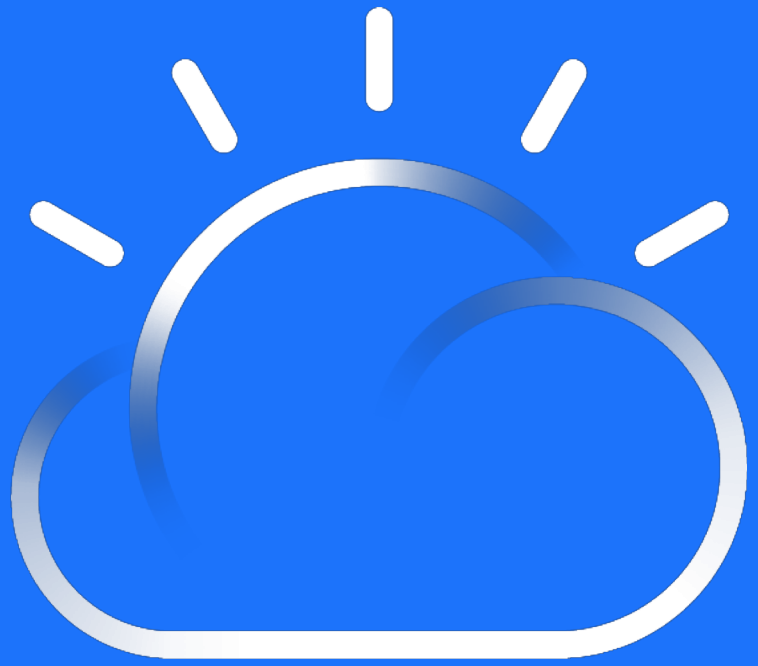
Integration Technical Conference 2019

M14 – MQ Security Deep Dive

Rob Parker
Software Engineer, Security Focal, IBM MQ Development.
parrobe@uk.ibm.com



IBM **Cloud**

IBM

Please note:

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.
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.
Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

Agenda

- What user will be authorized?
- What is Channel Authentication Early Adopt?
- Advanced Message Security

What user will be authorized?

What user will be authorized?

Recap

- This is performed by creating authority records
  - We create authority records for a specific user or group.
  - User level authority records are available on Linux but not by default
- Authority is given on MQ objects and dictate what actions they can performed (PUT, GET, OPEN, etc)
- MQ Administrators (mqm) has full permissions.
  - Should rarely allow people to use this userid.
- Applications connecting use a user for authorization.
  - Group membership for that user is determined once but can be refreshed
  - Group membership can be determined from a number of repositories (OS,LDAP,PAM)

What user will be authorized?

Recap

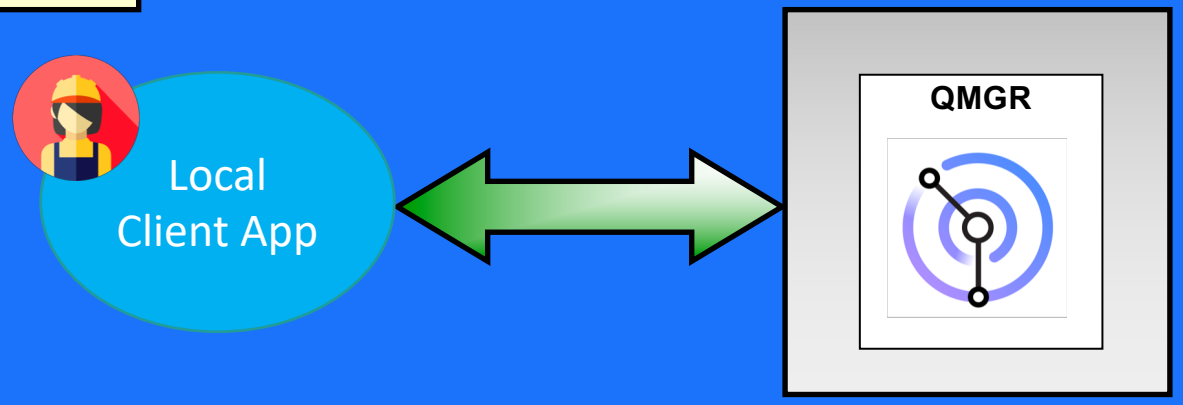
- Applications can flow two userids:
  - The userid that the application is running as (always)
  - The userid & password that the application wants to authenticate as (optional)
- A client application connecting via network connections will go through the following security checks
  - Channel Authentication
  - Connection authentication
  - Security Exits
- There are multiple places that the userid used for authority checks can be set

What user will be authorized?

