# IBM MQ Security: Deep dive including AMS

**Rob Parker, IBM**

**parrobe@uk.ibm.com**

# Important Disclaimer

- **THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY.**
- **WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.**
- **IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE.**
- **IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION.**
- **NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, OR SHALL HAVE THE EFFECT OF:**
  - CREATING ANY WARRANTY OR REPRESENTATION FROM IBM (OR ITS AFFILIATES OR ITS OR THEIR SUPPLIERS AND/OR LICENSORS); OR
  - ALTERING THE TERMS AND CONDITIONS OF THE APPLICABLE LICENSE AGREEMENT GOVERNING THE USE OF IBM SOFTWARE.
- **Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.**

# Agenda

- **AMS**
  - Recap
  - Important considerations
  - Message format
  - When will my message be protected?
  - Errors
  - Implementation

- **Channel Authentication**
  - Channel Authentication
  - Channel Authentication + Connection Authentication
  - Channel Authentication + Authorization
  - Early Adopt

# AMS

# Introduction

- **AMS means Advanced Message Security**

- **Provides message level security for messages**
  - Protects messages in transit and at rest
  - Protects messages from creation until destruction
  - Uses TLS features (encryption/signing) to protect message

- **Available as a separate license or in IBM MQ Advanced**

- **MQ has three options for AMS protection**
  - Integrity – Signing protection
  - Privacy – Signing and Encryption protection
  - Confidentiality – Encryption protection – MQ v9+ Only

# Important considerations

- **Performance**
  - Increase in CPU requirements (but in relation to MQ CPU requirements)
  - Cryptographic operations cause a decrease of message throughput
  - Impact depends on protection level (Integrity, Confidentiality, privacy)

- **Message size**
  - To accommodate AMS properties, overall message size will increase.
  - New message size = 1280 + [Old Message Length] + (200 x [# of recipients])

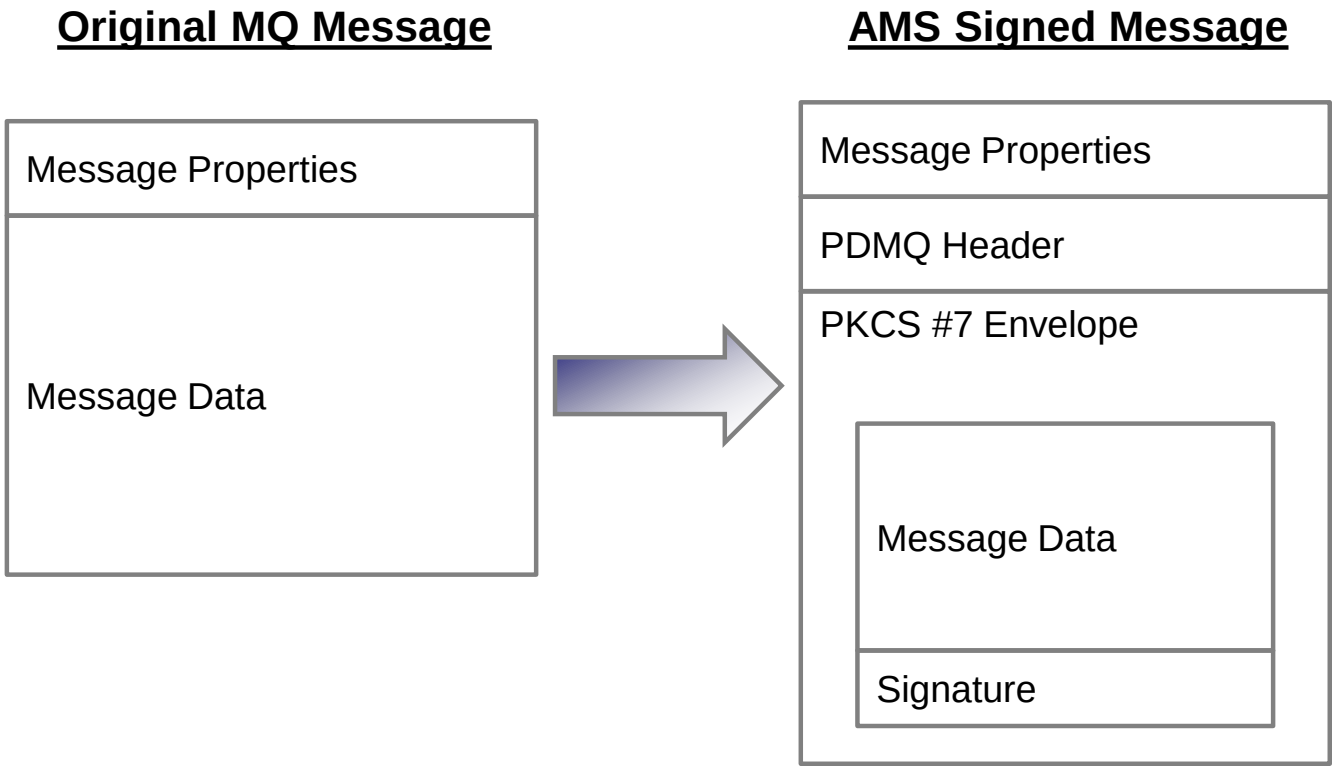
- **AMS does not perform access control**
  - It just protects the message contents from change and/or reading

