PCF
- IBM MQ Explorer
- IBM MQ Telemetry (MQTT)
- IBM MQ Light (AMQP)
- IBM i and ISPF panels
- plus various bridges to other products, including CICS, IMS, Salesforce & Blockchain

Administration and messaging operations secured using authentication, role mapping and authorization

Authentication can use:

- Asserted username
- Username and password (OS, LDAP, etc.)
- Source network/IP address
- X.509 digital certificate
- Security tokens
- Custom security using exits

Users can be granted different authorities to messaging resources

Logging activity

IBM MQ includes features to create an audit record of access, which might be required for regulatory compliance

However, note:

- Queue manager event messages are non-persistent by default
- Privileged administrators might be able to disable events, clear logs, or delete queue managers

Sources for auditing in IBM MQ:

- ✓ Command events
  Produced when an administrative command has been executed successfully
- ✓ Configuration events
  Produced when a queue manager resource is created, deleted or modified
- ✓ Authority events
  Produced when an authorization check fails
- ✓ Queue manager error logs (system log on z/OS)
  Record failed authorization checks
- ✓ IBM MQ Console and REST API
  Writes audit messages to its log when authentication/authorization checks fail, or when queue managers are created, started, stopped or deleted

Personal data deletion

IBM MQ provides facilities to delete data that relates to an individual, should this be required.

However, IBM MQ is not a database so it might be difficult to find personal data in messages unless you know the queue, message and correlation identifiers of a message.

Deleting queue manager resources

- ✓ Delete data stored on a queue manager by deleting the queue manager
- ✓ Delete trace files, FFSTs and dumps
- ✓ Delete archive, backup or other copies of queue manager data

Deleting personal data in messages on a queue

- ✓ Remove applicable messages using a messaging API, tooling or message expiry
- ✓ Specify messages are non-persistent and restart the queue manager
  Provided they are held on a queue where the non-persistent message class is normal
- ✓ Administratively clear the queue
- ✓ Delete the queue
- × Data might remain in logs, and on disk until overwritten

Deleting retained publication data for a topic

- ✓ Specify messages are non-persistent and restart the queue manager
- ✓ Replace retained data with new data, or use message expiry
- ✓ Administratively clear the topic string
- × Data might remain in logs, and on disk until overwritten

Account data deletion

Delete the following resources that define account data and preferences stored by IBM MQ.

See Knowledge Center for a complete list.

- ✓ Queue manager authentication information objects that store credentials
- ✓ Queue manager authority records that reference user identifiers
- ✓ Queue manager channel authentication records that map or block specific IP addresses, certificate DNs or user identifiers
- ✓ X.509 digital certificates for an individual from keystores used by SSL/TLS or AMS
- ✓ Credential files used by Managed File Transfer
- ✓ MQ Explorer workspace meta data, Eclipse settings and stored passwords
- ✓ MQ Console and mqweb configuration files
- ✓ User accounts on the MQ Appliance

Deployment

IBM MQ is often used to:

- Connect systems that are geographically dispersed
- Connect to business partners and other third-parties
- Build a highly available enterprise solution that spans physical sites and regions

IBM MQ is also increasingly deployed in cloud environments

Consider how your IBM MQ deployments are affected.

Do you have appropriate safeguards for the data transferred using IBM MQ?

GDPR restricts the transfer of personal data outside the European Union.

Ensures the same level of protection is present for EU citizens when their data is processed outside the EU.

Advanced Message Security (AMS)

Provides message-level security for valuable/sensitive messages

- In flight on the network
- At rest, on disk

Without AMS it might be difficult to prove security of messages in large networks

- Injection
- Modification
- Unauthorized viewing

Data subject to standards compliance e.g. PCI, HIPAA, GDPR

- Credit card data
- Government data
- Personal information

Available with:

- IBM MQ Advanced
- IBM MQ Advanced VUE for z/OS

Benefits of AMS

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

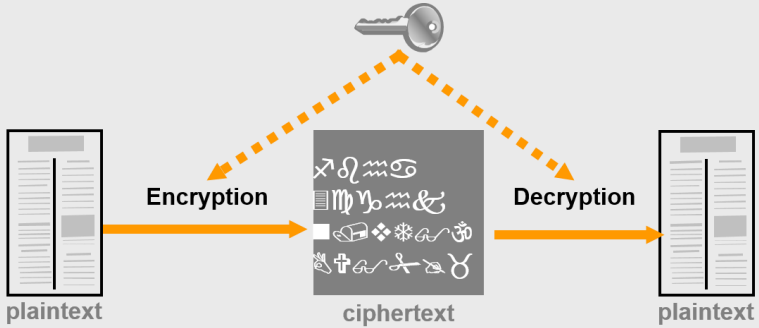
Assurance that messages can only be viewed by intended recipient(s)

- When sending confidential information

Important: Does not replace the need for standard MQ resource security

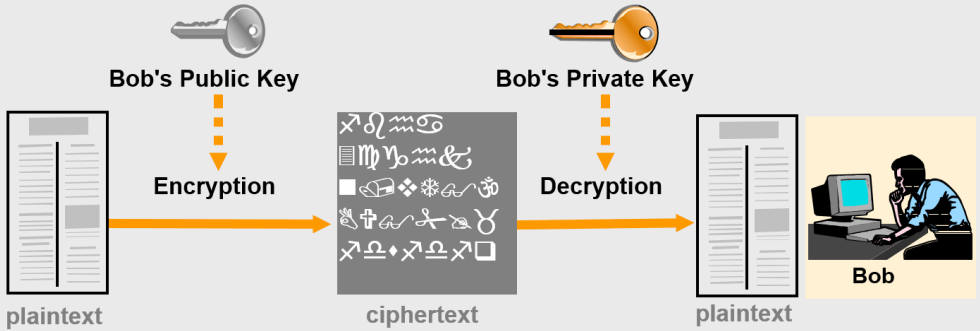
Cryptography choices

Symmetric Key



- Single secret key
- Relatively fast
- Poses key distribution challenges when large numbers of senders/receivers
- The key has to be known by the sender and receiver