Our scenario

App1
Running as: UserA
Supplied User: ---
Channel: IN

QM1
DEFINE CHANNEL(IN) CHLTYPE(SVRCONN)
SET AUTHREC OBJTYPE(QMGR) **PRINCIPAL('UserB')** AUTHADD(CONNECT)

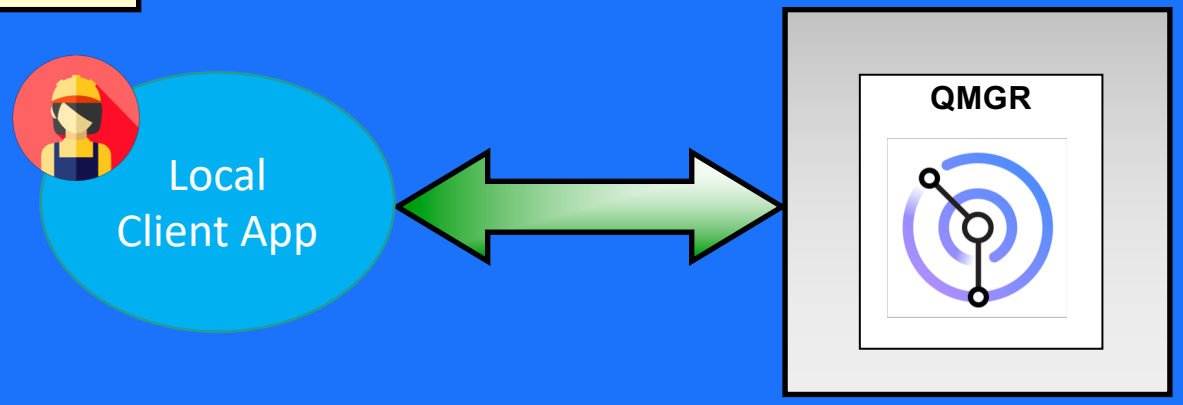


What user will be authorized?

The Userid running the application

App1
Running as **UserB**
Supplied User: ---
Channel: IN

QM1
DEFINE CHANNEL(IN) CHLTYPE(SVRCONN)
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('UserB') AUTHADD(CONNECT)

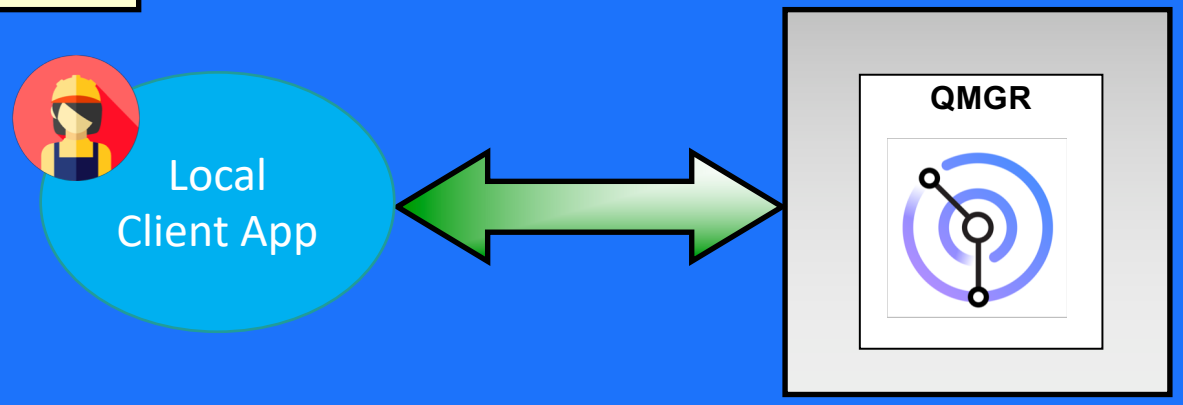


What user will be authorized?