# Important considerations

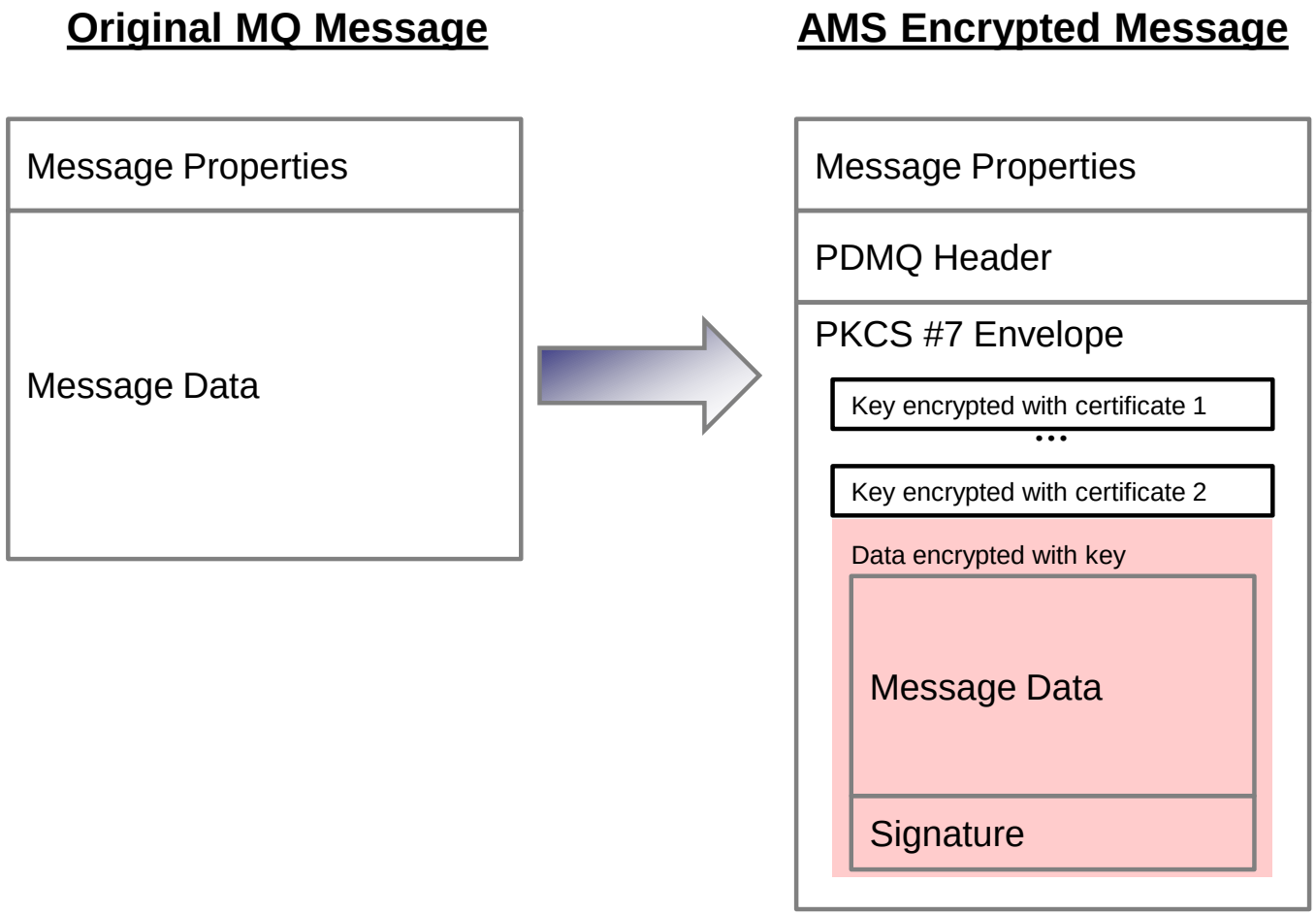
- **The following MQ Options are not supported with AMS**
  - Publish/Subscribe
  - Channel Data Conversion – message data conversion still supported
  - Distribution lists
  - IMS Bridge nor IMS programs in SRB mode (Only Pre MQ v8 AMS)
  - Non-Threaded applications using API exit on HP-UX
  - Java (JMS and Java “base” classes) only supported with MQv7
  - MQ message properties on z/OS
  - Only the IBM JRE is supported in MQv8 and before.

- **Unlike TLS, the entire certificate chain must be present in the keystore**
  - The sender must also have a copy of all the recipients public certificates

