Click to add text

MQ Security Overview

Robert Parker
parrobe@uk.ibm.com

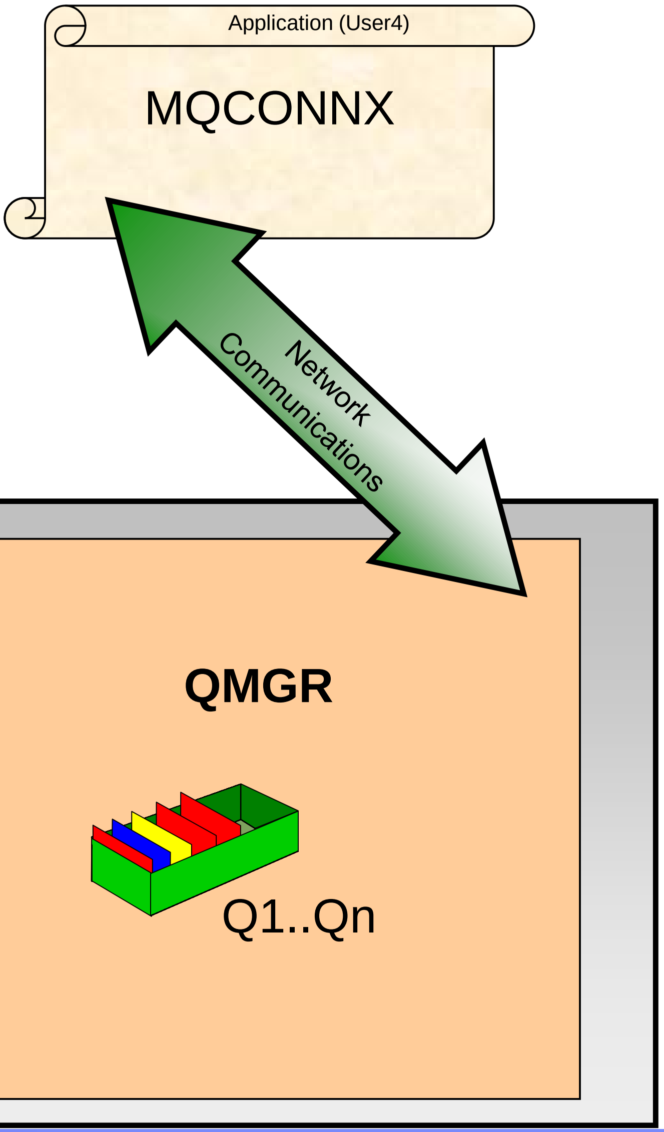
Agenda

- Introduction
- Connection Authentication
- Authorization
- SSL/TLS on a channel
- Channel Authentication
- Security Exits
- AMS

Introduction – Typical MQ

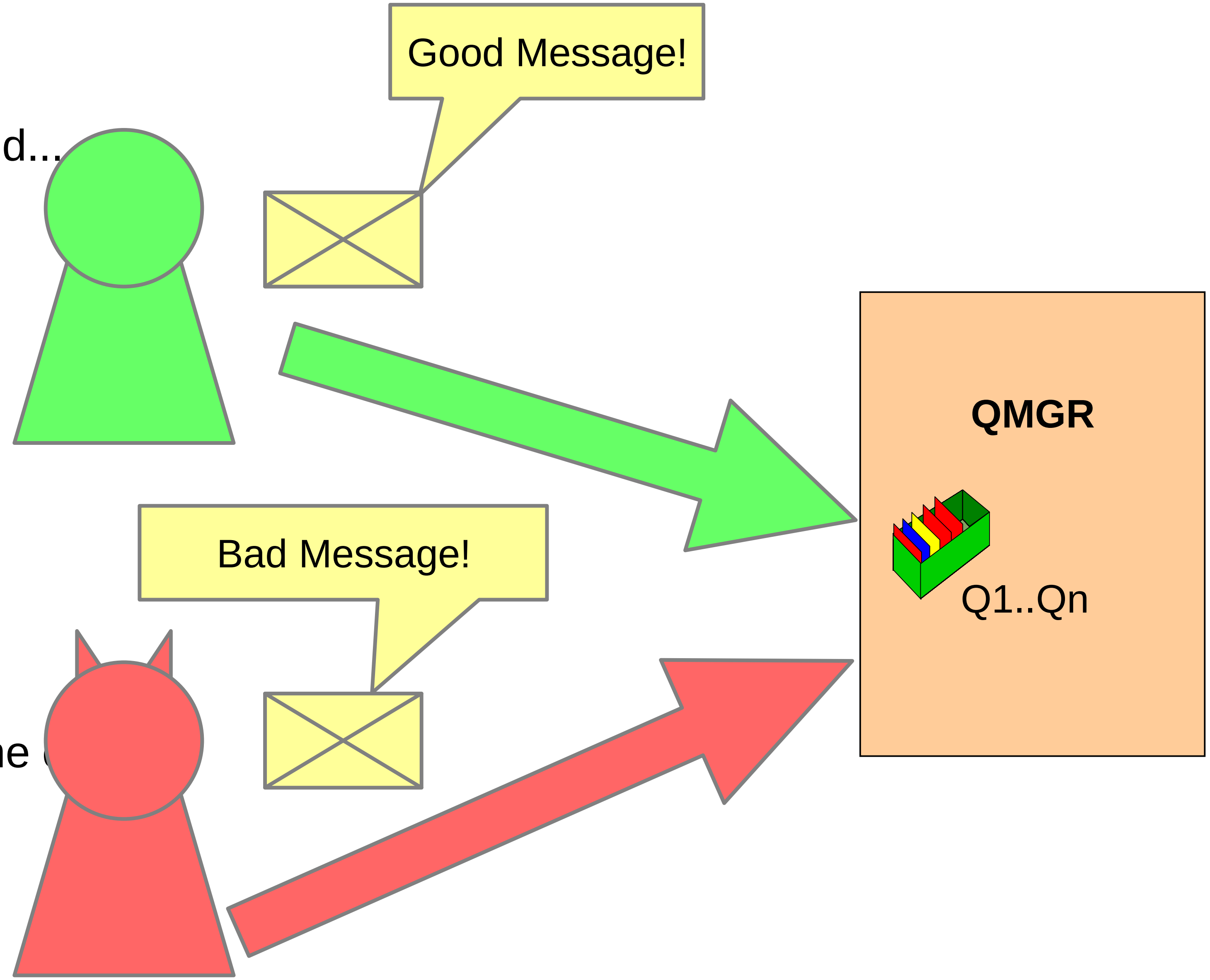
In a Typical MQ setup there is:
- A Queue Manager (QMGR)
- A number of Queues
- Applications that connect to the QMGR via:
- Local Bindings
- Client connections