Channel MCAUSER

App1
Running as: UserA
Supplied User: ---
Channel: IN

QM1
DEFINE CHANNEL(IN) CHLTYPE(SVRCONN) **MCAUSER('UserB')**
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('UserB') AUTHADD(CONNECT)

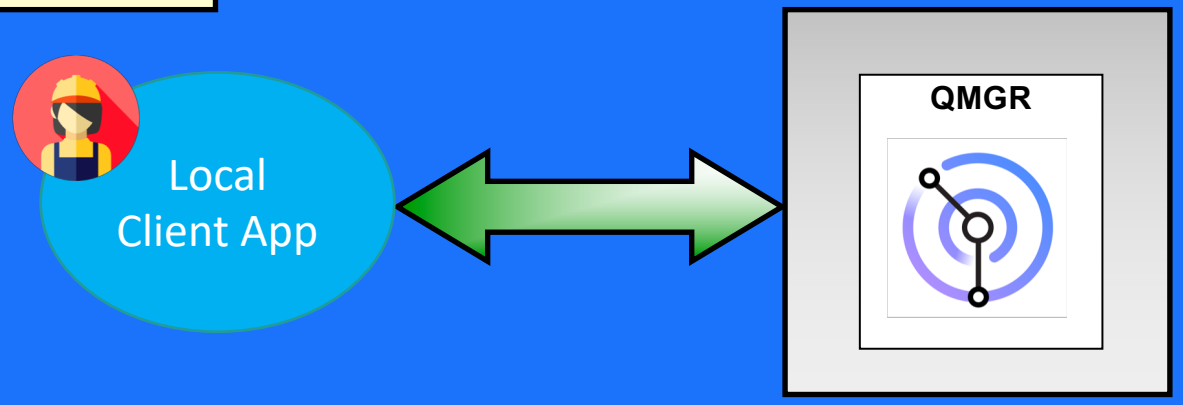


What user will be authorized?

Connection Authentication ADOPTCTX

App1
Running as: UserA
Supplied User: **UserB**
Channel: IN

QM1
DEFINE CHANNEL(IN) CHLTYPE(SVRCONN)
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('UserB') AUTHADD(CONNECT)
DEFINE AUTHINFO(**) AUTHTYPE(**) *** **ADOPTCTX(YES)**

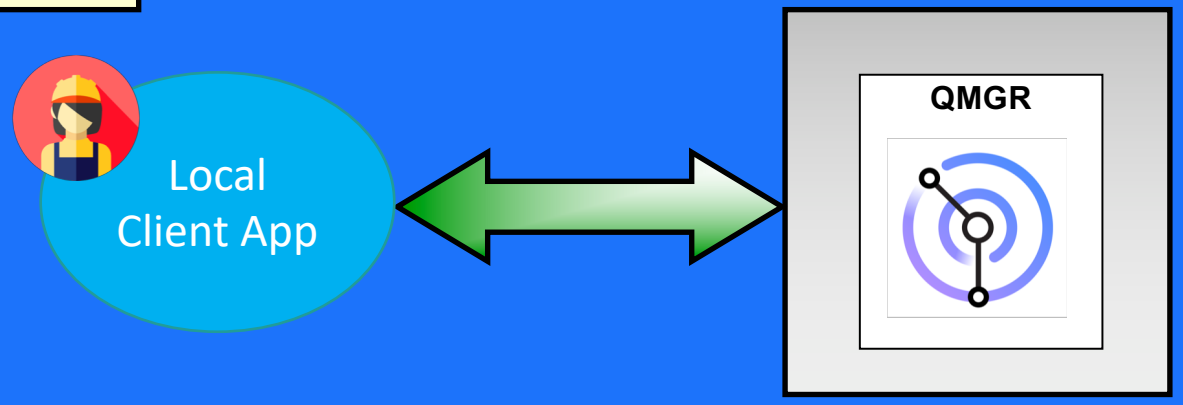


What user will be authorized?