# Message format – Integrity policy



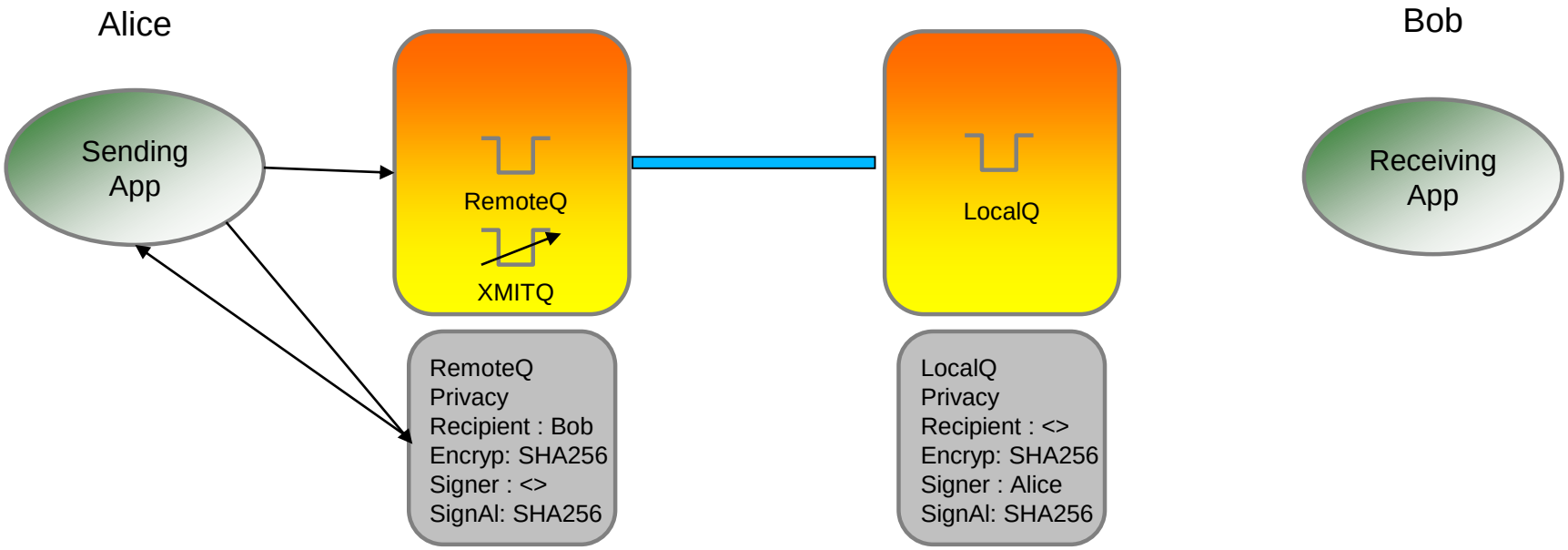
# Message format – Privacy policy



# When will my message be protected?

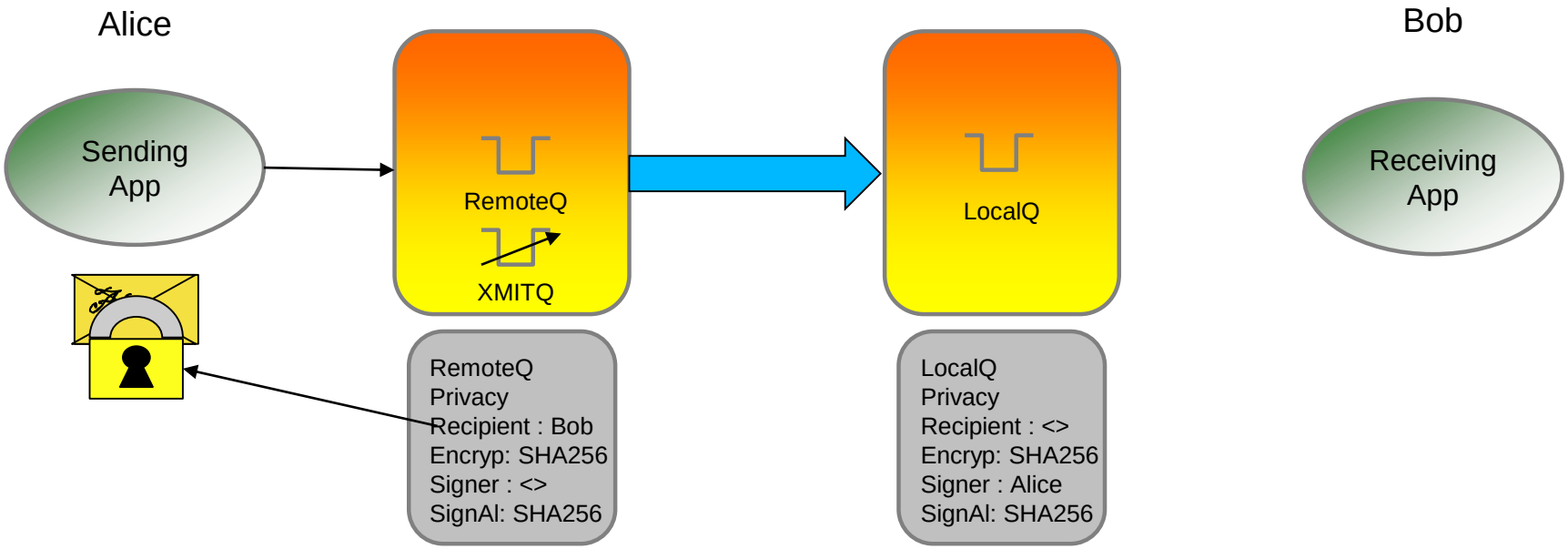
- **Messages are protected when they are created**
  - Level of protection depends on Policy: None, Integrity, Privacy, Confidentiality
  - Policies apply to all Queue Types: Remote, Alias, Local, Cluster, etc
- **During MQOPEN call, policies are queries**
  - IBM MQ looks for policies named the same as the Object being opened.
- **Once protected, the message retains the policy for its lifetime.**
- **At MQPUT:**
  - If there is a Integrity or privacy policy we sign the message data
  - If it is a privacy or confidentiality policy we encrypt for the specified recipients
- **At MQGET**
  - If there is a confidentiality or privacy policy we will decrypt the using our certificate or error
  - If there is a Integrity or privacy we check the message was signed by a signer listed in the policy