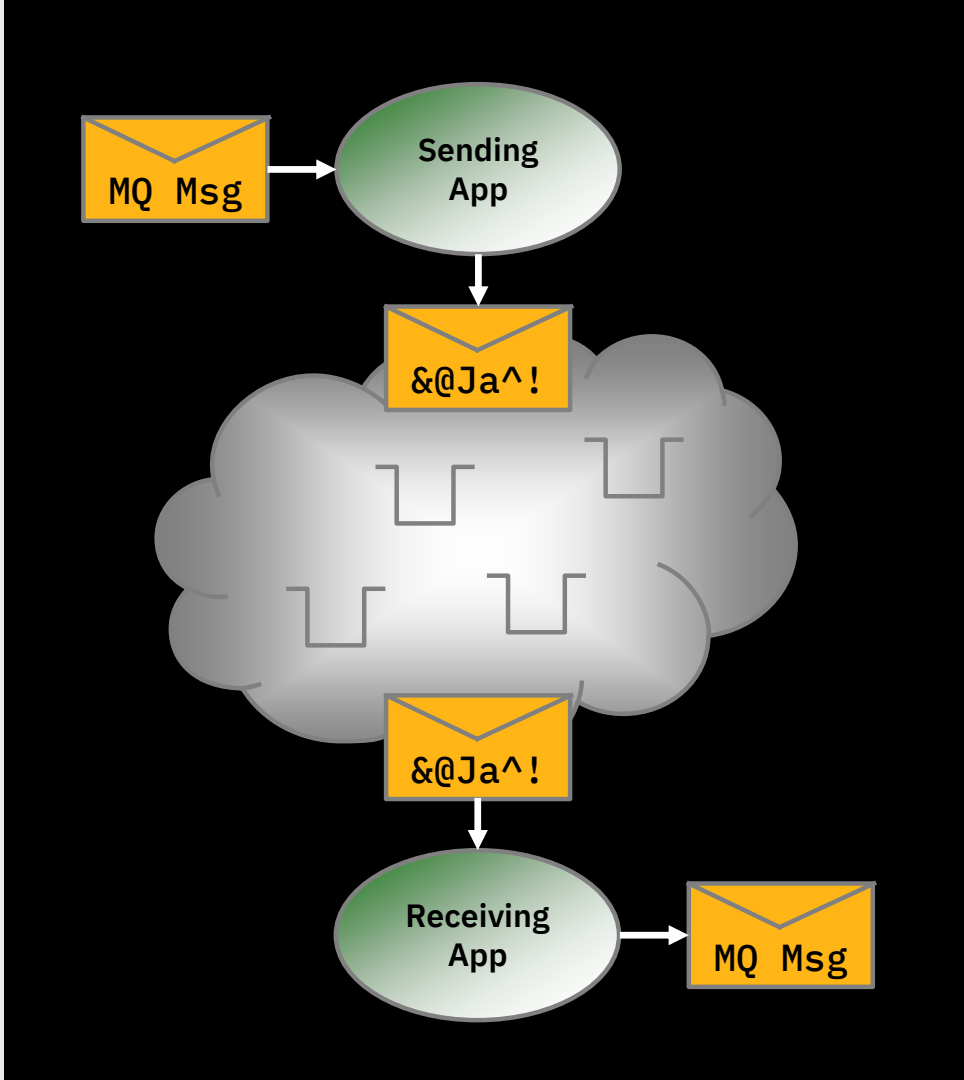
Asymmetric Keys



- Private & Public key pairing
- 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

IBM MQ Advanced Message Security

- Provides additional security to that provided by base MQ
- End-to-end security, message level protection
  - A security policy defines what protection should be applied to messages
  - AMS intercepts messages at “endpoints” and applies the policy
- Each message protected using a symmetric key, which is protected using asymmetric cryptography
- No code changes or re-linking of applications



IBM MQ Advanced Message Security – Security Features

IBM MQ Base

- Authentication (CONNAUTH and mutual TLS)
- Authorization (OAM on distributed, RACF on z/OS and CHLAUTH for channels)
- Integrity (SSL/TLS for channels)
- Privacy (SSL/TLS for channels)

IBM MQ Advanced Message Security

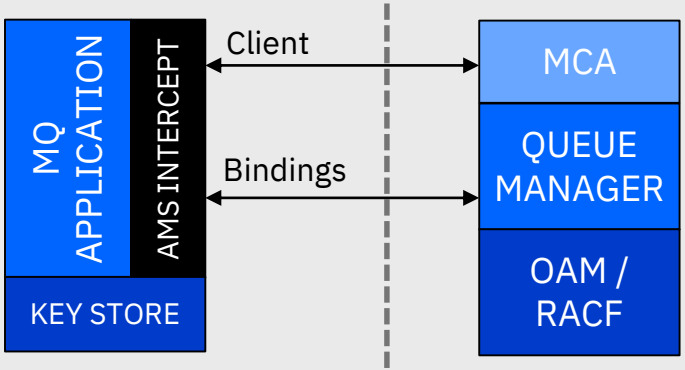
- Integrity (digital signing of messages)
- Confidentiality (encryption of messages)
- Privacy (digital signing and encryption of messages)

Policies

- Define policies for individual queues
- Administer policies using administrative commands or MQ Explorer
- Define matching policy at application end-points – not needed for intermediate queues
- Policy attributes (as applicable)
  - Signing algorithm – SHA256, SHA512, …
  - Authorized signers – DN list
  - Encryption algorithm – AES128, AES256, …
  - Message recipients – DN list
  - Key reuse count – reduce asymmetric key operations