Chanenl Authentication MAP

App1
Running as: UserA
Supplied User: ---
Channel: IN

QM1
DEFINE CHANNEL(IN) CHLTYPE(SVRCONN)
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('UserB') AUTHADD(CONNECT)
SET CHLAUTH(**) TYPE(**MAP) **USERSRC(MAP) MCAUSER('UserB')**

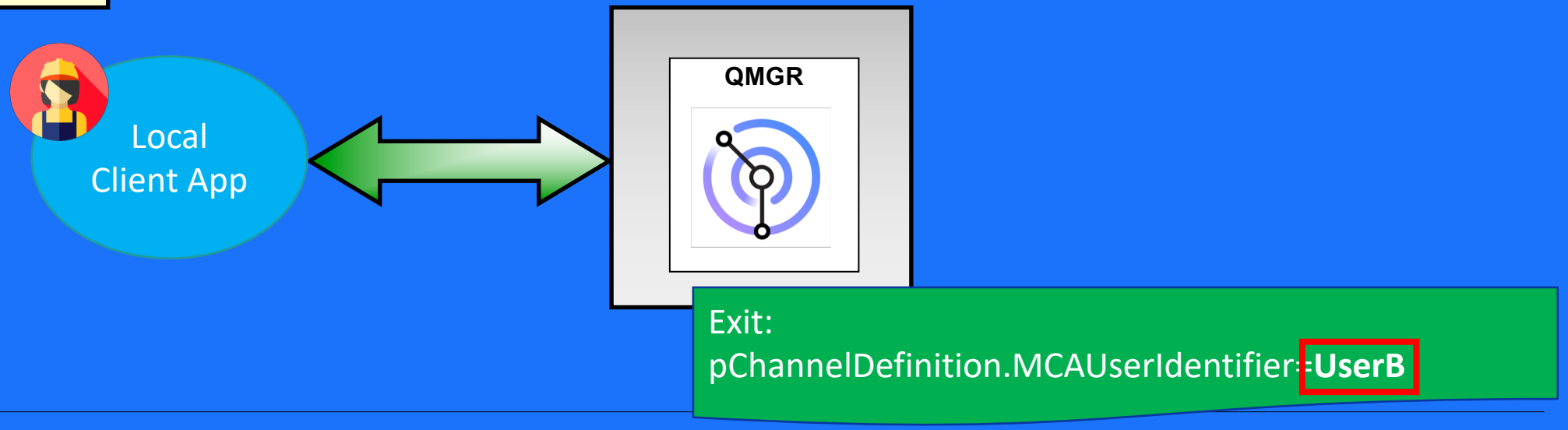


What user will be authorized?

Security Exits

App1
Running as: UserA
Supplied User: ---
Channel: IN

QM1
DEFINE CHANNEL(IN) CHLTYPE(SVRCONN) **SCYEXIT('Exit')**
SET AUTHREC OBJTYPE(QMGR) PRINCIPAL('UserB') AUTHADD(CONNECT)



What user will be authorized?

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.

EarlyAdopt

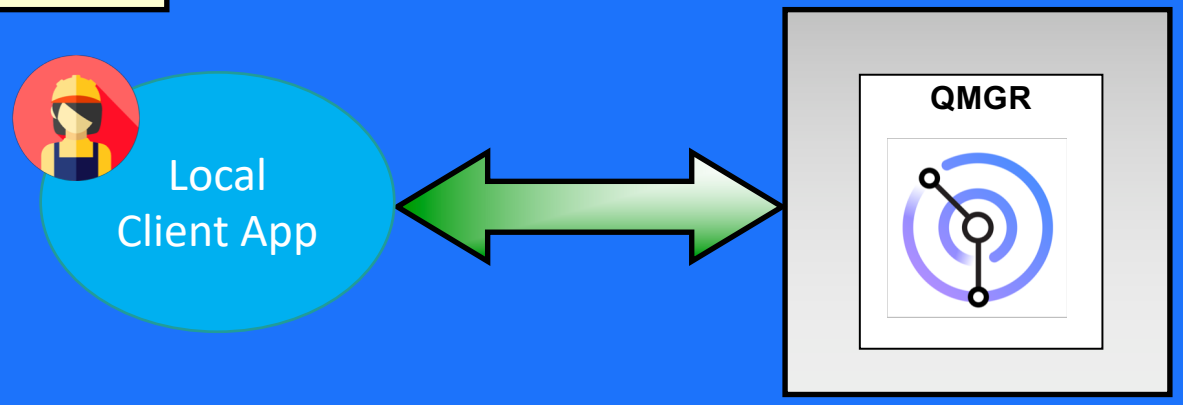
What user will be authorized?