# When will my message be protected



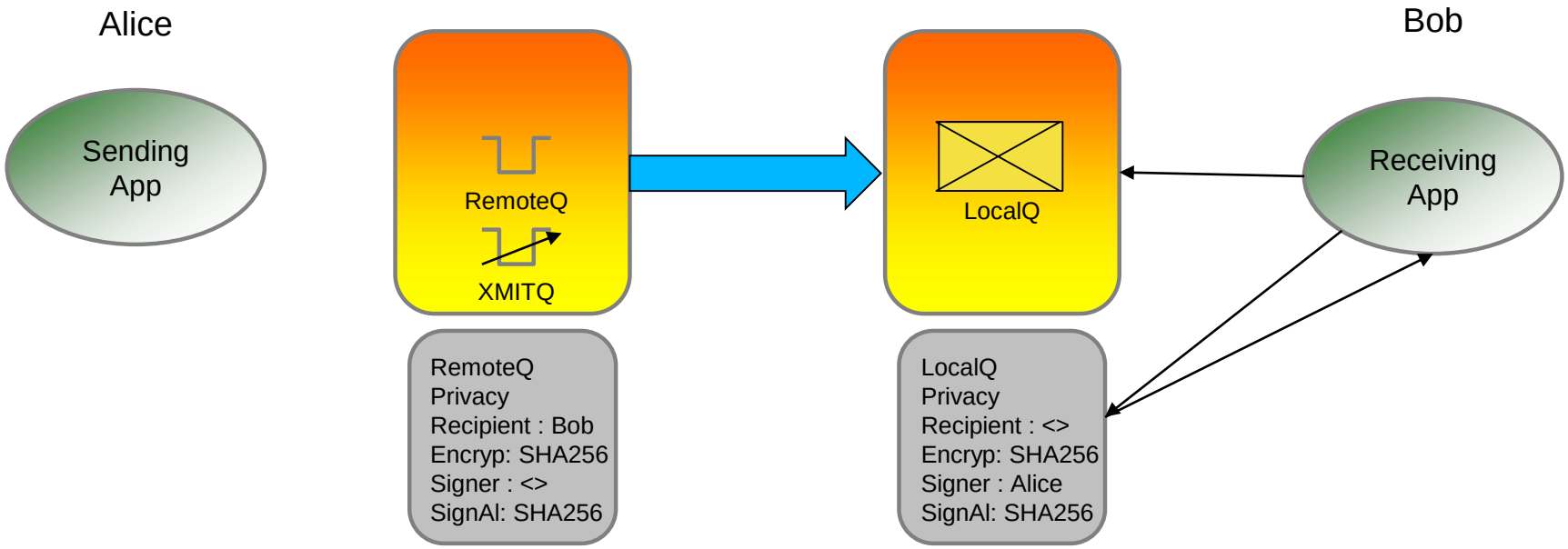

1. Alice's Application Calls MQOPEN on RemoteQ
2. MQOPEN Queries for Policy called RemoteQ and passes info back

# When will my message be protected



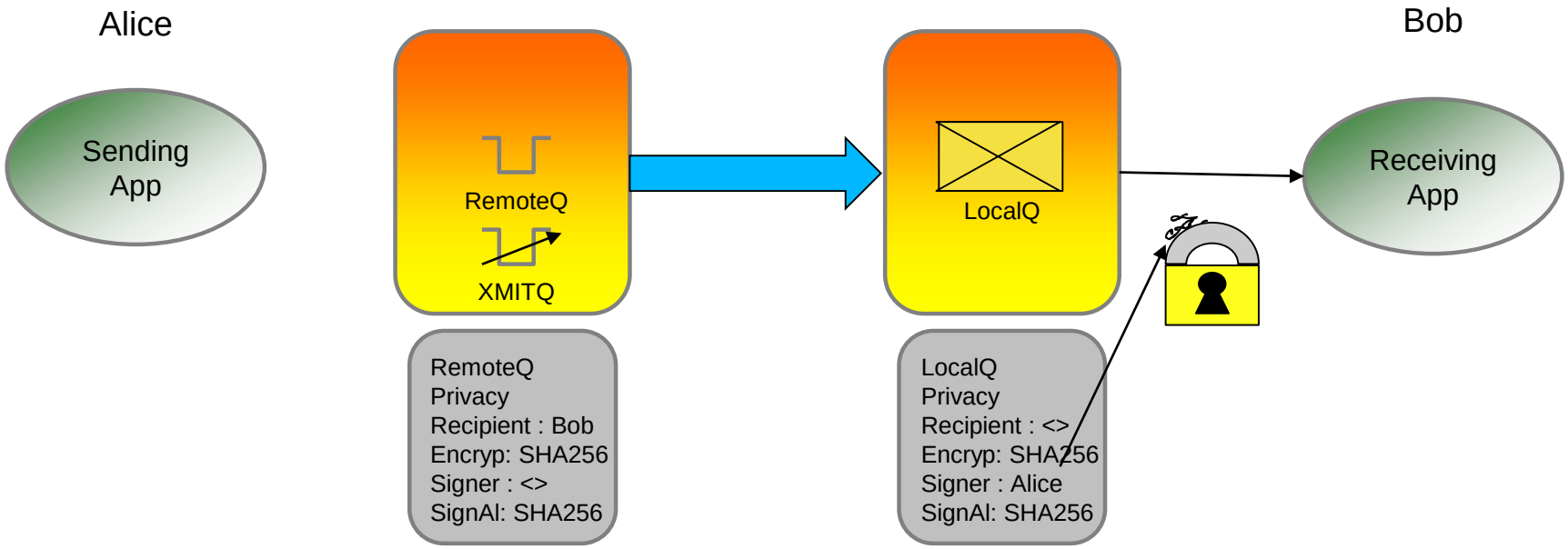

3. Alice issues a MQPUT to RemoteQ
    a) Because there is a privacy policy AMS signs the message data
    b) Because there is a privacy policy it also encrypts it for the recipients
4. The message is put to RemoteQ and flows over to the LocalQ

# When will my message be protected




5. Bob Issues an MQOPEN call to LocalQ
6. MQOPEN queries for any policies called LocalQ and returns the info

# When will my message be protected




7. Bob Issues MQGET
    a) Checks the Encryption Algorithm used is same or stronger
    b) Checks Bob can decrypt the message
    c) Checks the Signing Algorithm used is same or stronger
    d) Checks the message was from an authorised signer listed in the policy

