

Securing your IBM MQ environment.

Rob Parker, IBM

parrobe@uk.ibm.com

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

■ Introduction

- Why security matters
- What security features there are

■ Overview of each security feature

■ Designing your security implementation

■ Questions

Security Matters

■ A data breach can mean:

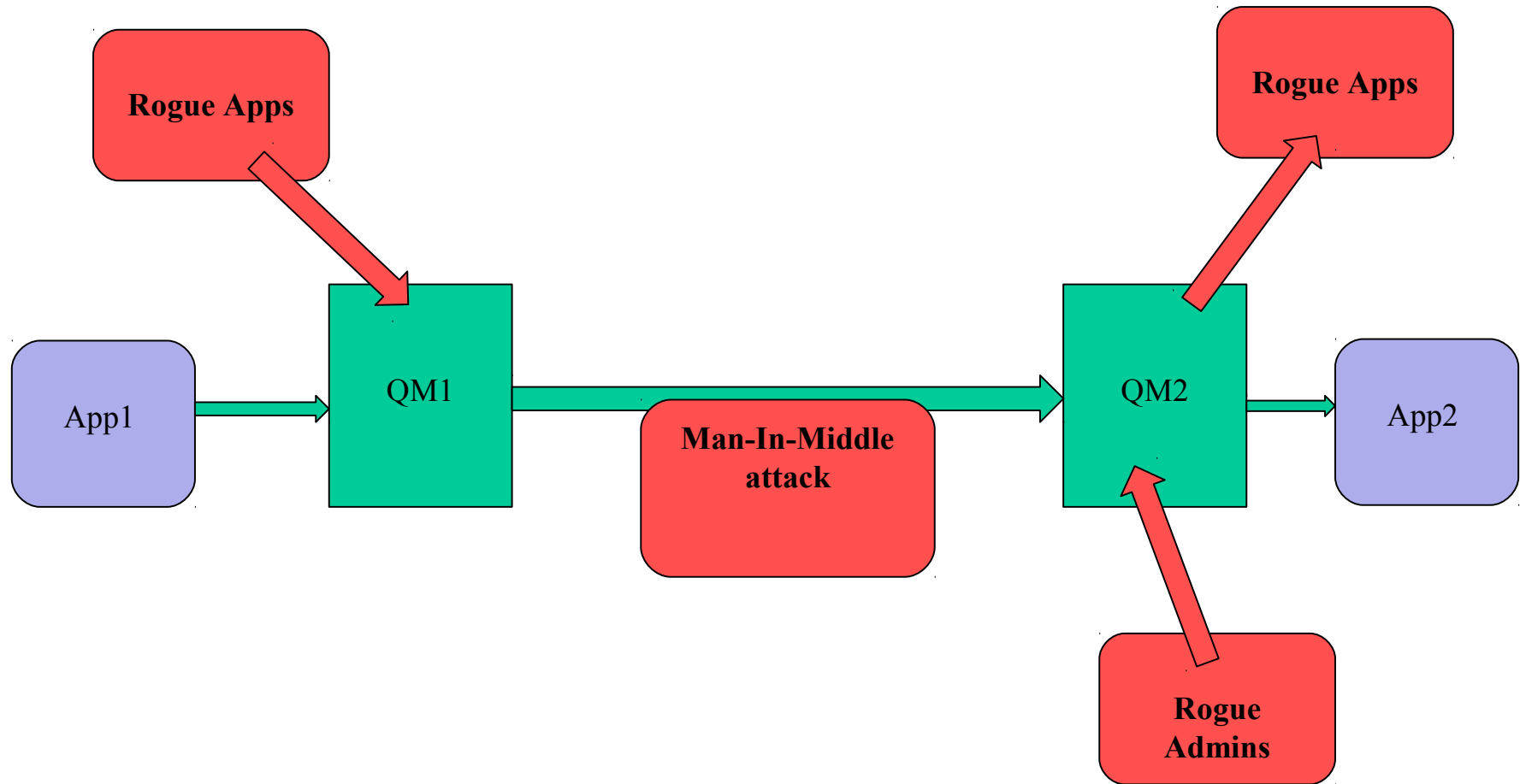
- Loss of customer trust – which results in loss in customers.
- Loss of revenue – because of fines or losing customers.
- Damage to your systems
- Damage to your reputation – new customers may look elsewhere.