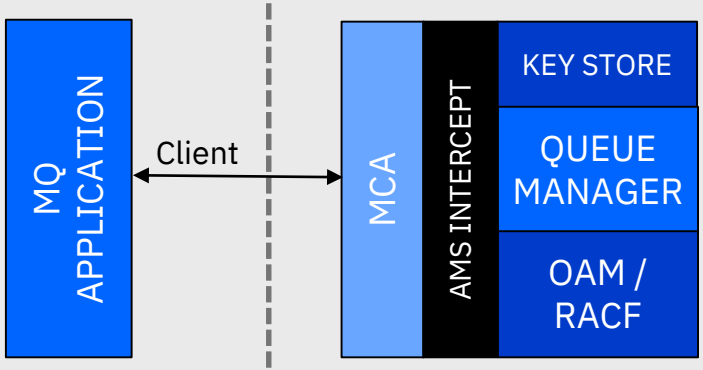
AMS Architecture

Application Interception



- AMS intercepts PUT / GET at client
- Key store on client system contains the necessary signing/encryption certificates
- Message signed/encrypted before sent over the network
- Message verified/decrypted after received over the network

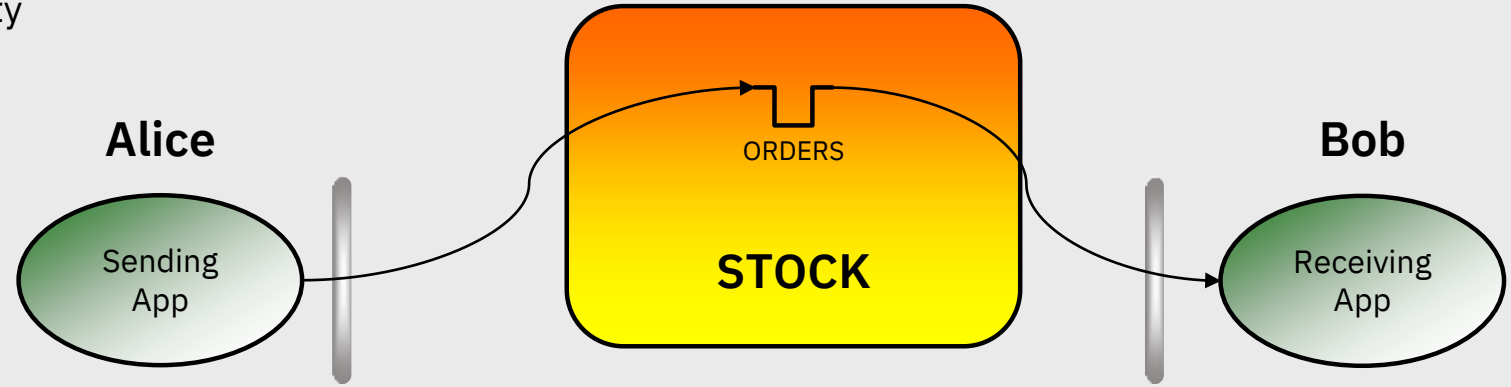
MCA Interception



- AMS intercepts PUT / GET at MCA (queue manager)
- Queue manager key store contains the necessary signing/encryption certificates
- Message signed/encrypted after received over the network
- Message verified/decrypted before sent over the network
- Supported for non-AMS capable clients, or where certificate distribution is not practical