- Configuration is updated via Command line or Explorer



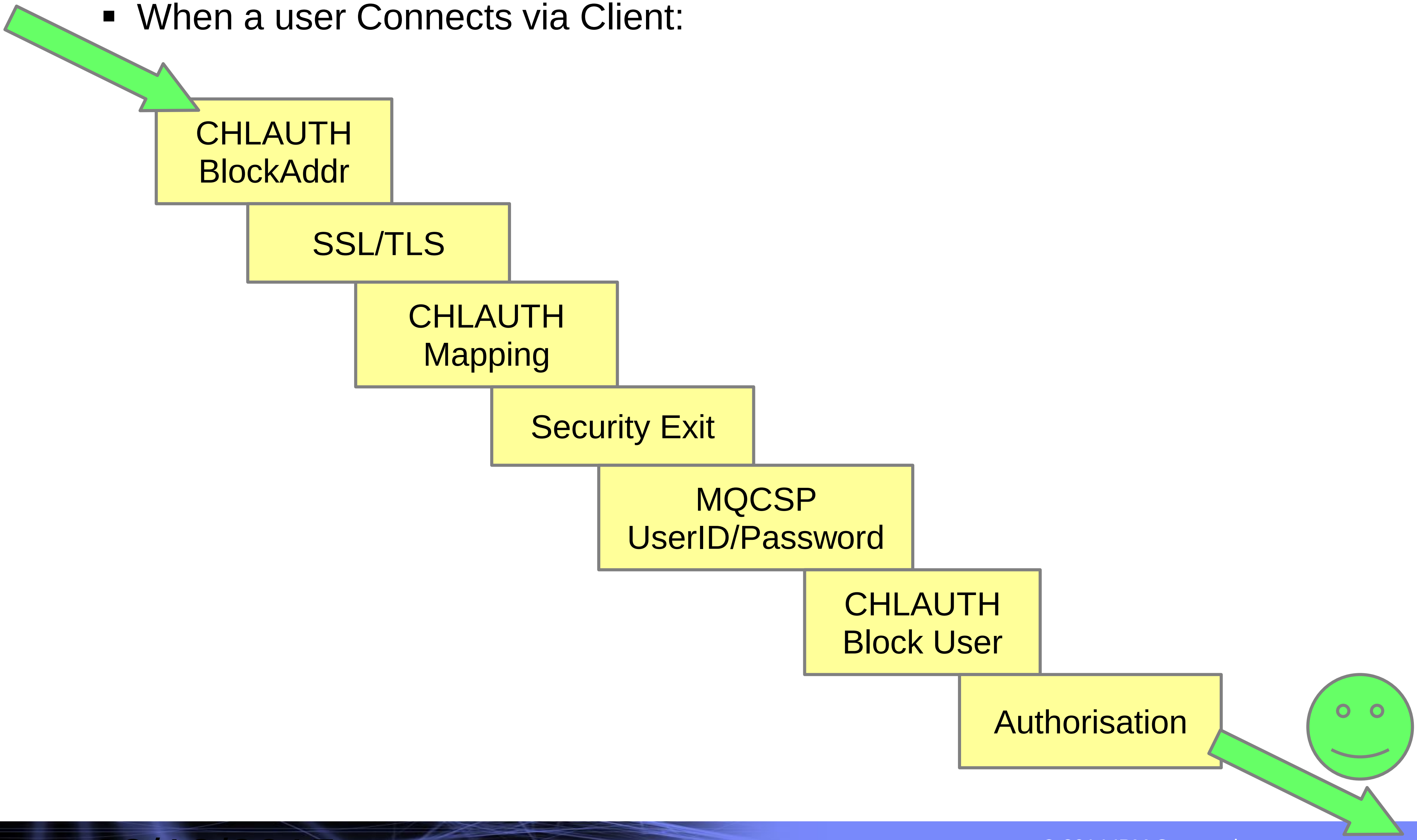
Introduction – Use case

- In a perfect world...
- ...but this isn't the