■ With movement to cloud security is becoming even more paramount

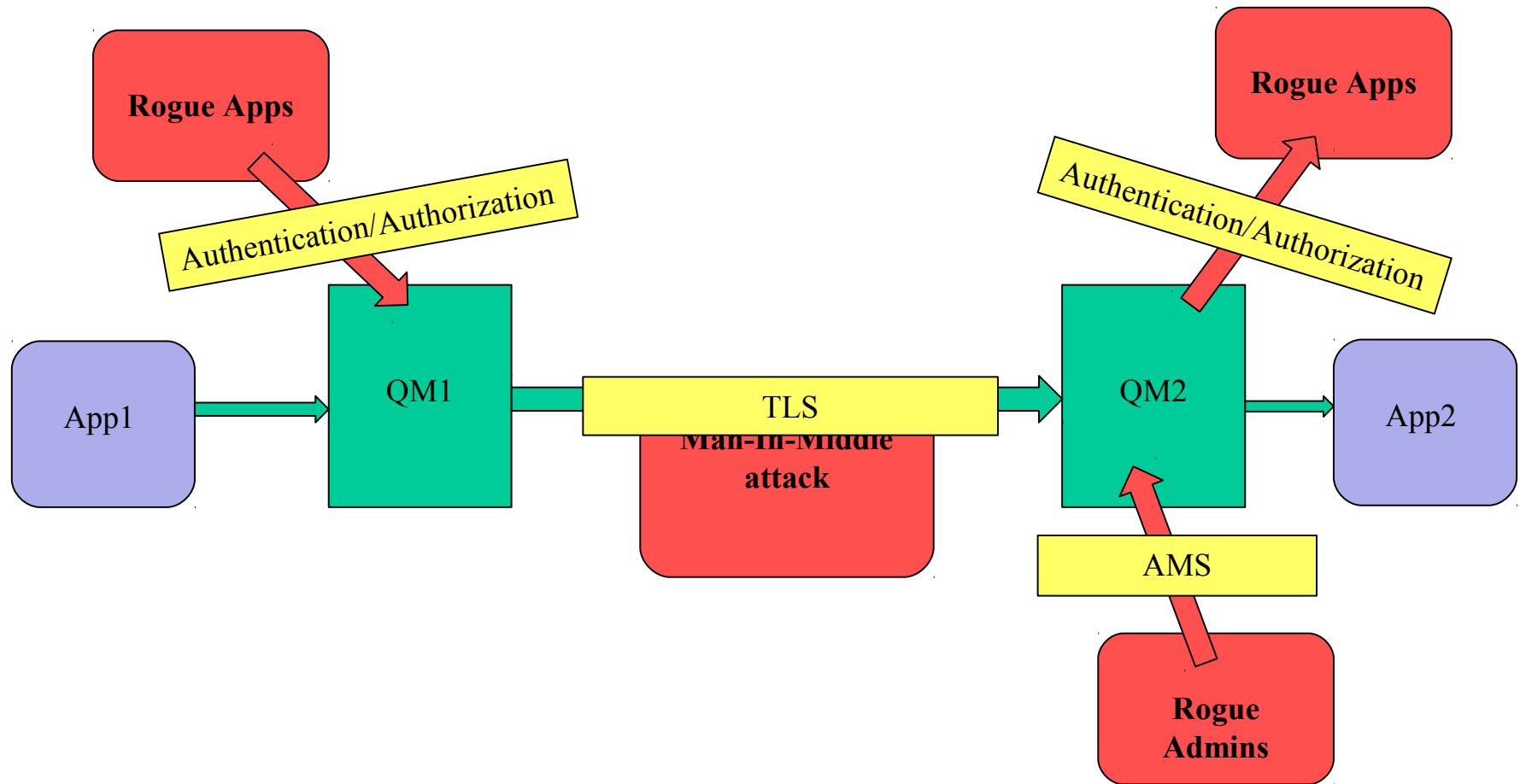
- Data could be anywhere in the world
- Shared data systems
- Connections into your system could come from anywhere.

■ IBM MQ has a large set of feature-rich, secure security systems to meet your operational needs.

Attacks can come from anywhere.



IBM MQ Security can protect you from them



Security Matters

- **IBM MQ's security features can be split into 5 categories:**
 - ▢ Although most features have interactions with multiple categories.
- **Authentication**
 - ▢ Can you prove who you are?
- **Authorization**
 - ▢ What can you do?
- **Encryption**
 - ▢ Sending data securely
- **Integrity**
 - ▢ Sending data unedited
- **Firewall-like**
 - ▢ Filtering connections on certain parameters

IBM MQ Security Features

- Connection Authentication
- Authorization
- TLS
- Advanced Message Security
- Channel Authentication Records
- Security Exits