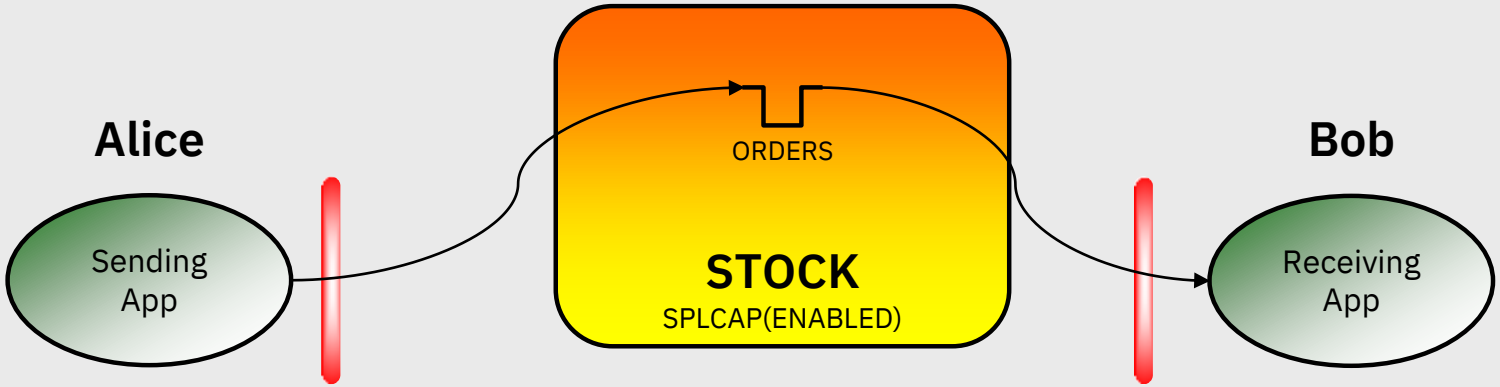
Securing an existing MQ application

Initially no protection other than base MQ security



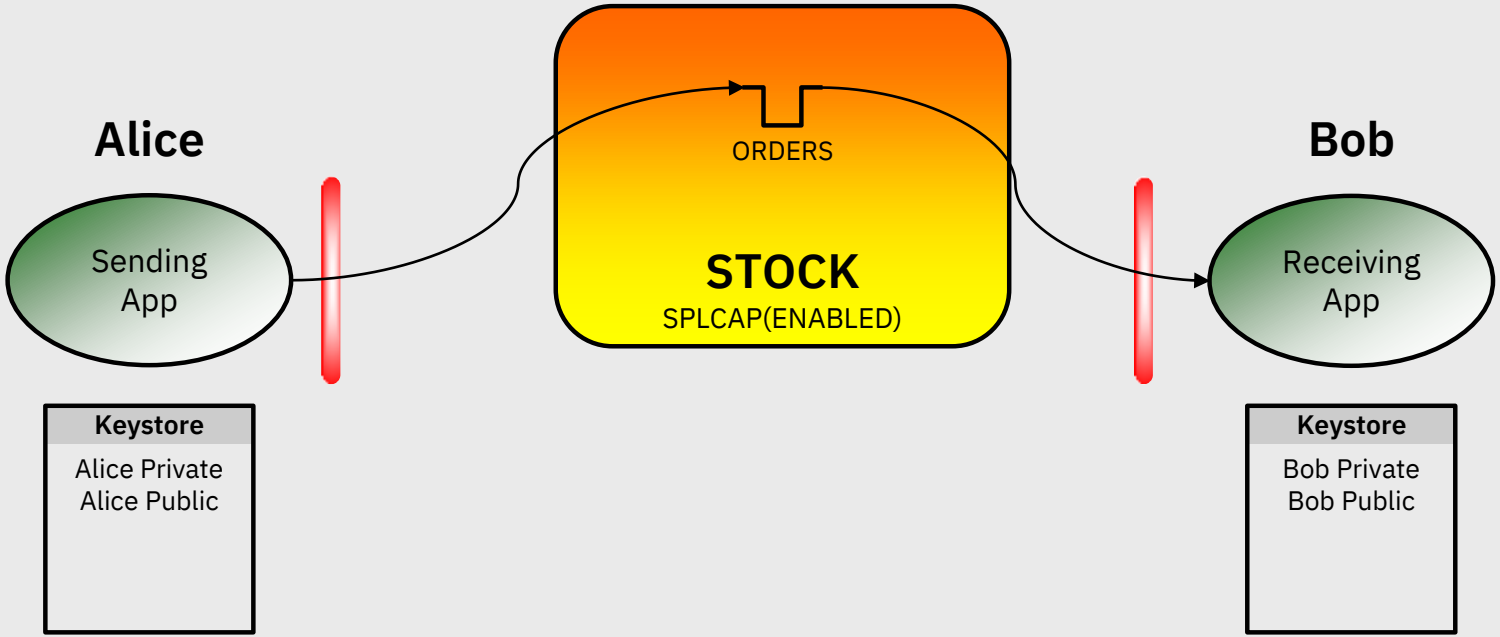
Securing an existing MQ application

1. Install AMS on the server



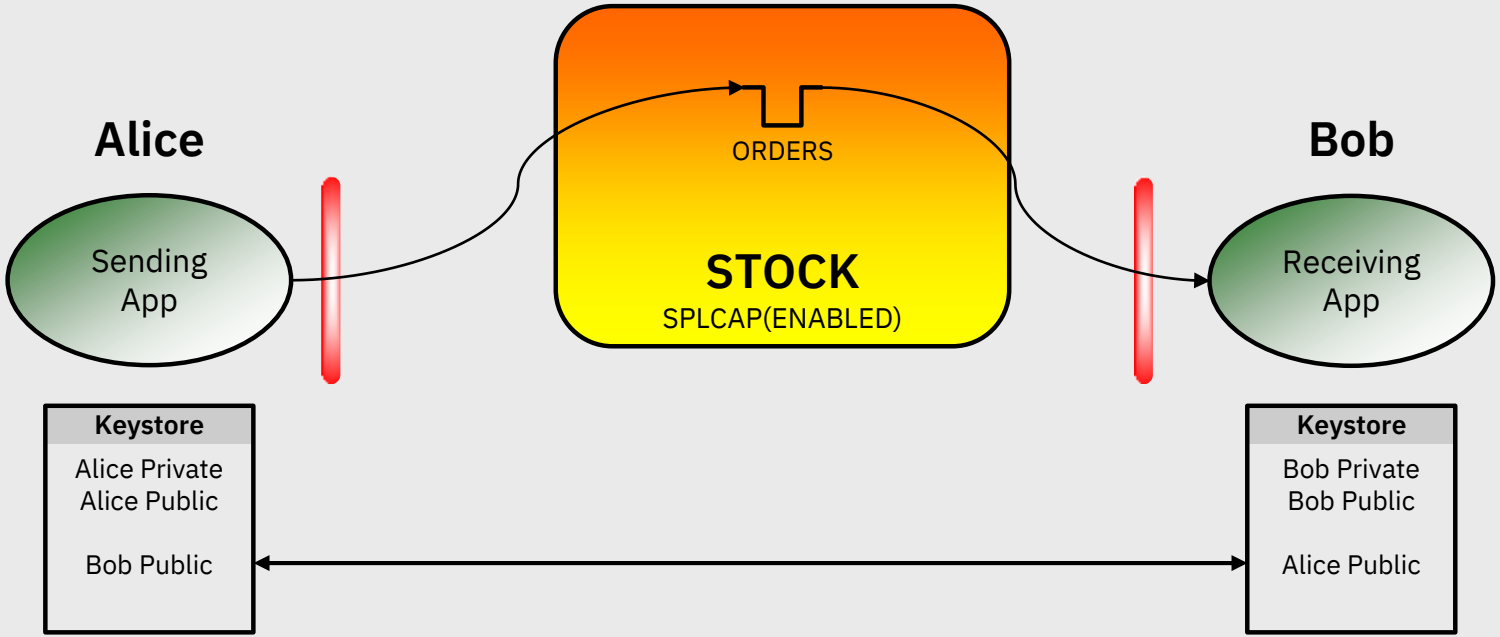
Securing an existing MQ application

1. Install AMS on the server
2. Create certificates (public/private key pairs)



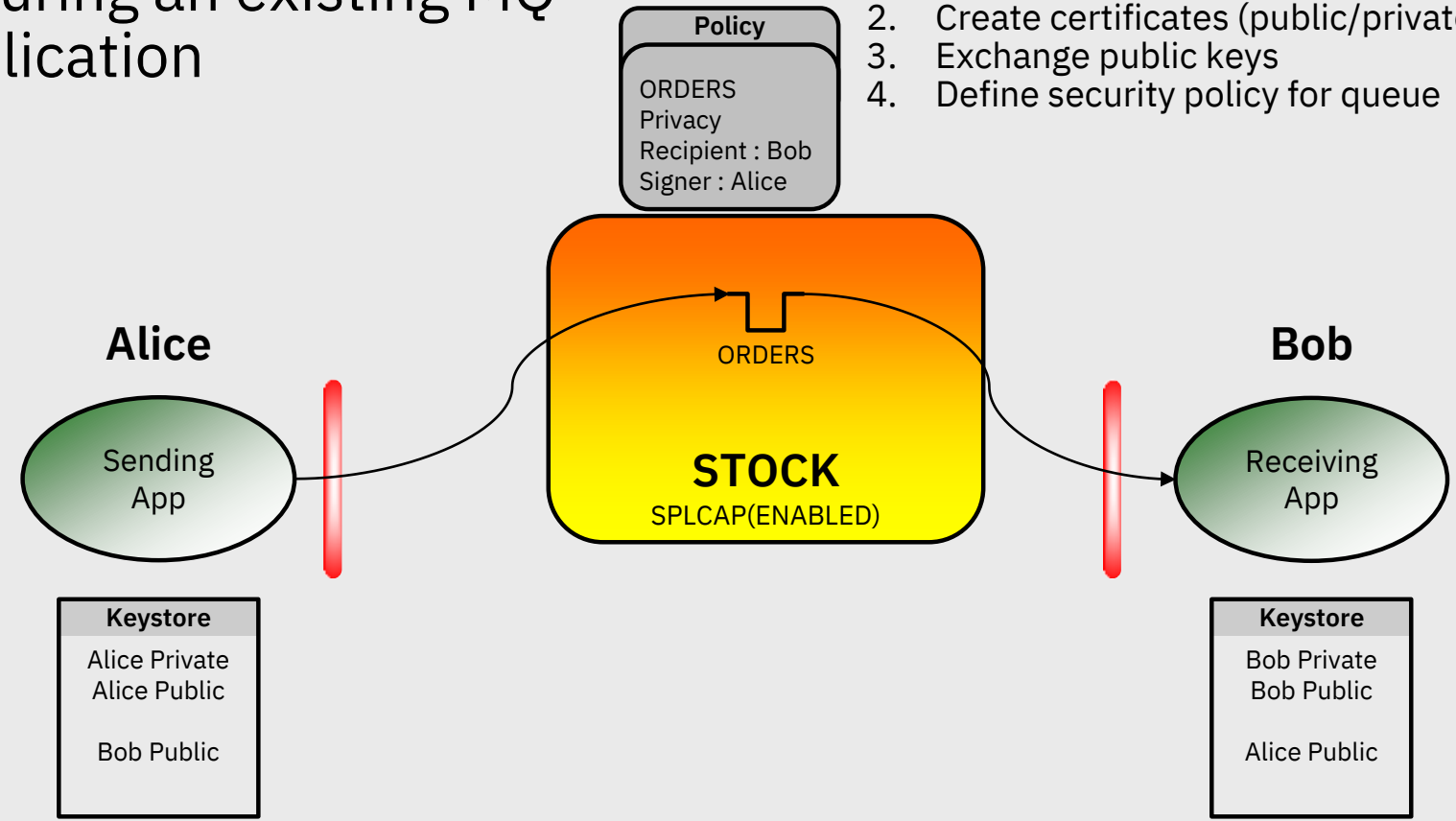
Securing an existing MQ application