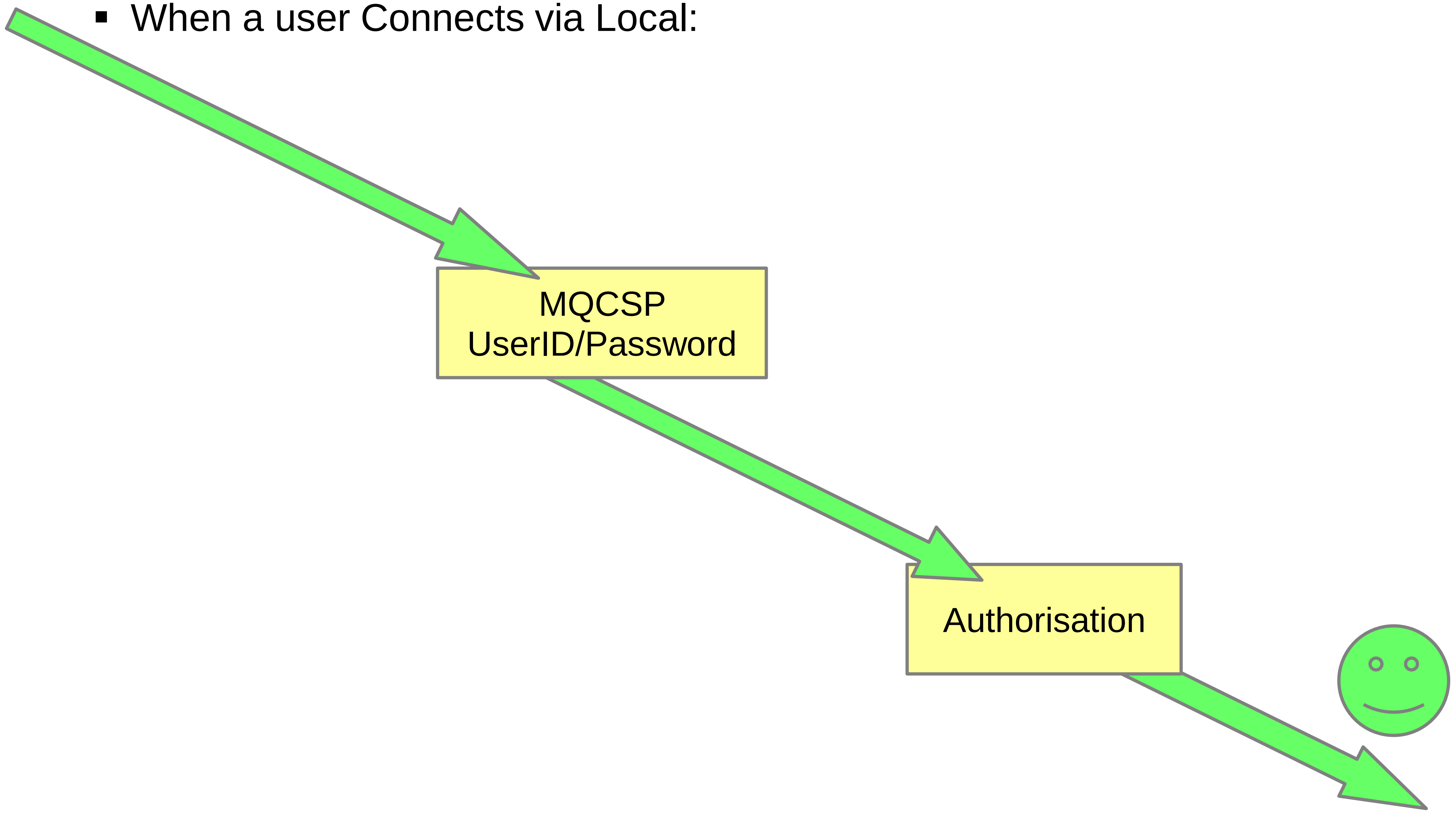
Introduction – Security Checks (Client)

- When a user Connects via Client:



Introduction - Security Checks (Local)