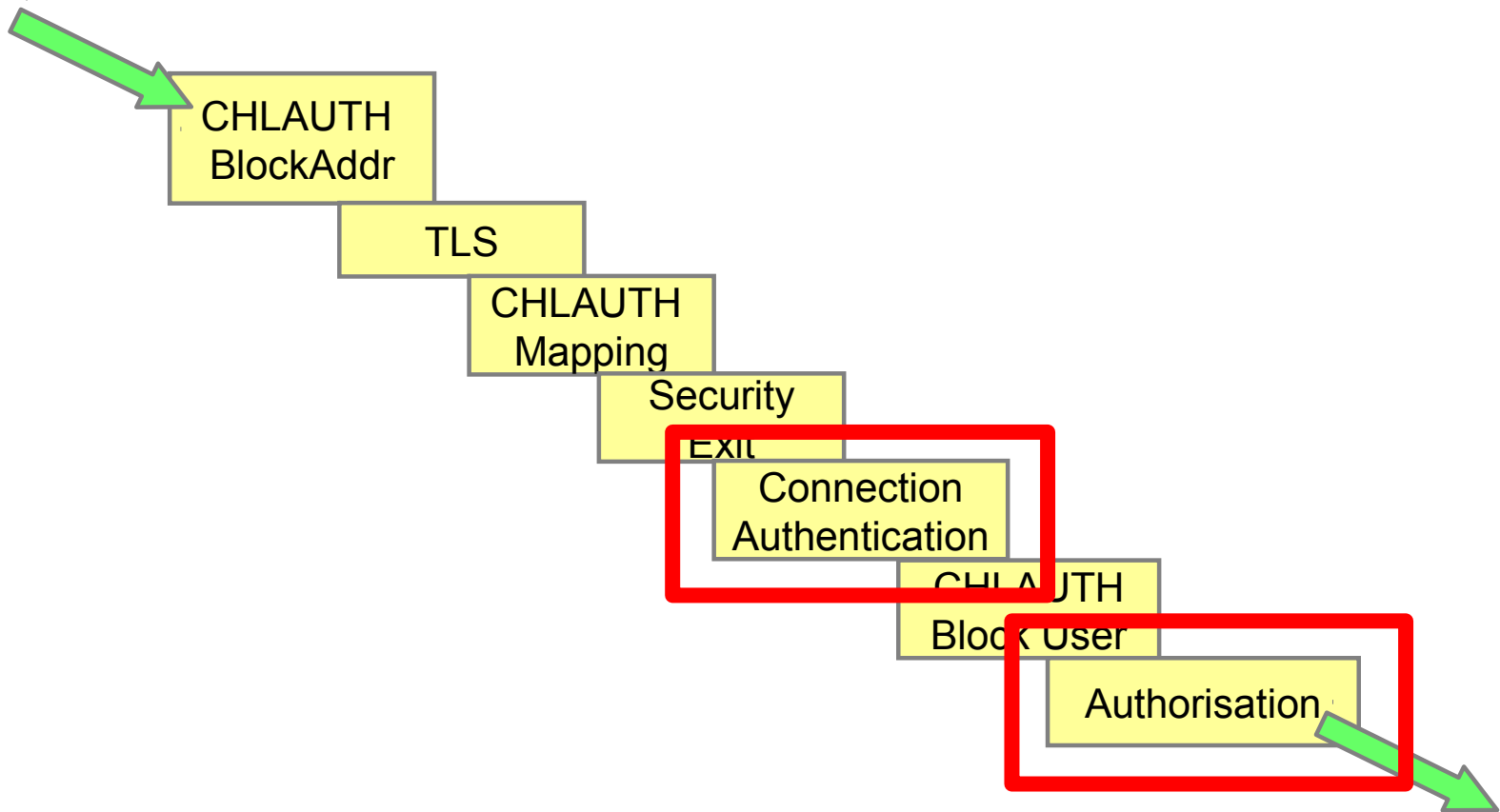
- REST/MQ Console Security

Common Features

- **Security features can be enabled/disabled through configuration**
 - Except Authorization which is always enabled.
- **When a client fails a security check it will receive a 2035 return code**
 - It will not receive any details on what check it failed or why.
 - Administrators can check the queue manager error logs for more details.
- **Security checks are performed in the same order on clients that connect**
 - Both network clients and local binding clients have security checks imposed on them
 - Local bindings only have connection authentication & authorization.
- **Configuration can be done through standard MQ admin interfaces:**
 - MQ Explorer
 - MQSC
 - PCF

Introduction – Security Checks (Client)

- When a user connects via client:



OVERVIEW OF EACH SECURITY FEATURE

Connection Authentication

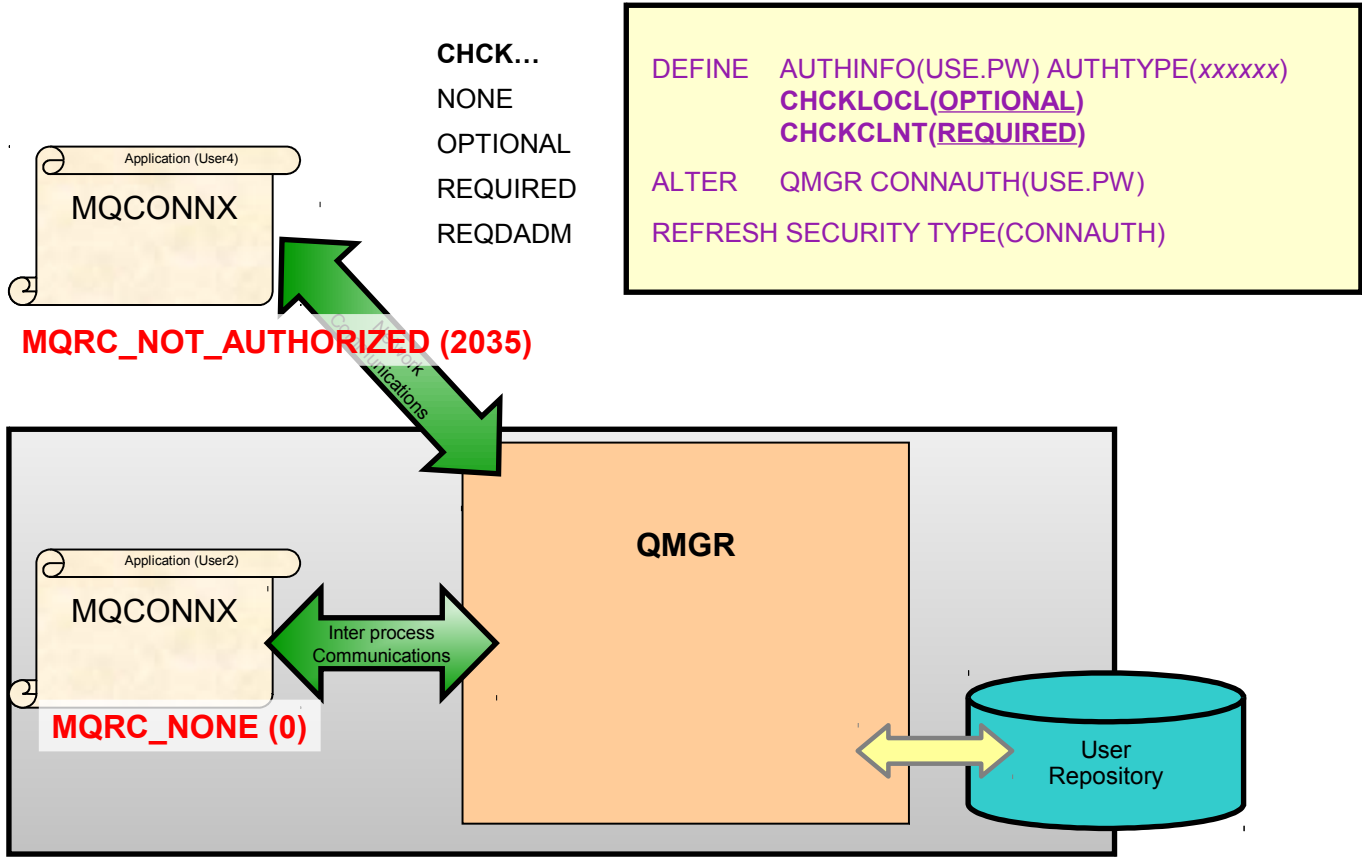
- **Connection authentication feature available in MQ v8 and above.**
 - Allows authentication using user credentials supplied by client applications.
 - User credentials can be local OS users or LDAP users.
 - A failure to authenticate results in a MQRC_NOT_AUTHORIZED 2035 error being returned.

- **User ID can be validated against a number of user repositories**
 - OS
 - LDAP
 - PAM Module

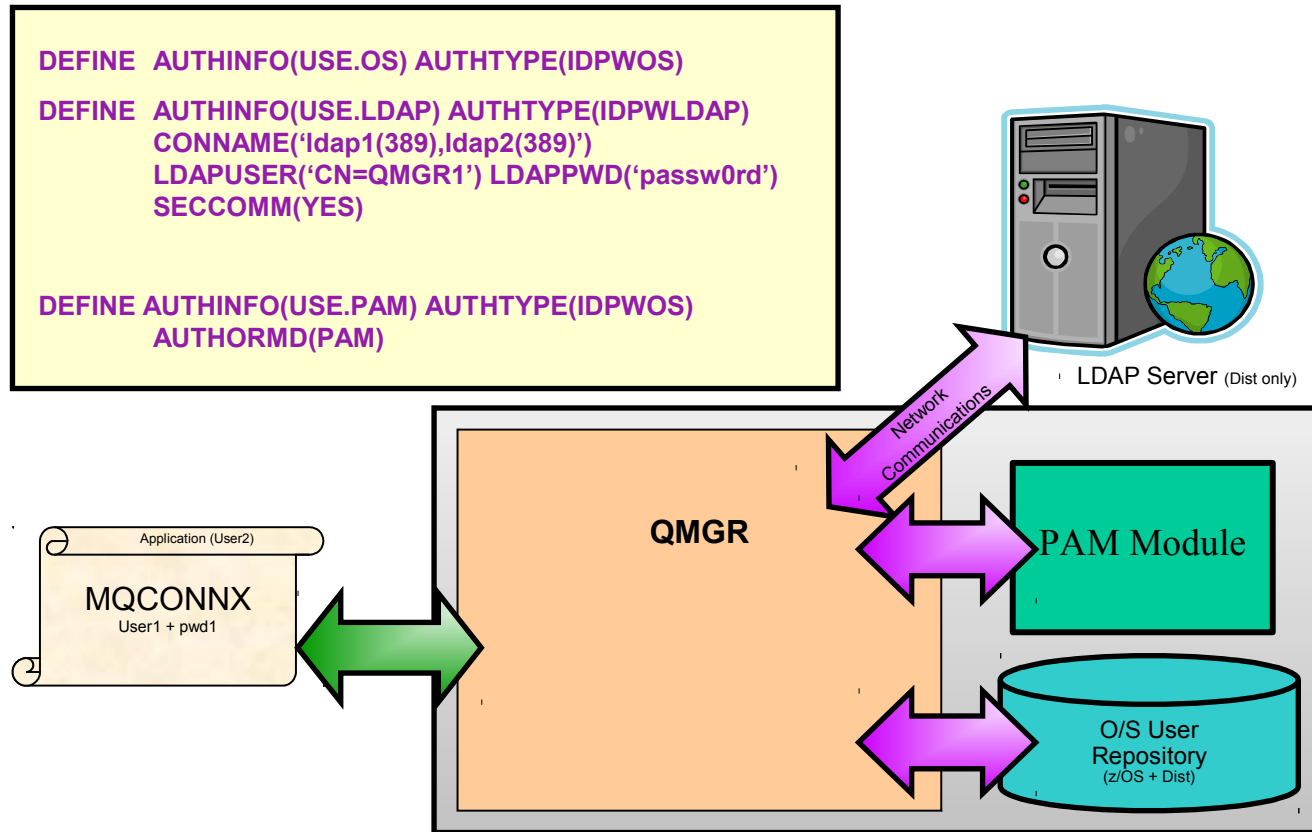
- **IBM MQ sends two different userids in the connection data.**
 - The userid that is running the application.
 - The userid and password that the application wants to authenticate with.