1. Install AMS on the server
2. Create certificates (public/private key pairs)
3. Exchange public keys



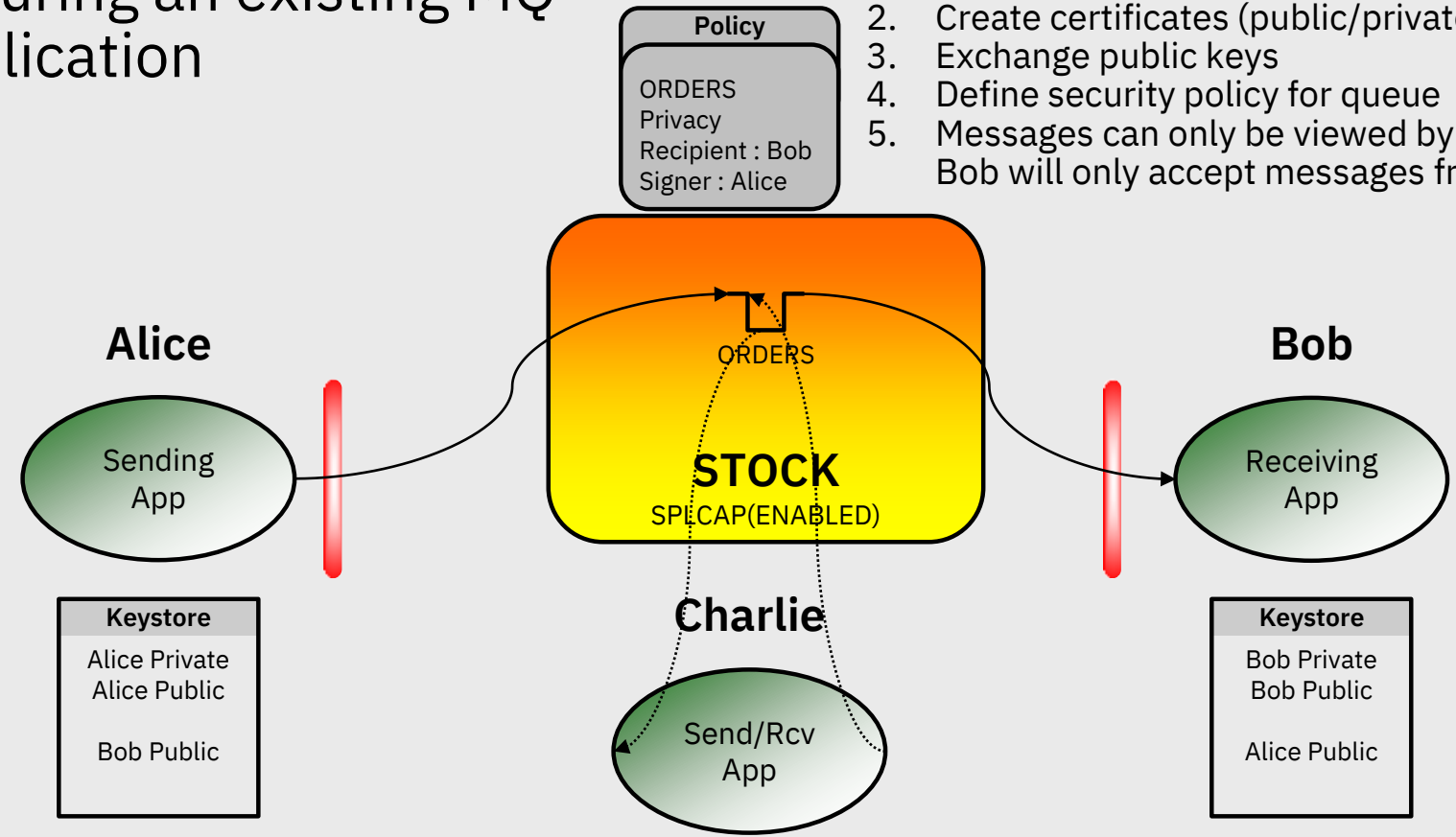
Securing an existing MQ application

1. Install AMS on the server
2. Create certificates (public/private key pairs)
3. Exchange public keys
4. Define security policy for queue



Securing an existing MQ application

1. Install AMS on the server
2. Create certificates (public/private key pairs)
3. Exchange public keys
4. Define security policy for queue
5. Messages can only be viewed by Bob
   Bob will only accept messages from Alice



Summary

- General Data Protection Regulation (GDPR) requires protection of personal data
- It applies to the personal data throughout its lifecycle, wherever it resides
- You might need to consider how IBM MQ is configured as part of your GDPR compliance
- IBM MQ Advanced Message Security provides message-level protection
  - Protects sensitive data from end to end (including from MQ administrators)

Additional resources

- IBM MQ Knowledge Center - https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_9.1.0/
- IBM Messaging developerWorks - https://developer.ibm.com/messaging
- IBM Messaging Youtube - https://ibm.biz/MQplaylist
- LinkedIn - ibm.biz/ibmmessaging
- Twitter - @IBMintegration

We want your feedback!

- Please submit your feedback online at ….
  - http://conferences.gse.org.uk/2018/feedback/JM
- Paper feedback forms are also available from the Chair person
- This session is JM