A quick test – What user will be authorized?

App1
Running as: UserA
Supplied User: UserC
Channel: IN

QM1

```
DEFINE CHANNEL(IN) CHLTYPE(SVRCONN) MCAUSER('UserB')
SET CHLAUTH(**) TYPE(USERMAP) CLNTUSER('UserA')USERSRC(MAP)
MCAUSER('UserD')
DEFINE AUTHINFO(**) AUTHTYPE(**) *** ADOPTCTX(NO)
```



Answer:
UserD!

Channel Authentication Early Adopt

Integration Technical Conference 2019

CHLAUTH EarlyAdopt

Channel authentication records & Connection authentication

- In the first release of Connection Authentication (v8), ADOPTCTX(YES) had a higher precedence than CHLAUTH
  - If you changed the MCAUSER with a chlauth map rule, adoptctx would override it.
- A thorough investigation by T.Rob of IoPT Consulting provided examples of areas this could cause problems:
  - SET CHLAUTH(*) ** MCAUSER(‘*nobody’)
- EarlyAdopt was developed and backported to allow users to influence the precedence between chlauth and connauth.
- Additionally the defaults for MQ were changed so that:
  - ADOPTCTX = YES
  - EarlyAdopt = YES

CHLAUTH EarlyAdopt

Channel authentication records & Connection authentication

- EarlyAdopt is configured using qm.ini attributes
  - Channels: ChlauthEarlyAdopt=y|n

- More information on interactions between Channel Authentication and Connection Authentication: https://www.ibm.com/developerworks/community/blogs/messaging/entry/Connection_Authentication_Channel_Authentication_interactions?lang=en