- **Allows granular controls over whether an application *has* to provide valid credentials**

Connection Authentication



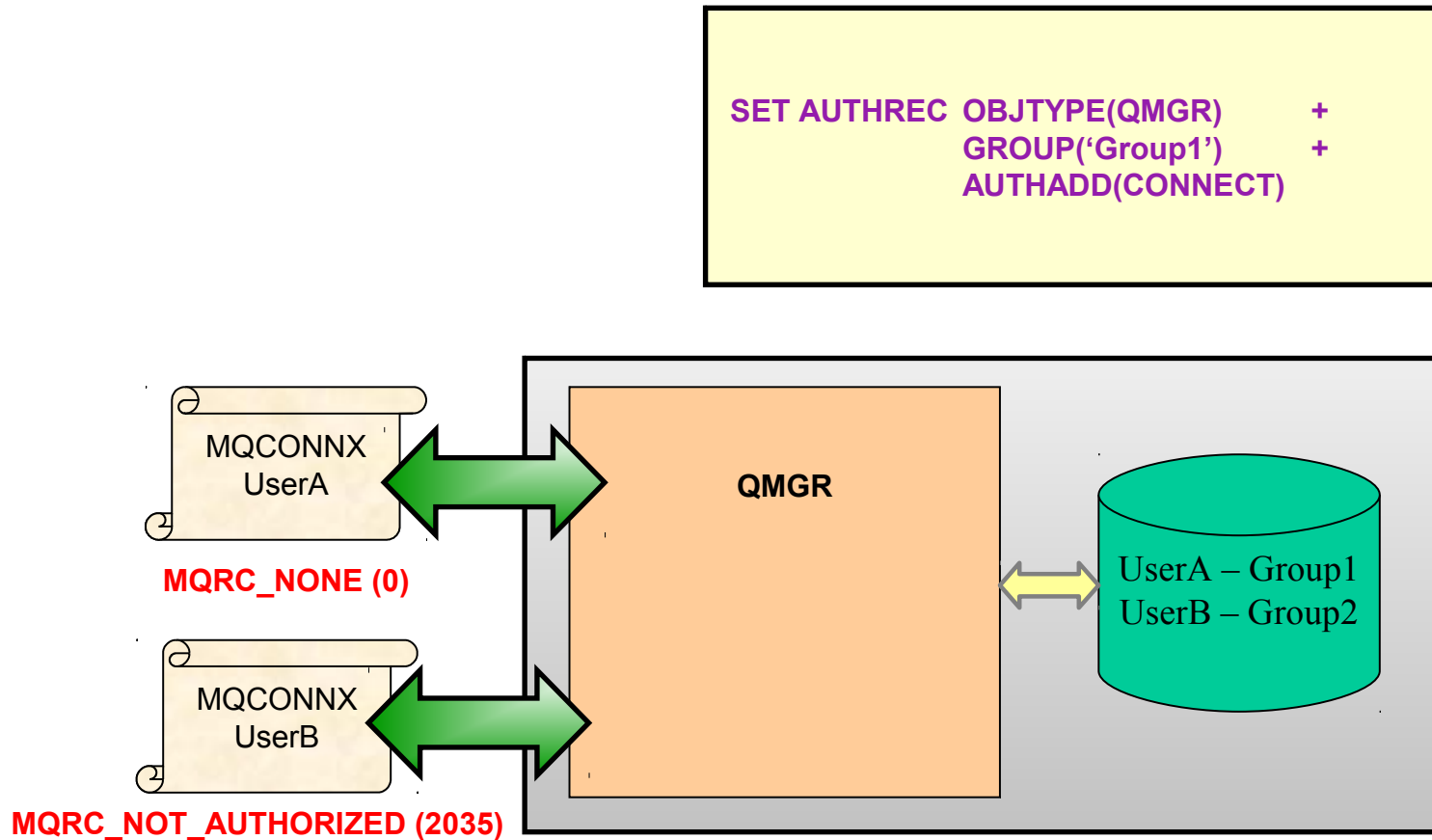
Connection Authentication



Authorization

- **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)**
- **If a user or group does not have authority to do what they are trying to do, they get blocked.**
 - MQRC_NOT_AUTHORIZED (2035)
 - Users who are members of the mqm group have full administrator access.
- **A channel or channel authentication rule can change the userid used for authority checks**
- **MQ Administrators (mqm) has full permissions.**
 - Should rarely allow people to use this userid.

Authorization



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.