8. Bob reads his message

# Errors

- **AMS uses the same error codes as security but interpreted differently**

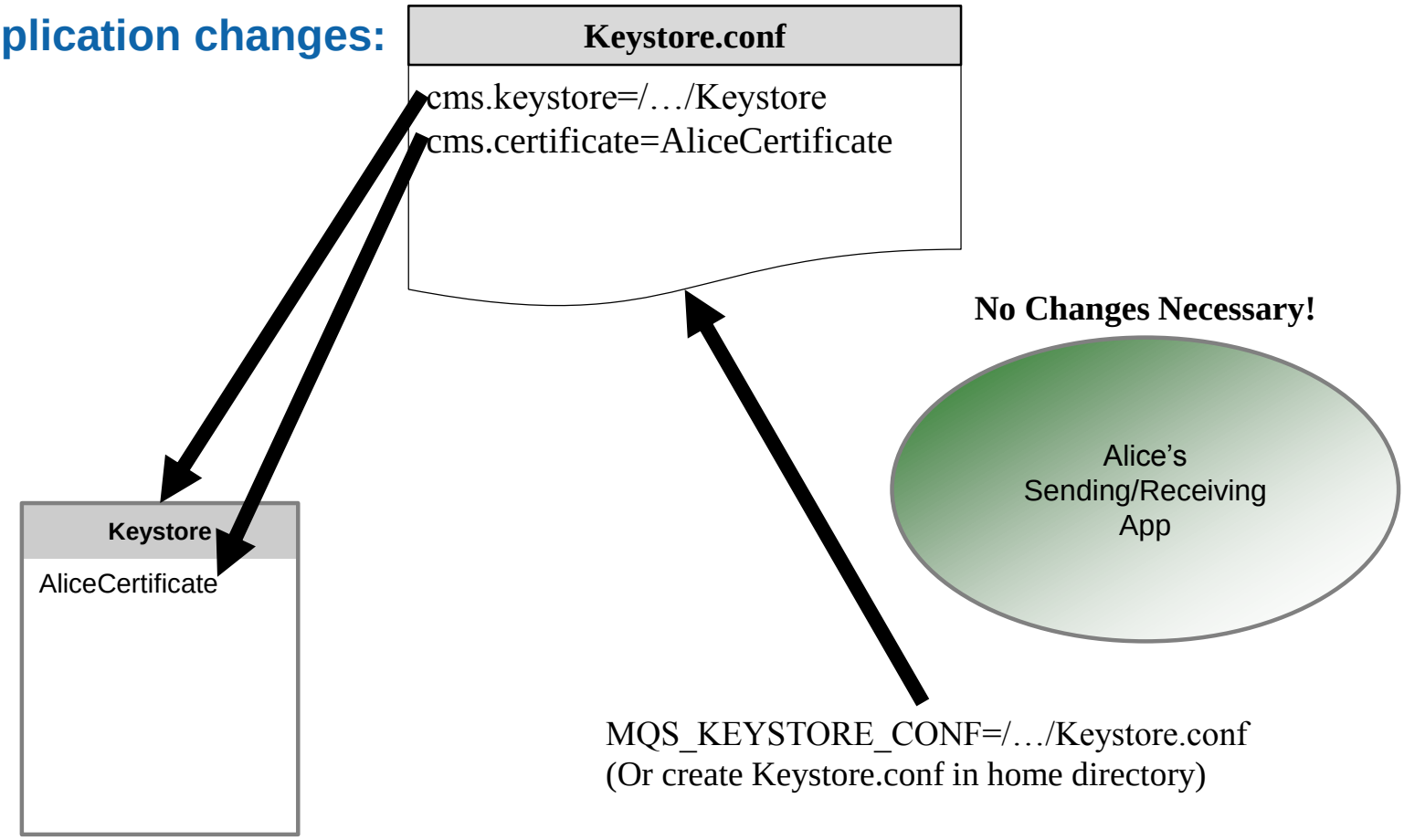
- **Several scenarios where something could go wrong:**
  - Putting to a protected Queue without Client AMS setup
  - GET/BROWSE a message you are not a recipient for
  - GET/BROWSE a message signed by someone not authorized
  - GET/BROWSE a message that has NOT been protected (got onto Q via AliasQ/RemoteQ etc)
  - Signing or encryption Algorithm in message is weaker than policy dictates during GET/BROWSE
  - Do not have correct certificates for the all listed Recipients
  - Misspelt Distinguished names for Authorized Signers or Recipients
  - Recipient does not have the signers certificate
  - Unlike TLS - full trust chain is not supplied. E.g. Signer cert, Intermediate CA cert, CA cert, etc
  - Error with Key Store configuration – Key Store Permissions, stanzas, etc

# Errors

- **What happens depends on operation being performed:**
  - MQPUT – 2063 error returned and message not accepted.
  - MQGET – 2063 error returned, message gains a DLQ header and is moved to SYSTEM.PROTECTION.ERROR Queue.
  - MQBROWSE – 2063 error returned.
  - Key Store related problems 2035 error returned.