Advanced Message Security

Integration Technical Conference 2019

Advanced Message Security

Introduction

- 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

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

Advanced Message Security

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

Advanced Message Security

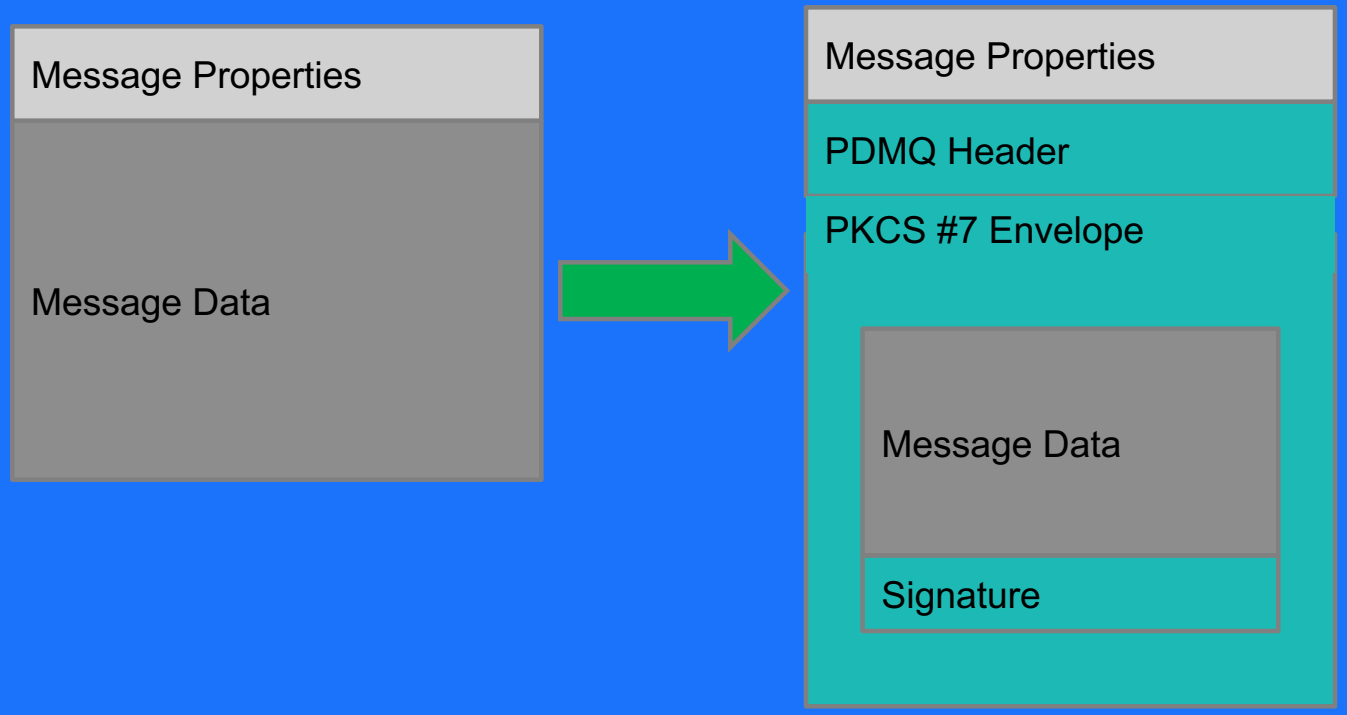
Limitations

- 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

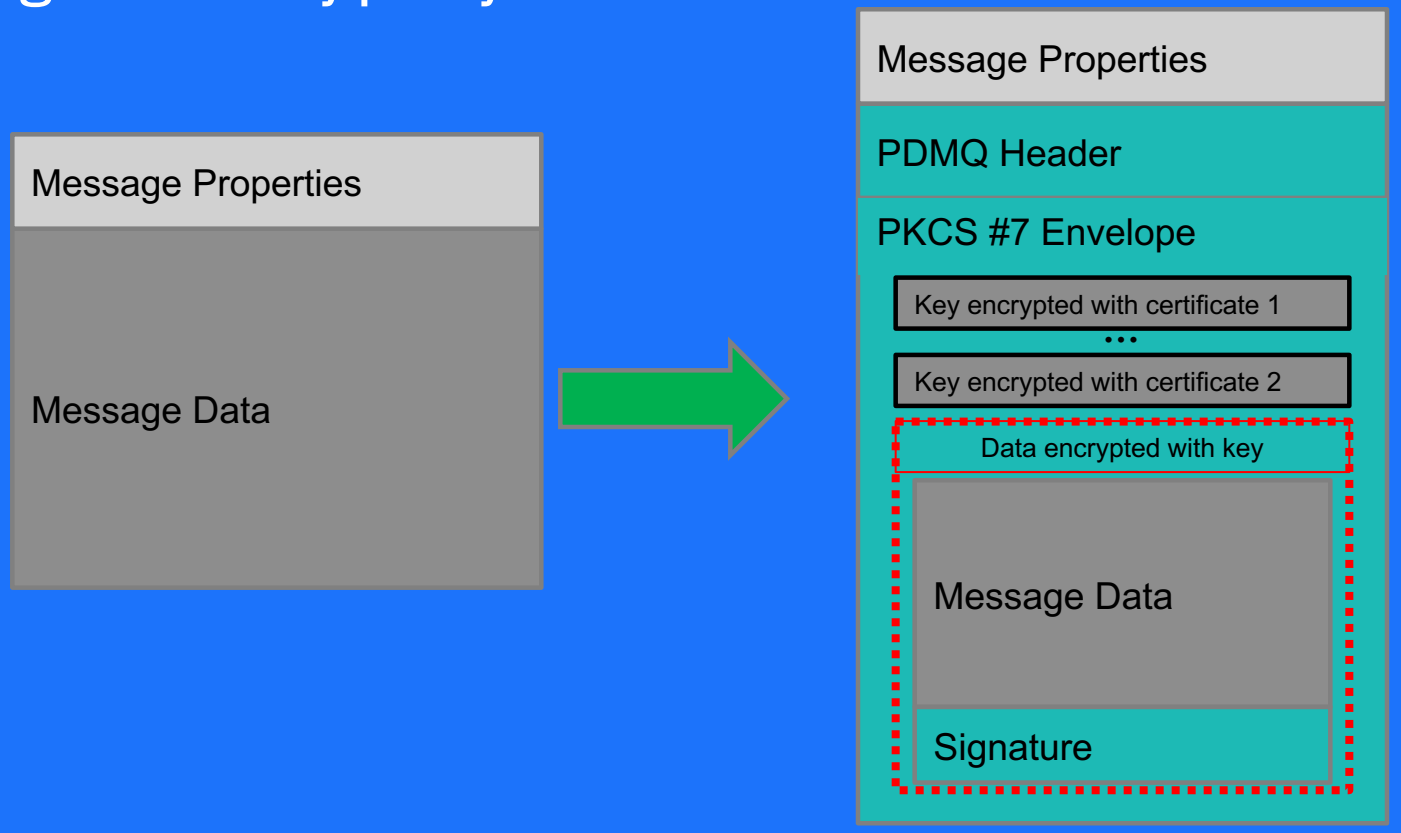
Advanced Message Security