TLS

■ IBM MQ's integration of TLS provides the following features:

- Encryption of transmissions between client/queue manager to queue manager.
- Integrity of transmissions between client/queue manager to queue manager.
- [optional] Authentication with a queue manager.

■ Requires Certificates in order to function

- Supports both RSA and ECDSA certificates
- Stored in a keystore,

■ MQ supports a number of TLS providers

- GSKit
- JSSE
- .NET

TLS

- **Certificates are created, stored and managed using tools supplied with IBM MQ**
 - runmqakm
 - runmqckm
 - iKeyman (strmqikm)

- **IBM MQ Channels can only have a single CipherSpec set on them**
 - A CipherSpec is a string which details the hashing and encryption algorithm to use.
 - A list of the cipher strings you can supply are detailed on the knowledge centre.

TLS

- **IBM MQ allows clients to either connect anonymously or with mutual authentication**
 - If a client connects with a certificate then it must be known and trusted by the queue manager.
- **CipherSpec lists are updated when new vulnerabilities arise**
 - In later versions of IBM MQ you may notice the list size changing.
 - We do not delete CipherSpecs, we disable them by default.
- **MQv8 added in multiple certificates feature**
 - Allows you to specify a different certificate to use at the channel level
 - Allows you to specify a certificate to use on the queue manager
 - Before you would be forced to name your certificate `ibmwebspheremq<QM name>`

Channel Authentication Records

- **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)

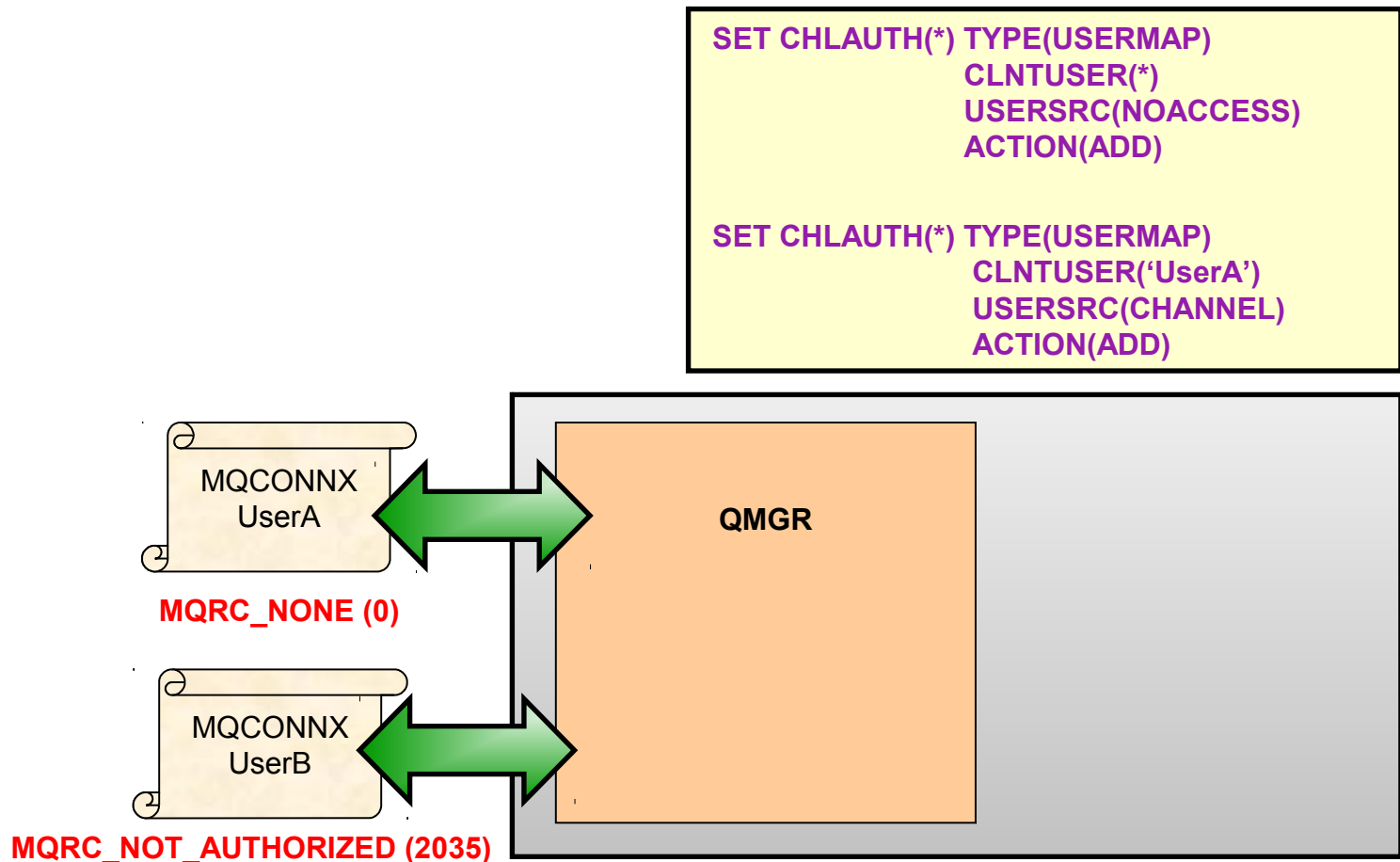
Channel Authentication Records

- **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**

Channel Authentication Records



Security Exits

- **Security exits are bespoke, customer created exits that are ran during the security checking.**
- **MQ comes with an API that can interact with MQ to provide extra control over a connection.**
 - They allow customers to expand MQ's security to suit their needs.
 - For example a customer could write a security exit to only allow connection to a channel during 08:00 to 17:00.
- **Before MQ v8 they could be used to provide connection authentication functionality.**
- **When executed the security exit will have access to the channel definition, information about the incoming connection and information**
 - It will also have a piece of data passed to it that is set on the channel - SCYDATA