- When a user Connects via Local:

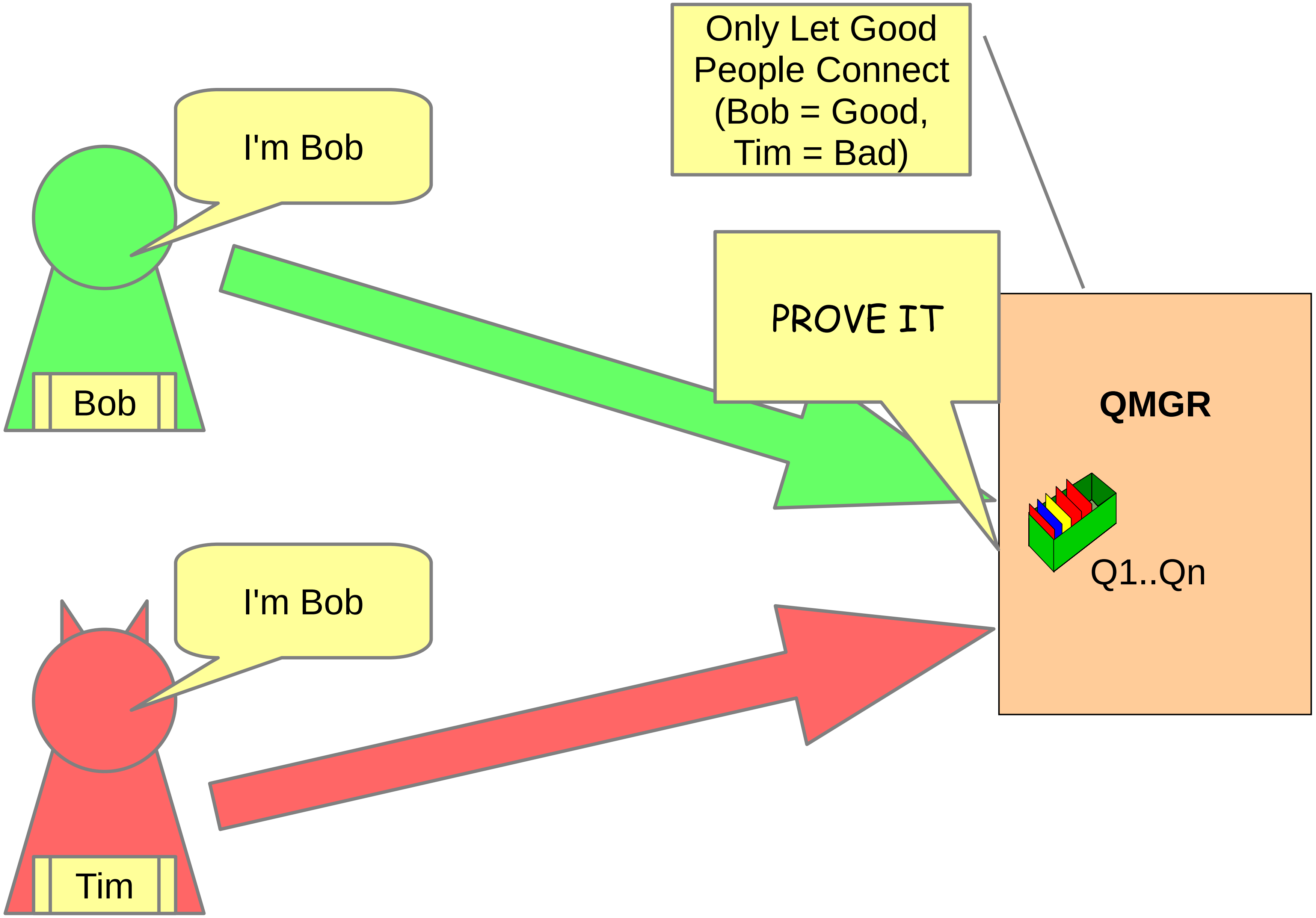


Authentication

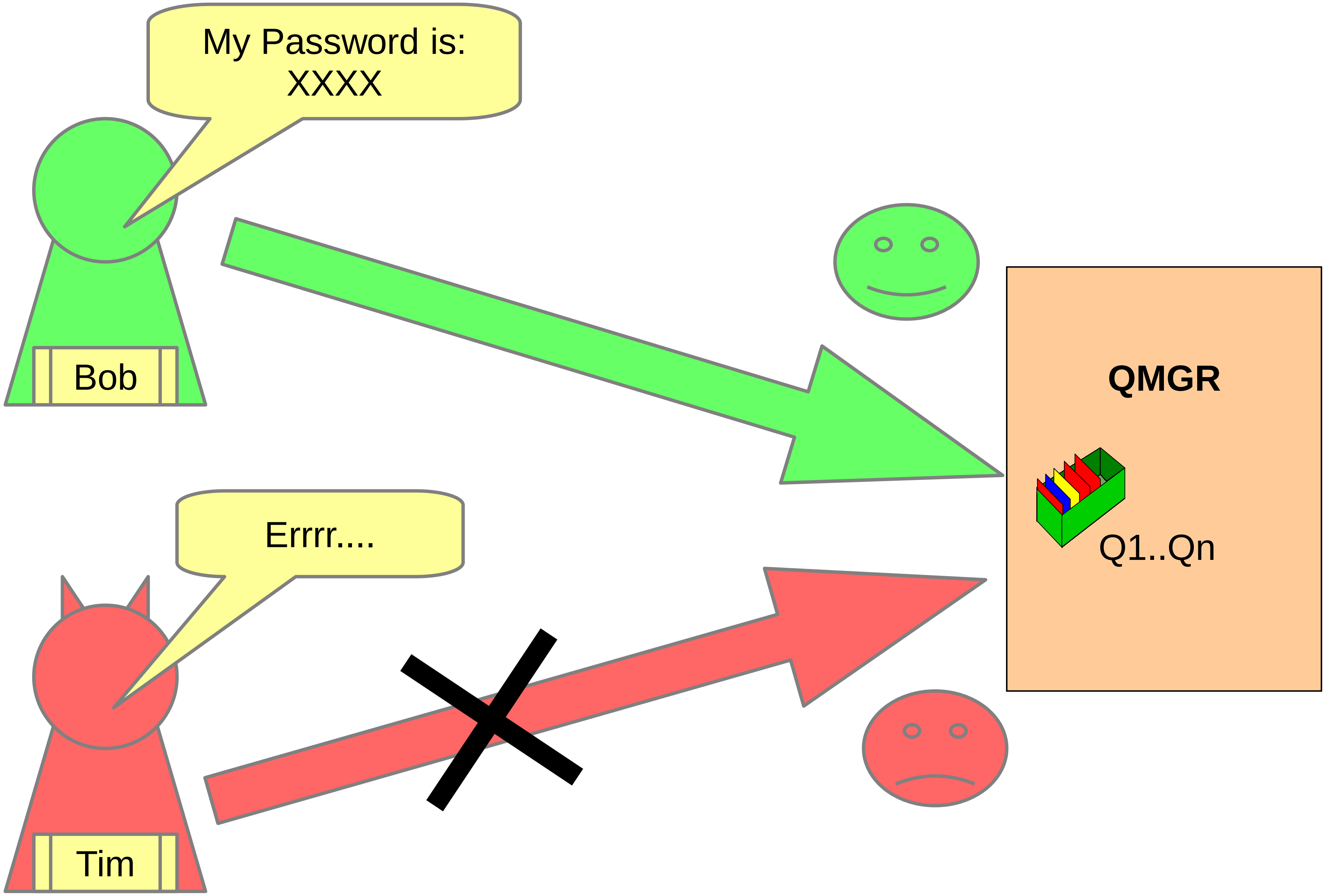
Connection Authentication – Use case

- 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.
- A failure to authenticate results in an error being returned. RC=2035