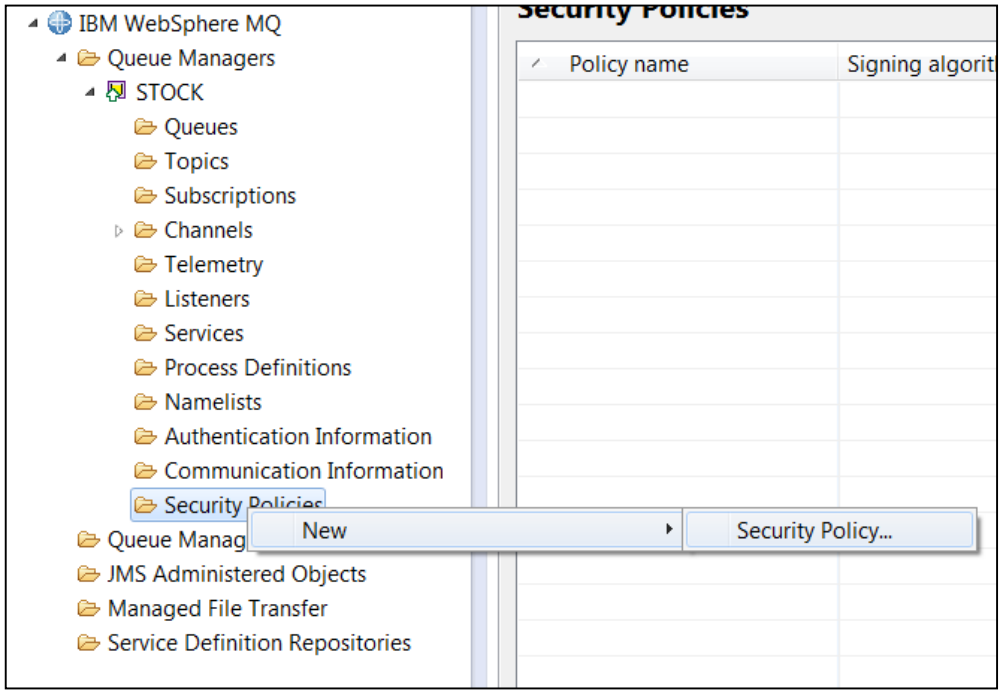
# Implementation

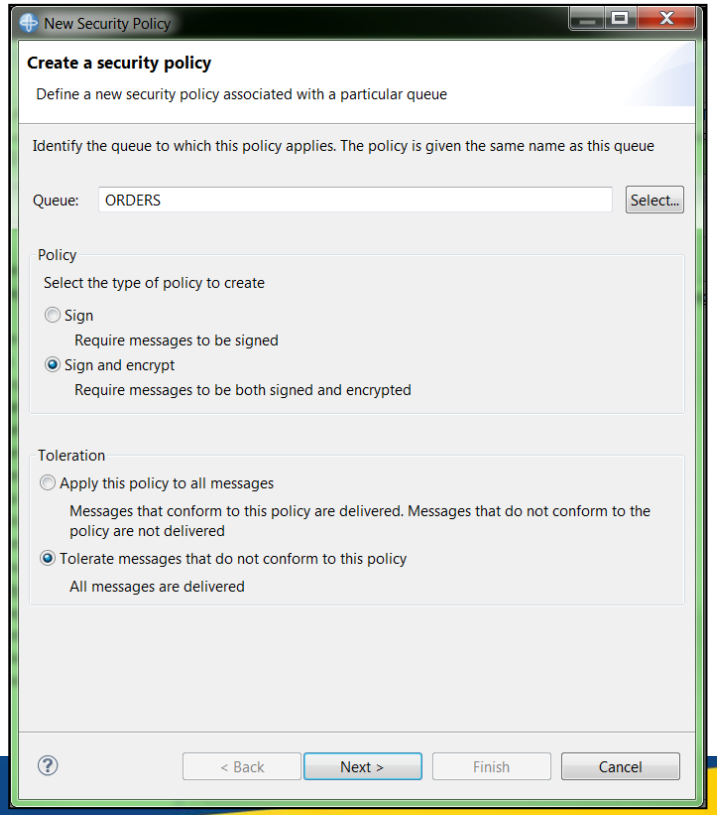
- We will assume the necessary certificates have already been exchanged
- Application changes:



# Implementation

- Set Security Policy using setmqspl, runmqsc or MQ Explorer
- `setmqspl -m STOCK -p ORDERS -s SHA256 -a "CN=ALICE,O=IBM,C=UK" -e AES256 -r "CN=BOB,O=IBM,C=UK"`



# CHANNEL AUTHENTICATION

# Details

- **Channel authentication rules are filters that can be applied for incoming connections**
  - Allowlisting – Allow connections based on a filter
  - Blocklisting – Block a connection based on a filter

- **The filters are applied on channels and are applied to all incoming connections for that channel**
  - The filter can be either very specific or generic. (Exact channel name or wildcard)

# Details

- **There are four types of filters:**
  - TLS Distinguished name (Issuer and Subject)
  - Client User ID name
  - Remote Queue Manager name
  - IP/Hostname

- **For IP/Hostname the connection can be allowed/blocked at the listener or channel**

- **For Client user ID, the userid blocked can be the userid connected with or the final adopted userid**

# Details

- **Channel Authentication rules have an order of checking:**
  1. BLOCKADDR
  2. ADDRESSMAP
  3. SSLPEERMAP
  4. QMGRMAP
  5. USERMAP
  6. BLOCKUSER

- **In addition if a connection matches two CHLAUTH rules where one has a specific filter and one has a generic filter then the CHLAUTH that is SPECIFIC will be acted on.**

- **For example two ADDRESSMAP:**
  - Block where address=*
  - Allow where address=129.12.9.9
  - Connection from 129.12.9.9 will be allowed through.

# Details

- **When you create a CHLAUTH rule you can specify what it should do when triggered.**

- **The options are:**
  - CHANNEL – Use the userid set in the channel MCAUSER for the future checks
  - MAP -Use the userid set in this CHLAUTH MCAUSER for the future checks
  - NOACCESS – Block the connection

- **In addition you can raise the security of the channel by setting a higher CHCKCLNT value on the CHLAUTH.**
  - If a user connects to CHANNEL.1 they are required to pass valid credentials
  - If a user connects to CHANNEL.2 they don't have to pass valid credentials.