Advanced Message Security

- **AMS stands for Advanced Message Security**
 - It is message level security
 - It is a separate licensable feature - included in MQ Advanced

- **AMS is an end-to-end security model, messages stay signed/encrypted through the whole lifetime of a message**
 - In transit
 - At rest

- **With AMS you can create policies for a queue that describe how messages should be protected when applications put or get messages using that queue name.**
 - Signing
 - Encryption
 - Both

Details

- **AMS does not perform any access control:**
 - Only privacy and integrity protection
 - Should be used with existing access control, authentication, etc
- **Encryption level protection prevents unauthorised users reading message data.**
 - Including MQ administrators.
- **Signing protection prevents messages from being altered.**
- **Signing & Encryption use certificates – Same as TLS.**
- **No application code changes required to use AMS.**

Configuration

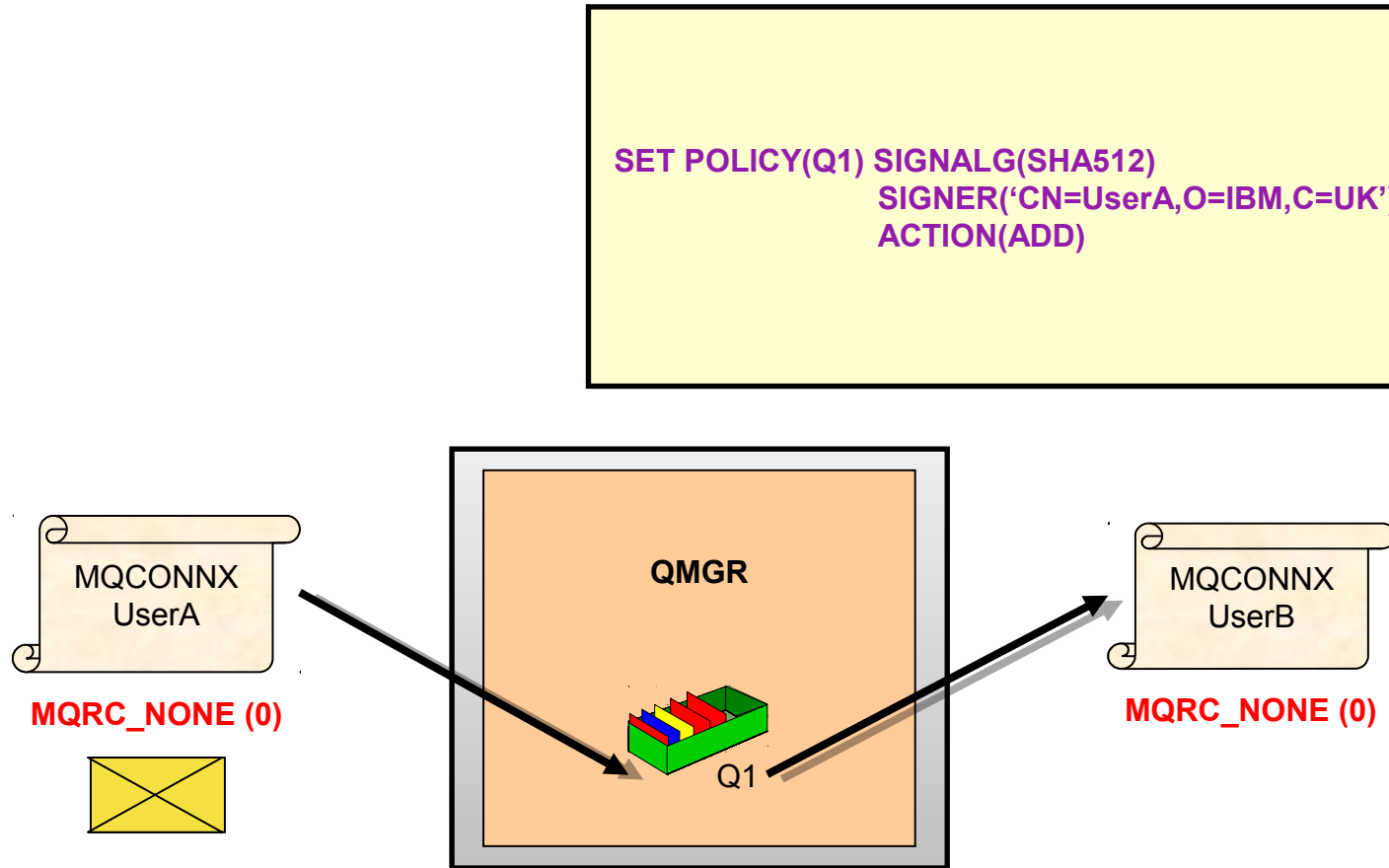
■ Differences between AMS & TLS configuration