Connection Authentication – Use Case



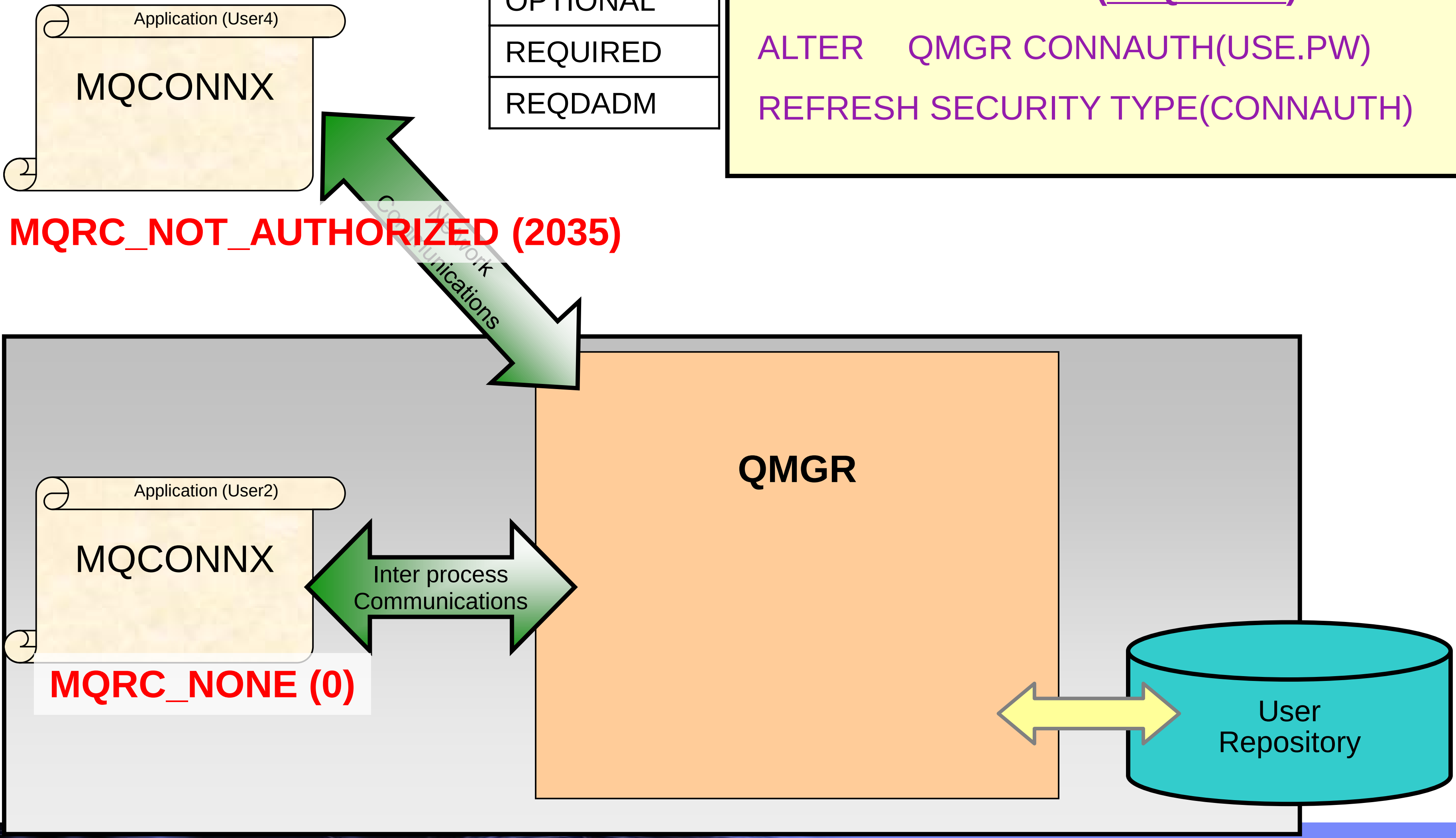
Connection Authentication – Use Case



Connection Authentication – Setting up and it's purpose

CHCK…
NONE
OPTIONAL
REQUIRED
REQDADM

```
DEFINE   AUTHINFO(USE.PW) AUTHTYPE(xxxxxx)
         CHCKLOCL(OPTIONAL)
         CHCKCLNT(REQUIRED)
ALTER    QMGR CONNAUTH(USE.PW)
REFRESH SECURITY TYPE(CONNAUTH)
```