Message changes – Integrity policy



Advanced Message Security

Message changes – Privacy policy



Advanced Message Security

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.
- You can set either the Client to handle AMS or the Queue Manager

Advanced Message Security

Error Cases

- 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

Advanced Message Security

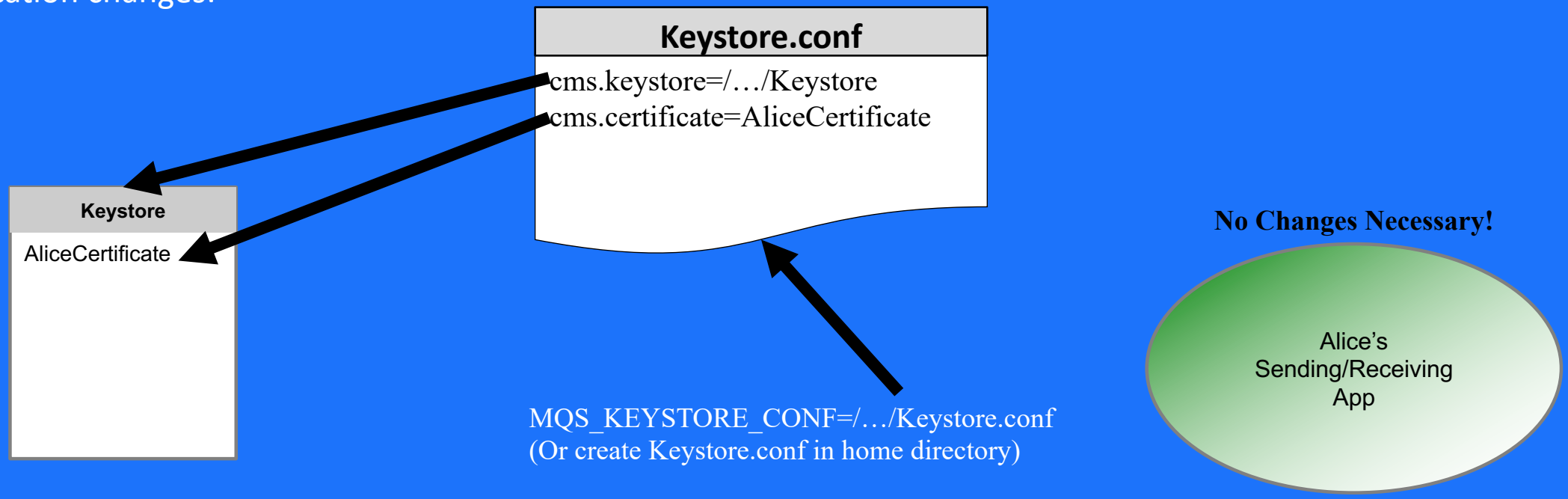
Error cases

- 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.