# Configuration

- **Channel Authentication rules are created or modified in:**
  - MQ Explorer
  - runmqsc
- **Channel Authentication can be enabled/disabled from a queue manager property:**
  - `ALTER QMGR CHLAUTH(ENABLED|DISABLED)`
- **There is also the ability to enable rules that only print warnings**
  - `SET CHLAUTH(*) … WARN(NO|YES)`
- **Upon creation of a queue manager 3 default channel authentication rules**
  - Block all users who are MQ administrators
  - Block access to all SYSTEM channels
  - Allow access to SYSTEM.ADMIN.SVRCONN channel

# CHLAUTH & CONNAUTH

# Introduction

- **We use Authentication to ask clients connecting to prove they are who they say they are.**
  - Usually used in combination with authorisation to limit user's abilities.
- **Connection authentication feature available in MQ v8 and above.**
  - Allows authentication user credentials supplied by client applications.
- **There are 4 levels of connection authentication security**
  - None – no authentication performed security (code disabled)
  - Optional – credentials do not have to be supplied, but if supplied must be valid
  - Required – credentials must be supplied and valid
  - REQDADM – If the user is a MQ administrator they must supply credentials, if not they follow optional level.
- **For channel authentication records there is one attribute that can impact connection authentication:**
  - CHCKCLNT

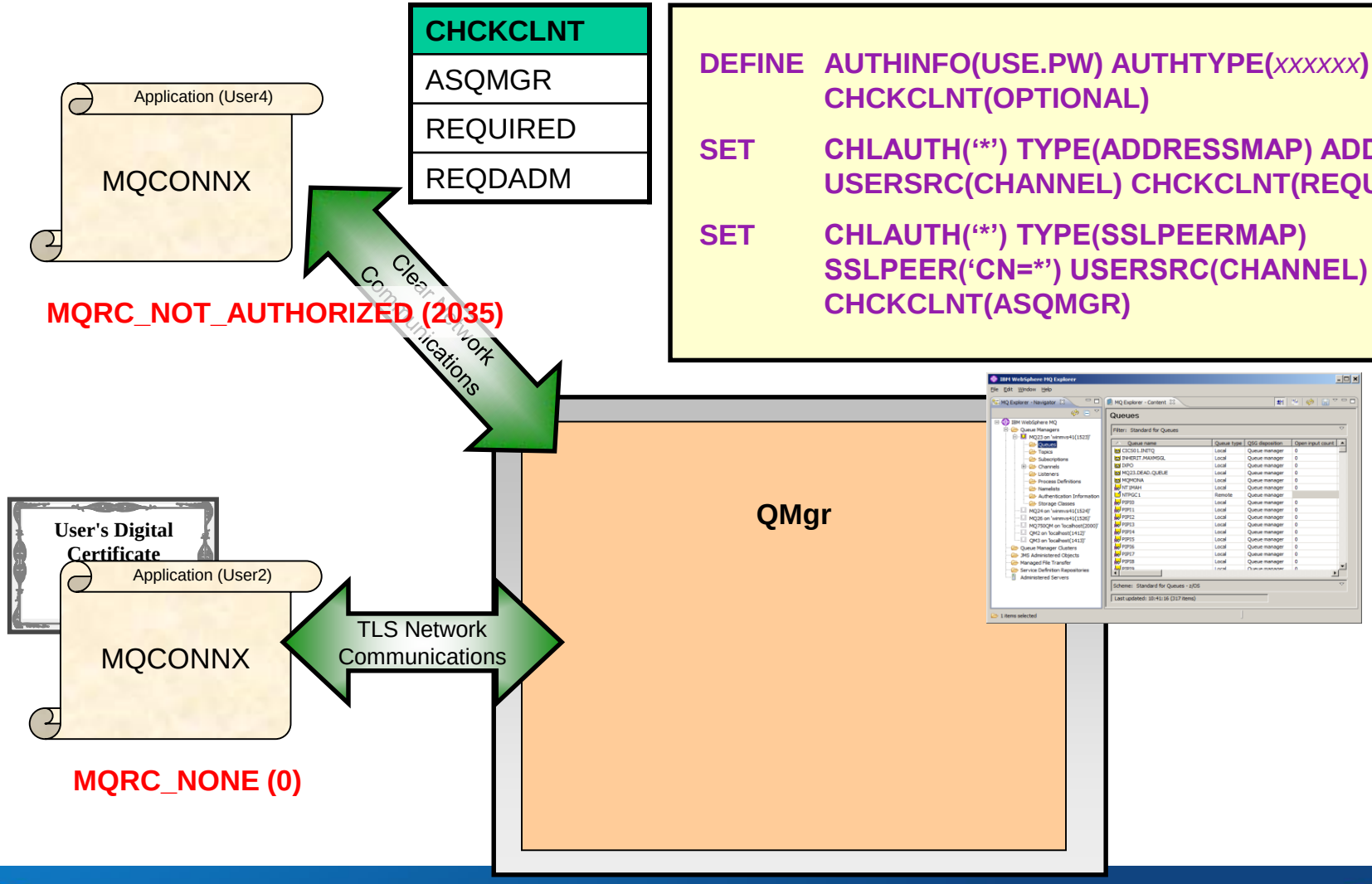
# CHCKCLNT

| CHCKCLNT |
| --- |
| ASQMGR |
| REQUIRED |
| REQDADM |

```
DEFINE  AUTHINFO(USE.PW) AUTHTYPE(xxxxxx)
        CHCKCLNT(OPTIONAL)

SET     CHLAUTH('*') TYPE(ADDRESSMAP) ADDRESS('*')
        USERSRC(CHANNEL) CHCKCLNT(REQUIRED)

SET     CHLAUTH('*') TYPE(SSLPEERMAP)
        SSLPEER('CN=*') USERSRC(CHANNEL)
        CHCKCLNT(ASQMGR)
```