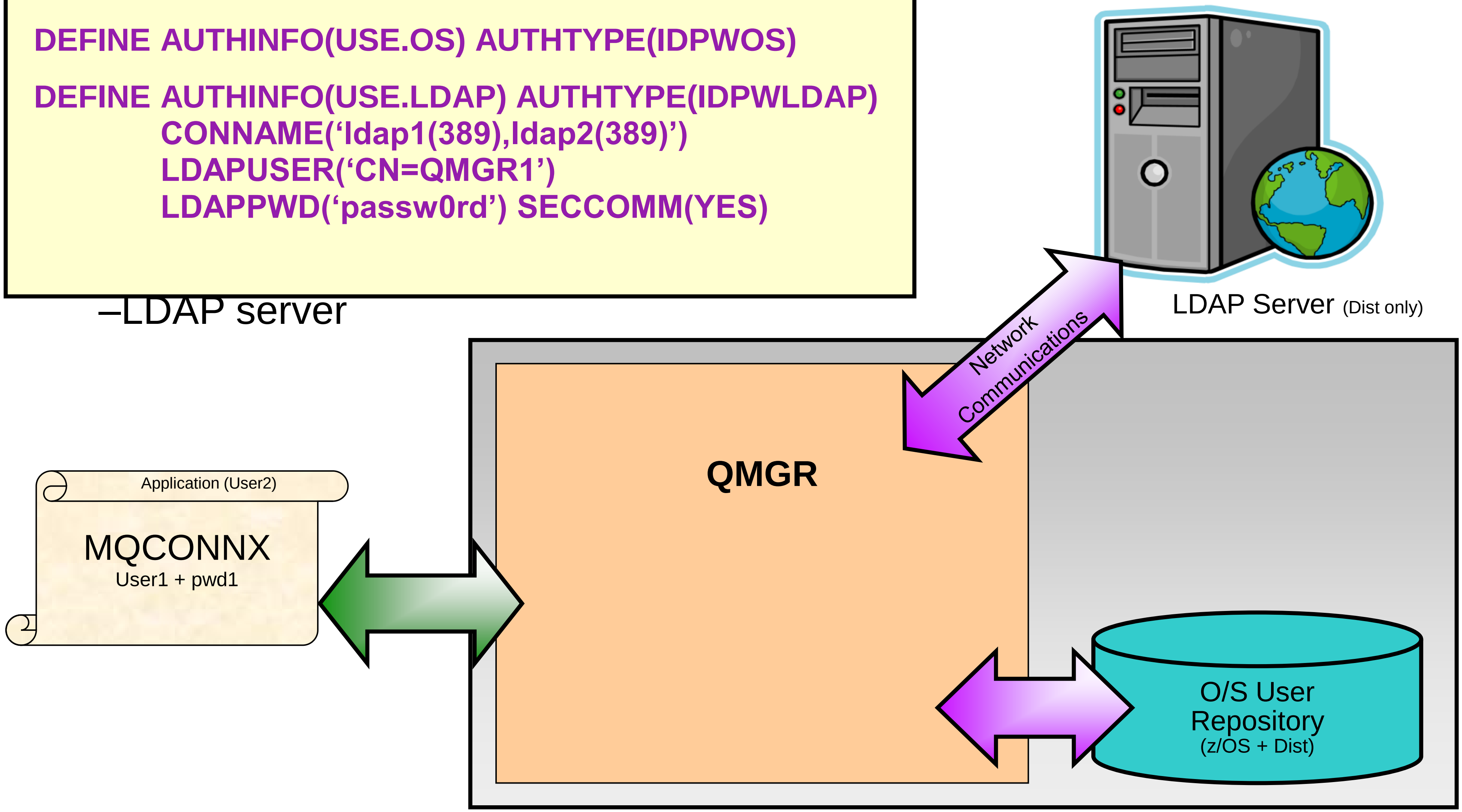


Connection Authentication – User repositories

```
DEFINE AUTHINFO(USE.OS) AUTHTYPE(IDPWOS)

DEFINE AUTHINFO(USE.LDAP) AUTHTYPE(IDPWLDAP)
       CONNAME('ldap1(389),ldap2(389)')
       LDAPUSER('CN=QMGR1')
       LDAPPWD('passw0rd') SECCOMM(YES)
```