- Both sides must have a certificate
- Both sides must have exchanged the public certificate
- The full certificate chain must be present in the key store

■ Policies can be created in explorer, runmqsc or using setmqspl

- `setmqspl -m <QM name> -p <Q Name> -s <Signing algorithm>
-a <Authorised signers> -e <Encryption algorithm> -r <Recipients>`
- `SET POLICY(<Q NAME>) SIGNALG(<Signing algorithm>)
ENCALG(<Encryption algorithm>) SIGNER(<Authorised signers>)
RECIP(<Recipients>) ACTION(ADD|REPLACE|REMOVE)`

Configuration



REST/MQ Console Security

■ Role based access control. Need to be a member of at least one role

- MQWebAdmin
- MQWebAdminRO
- MQWebUser
- MFTWebAdmin
- MFTWebAdminRO

■ User and groups defined in a registry

- Basic
- LDAP
- SAF (on z/OS)
- OS (on distributed)

■ REST is locked down by default, need to do some configuring

- Samples provided to make this simpler

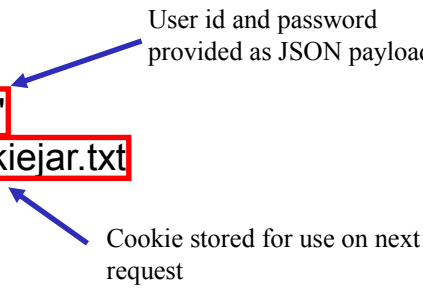
```
<!--  
Roles for the MQ REST API  
-->  
<enterpriseApplication id="com.ibm.mq.rest">  
  <application-bnd>  
    <security-role name="MQWebAdmin">  
      <group name="MQWebAdminGroup" realm="defaultRealm"/>  
    </security-role>  
    <security-role name="MQWebAdminRO">  
      <user name="mqreader" realm="defaultRealm"/>  
    </security-role>  
    <security-role name="MQWebUser">  
      <special-subject type="ALL_AUTHENTICATED_USERS"/>  
    </security-role>  
    <security-role name="MFTWebAdmin">  
      <user name="mftadmin" realm="defaultRealm"/>  
    </security-role>  
    <security-role name="MFTWebAdminRO">  
      <user name="mftreader" realm="defaultRealm"/>  
    </security-role>  
  </application-bnd>  
</enterpriseApplication>  
  
<!-- Sample Basic Registry -->  
<basicRegistry id="basic" realm="defaultRealm">  
  <!-- This sample defines two users with unencoded passwords -->  
  <!-- and a group, these are used by the role mappings above -->  
  <user name="mqadmin" password="mqadmin"/>  
  <user name="mqreader" password="mqreader"/>  
  <group name="MQWebUI">  
    <member name="mqadmin"/>  
  </group>  
</basicRegistry>  
  
<!-- Example LDAP Registry -->  
<ldapRegistry id="ldap">  
  realm="MyOrganizationRealm"  
  host="sso.example.com"  
  port="389"  
  ignoreCase="true"  
  baseDN="o=example.com"  
  certificateMapMode="EXACT_DN"  
  ldapType="IBM Tivoli Directory Server"  
  idsFilters="ibm_dir_server">  
</ldapRegistry>
```

REST Security

■ Token based

- User logs in once with user id and password and then gets a cookie which is used for subsequent requests

```
curl -k -X POST -H "Content-Type: application/json"  
-d "{\"username\":\"mqadmin\",\"password\":\"mqadmin\"}"  
https://localhost:9443/ibmmq/rest/v1/login -c c:\temp\cookiejar.txt
```



- DELETE to the login URL logs out

■ Or HTTP basic authentication

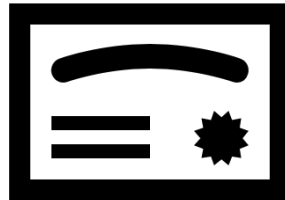
- User id and password provided as an encoded header, must be set for each request

```
C:\>curl -k https://localhost:9443/ibmmq/rest/v1/admin/installation -u mqadmin:mqadmin  
{  
  "installation": [{  
    "name": "MQ905",  
    "platform": "windows",  
    "version": "9.0.5.0"  
  }]  
}
```

RESTSecurity

■ Or use a client certificate

- Must be provided with each call to the REST API
- Distinguished name from certificate is mapped to user in configured user registry



Interactions between features

- Every security feature of MQ interacts with each other (except AMS and TLS)
- Channel authentication rules, Connection authentication & Security exits can change the userid used for authorization checks
- Connection authentication can change the userid which is tested during channel authentication rules.
- To effectively design your security you must consider all security features.

Where can I get more information?

IBM Messaging developerWorks
developer.ibm.com/messaging

IBM Messaging Youtube
[https:// ibm.biz/MQplaylist](https://ibm.biz/MQplaylist)

LinkedIn
<https://ibm.biz/ibmmessaging>

Blog posts
tagged with
“cloud”



Questions & Answers



Notices and disclaimers

Copyright© 2017 by International Business Machines Corporation (IBM). No part of this document may be reproduced or transmitted in any form without written permission from IBM.

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.