Advanced Message Security

Implementation

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



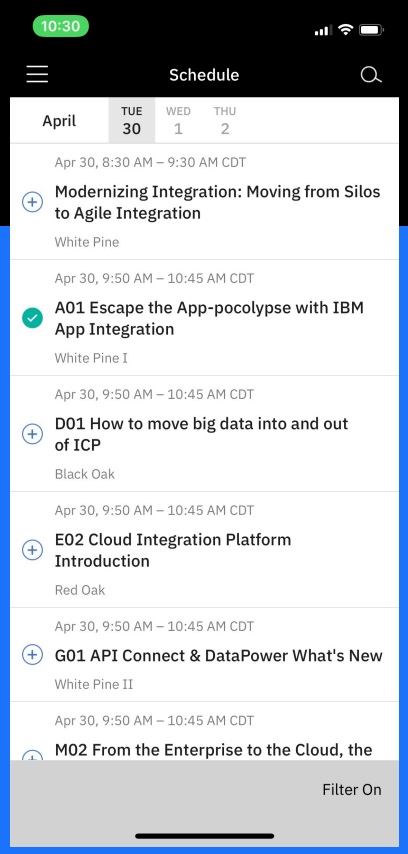
More information?

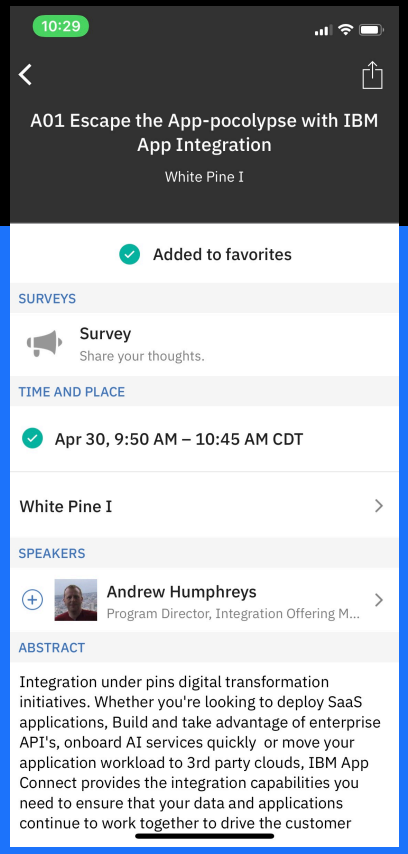
IBM Messaging developerWorks
developer.ibm.com/messaging

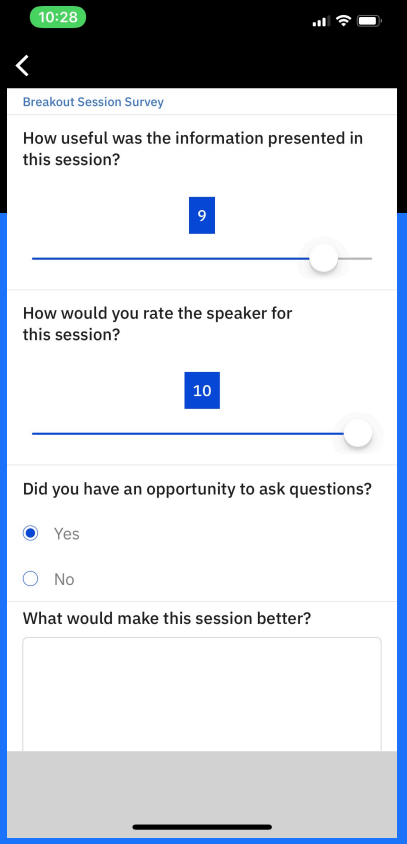
IBM Messaging Youtube
https:// ibm.biz/MQplaylist

LinkedIn
https://ibm.biz/ibmmessaging

Questions?







Don’t forget to fill out the survey!

Select your session, select survey, rate the session and submit!

Thank You

Notices and disclaimers

Notices and disclaimers

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.
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.

Notices and disclaimers