# CHLAUTH & AUTHORIZATION

# Introduction

- **We use Authorization to limit what connected users can and cannot do.**
- **This is performed by creating authority records**
  - We create authority records for a specific user or group.
  - User level authority records not available on Linux.
- **A channel or channel authentication rule can change the userid used for authority checks**
- **For channel authentication records there is one attribute that can impact authorization:**
  - MCAUSER

# MCAUSER

- **USERSRC(MAP) allows you to specify a new userid to adopt for authorization checks.**
- **It is available on most channel authentication records.**
- **You specify the user id to use by using the MCAUSER attribute**
  - If you specify USERSRC(MAP) then MCAUSER is required

```
SET CHLAUTH('*') TYPE(ADDRESSMAP) ADDRESS('*') USERSRC(MAP)
MCAUSER('UserA')
```

# CHLAUTH, CONNAUTH AND EARLYADOPT

# What is EarlyAdopt?

- **One year ago today….**

- **With ADOPTCTX(YES) Connection Authentication was overriding Channel authentication Map rules.**
  - Whatever user you (successfully) authenticated with would be used for authorization.
  - This was a problem for when you would do MCAUSER('*NOBODY')

- **EarlyAdopt was created to allow you to change this so the Channel Authentication Mapping Rules could override CONNAUTH.**
  - Now the Mapping rules could set a new MCAUSER

- **It is enabled using the "ChlauthEarlyAdopt=Y" parameter in the Channels stanza of the qm.ini.**

# Which user will be used for authorization?

| Method | Notes |
|---|---|
| **Client machine user ID flowed to server** | This will be over-ridden by anything else. Rarely do you want to trust an unauthenticated client side user ID. |
| **MCAUSER set on SVRCONN channel definition** | A handy trick to ensure that the client flowed ID is never used is to define the MCAUSER as ‘rubbish’ and then anything that is not set appropriately by one of the next methods cannot connect. |
| **MCAUSER set by CHLAUTH rule** | To allow more granular control of MCAUSER setting, rather than relying on the above queue manager wide setting, you can of course use CHLAUTH rules |
| **MCAUSER set by ADOPTCTX(YES)** | The queue manager wide setting to adopt the password authenticated user ID as the MCAUSER will over-ride either of the above. |
| **MCAUSER set by Security Exit** | Although CHLAUTH gets the final say on whether a connection is blocked (security exit not called in that case), the security exit does get called with the MCAUSER CHLAUTH has decided upon, and can change it. |

# Which user will be used for authorization with Early Adopt?

| Method | Notes |
|---|---|
| **Client machine user ID flowed to server** | This will be over-ridden by anything else. Rarely do you want to trust an unauthenticated client side user ID. |
| **MCAUSER set on SVRCONN channel definition** | A handy trick to ensure that the client flowed ID is never used is to define the MCAUSER as ‘rubbish’ and then anything that is not set appropriately by one of the next methods cannot connect. |
| **MCAUSER set by ADOPTCTX(YES)** | The queue manager wide setting to adopt the password authenticated user ID as the MCAUSER will over-ride either of the above. |
| **MCAUSER set by CHLAUTH rule** | To allow more granular control of MCAUSER setting, rather than relying on the above queue manager wide setting, you can of course use CHLAUTH rules |
| **MCAUSER set by Security Exit** | Although CHLAUTH gets the final say on whether a connection is blocked (security exit not called in that case), the security exit does get called with the MCAUSER CHLAUTH has decided upon, and can change it. |

# Details

- **Assuming the following:**
  - UserA is the user running the application
  - UserB is the user being supplied in MQCSP structure
    - Although this could also be set to BLANK
  - There are two Channel Authentication mapping rules:
    - 1. Maps UserA to UserA-2
    - 2. Maps UserB to UserB-2
  - All security checks pass

# Details

| MQCSP Supplied | ADOPTCTX | Early Adopt | Resulting MCAUSER |
|---|---|---|---|
| BLANK | NO | NO | UserA-2 |
| UserB | NO | NO | UserA-2 |
| BLANK | YES | NO | UserA-2 |
| UserB | YES | NO | UserB |
| BLANK | NO | YES | UserA-2 |
| UserB | NO | YES | UserA-2 |
| BLANK | YES | YES | UserA-2 |
| UserB | YES | YES | UserB-2 |

# Details

- **In Short:**
- **When UserID supplied in MQCSP is BLANK or ADOPTCTX is NO**
  - We honour the Channel authentication rule and so end up with UserA-2
- **When ADOPTCTX is set to YES it depends on what EarlyAdopt is set to:**
  - If Early Adopt is off – We get UserB
  - If Early Adopt is on – We get UserB-2

# Where can I get more information?

IBM Messaging developerWorks
developer.ibm.com/messaging


IBM Messaging Youtube
https://www.youtube.com/IBMmessagingMedia

LinkedIn
Ibm.biz/ibmmessaging

~~Twitter~~
~~@IBMMessaging~~

~~IBM MQ Facebook~~
~~Facebook.com/IBM-MQ-8304628654/~~

# Would you like to take part in IBM MQ Design Research?

- **The IBM MQ team is currently conducting some long term research with our MQ customer base.**
- **With this survey we would like to understand:**
  - Who is interreacting with MQ and what are their responsibilities?
  - Which customers are interested in moving IBM MQ into the cloud?
  - Which customers would like to take part in future research?
- **We estimate the survey should take 4 minutes to complete.**
- **Please note: This survey is for distributed users only.**
- **If you're interested, go to ibm.biz/MQ-Customer-Survey**

# Questions & Answers

# 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 according to 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 is in compliance with 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 in connection with 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 particular, 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, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services®, Global Technology Services®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli® Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, 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.