–LDAP server

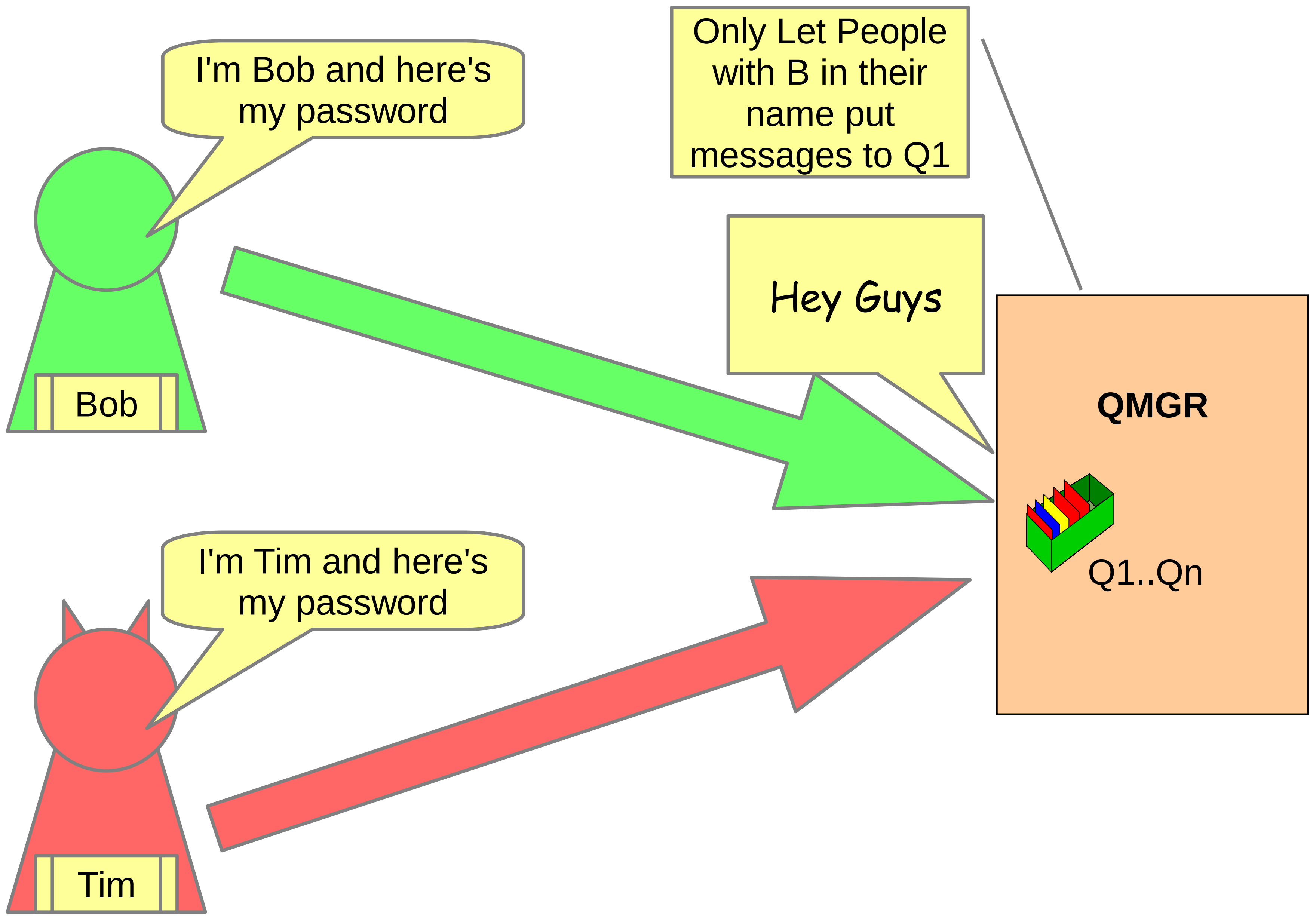


Authorization

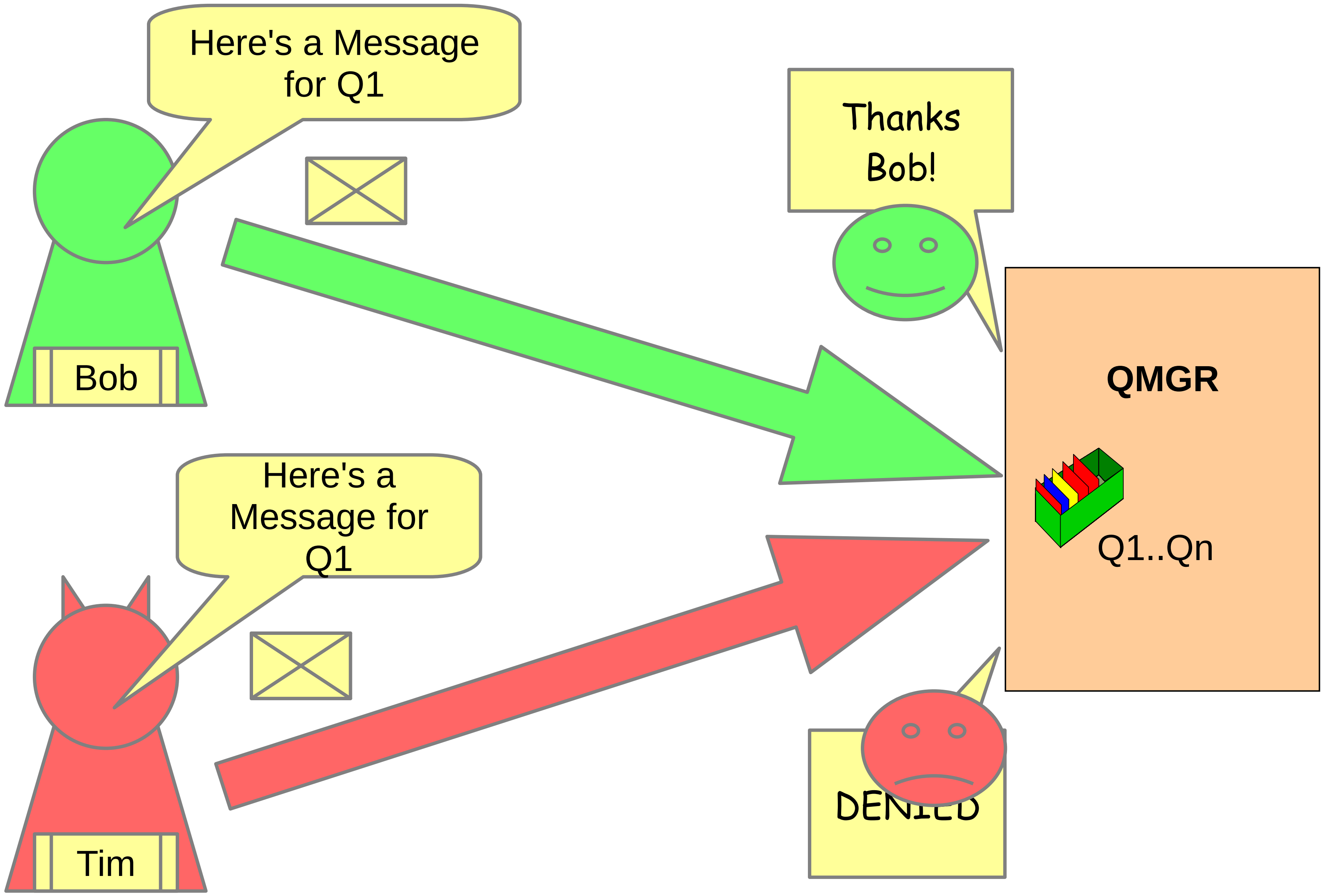
Authorization – Use Case

- We use Authorization to limit what connected users can and cannot do.
- We assign authority rules to a specific user or group.
- If a user or group does not have authority to do what they are trying to do, they get blocked.

Authorization – Use Case

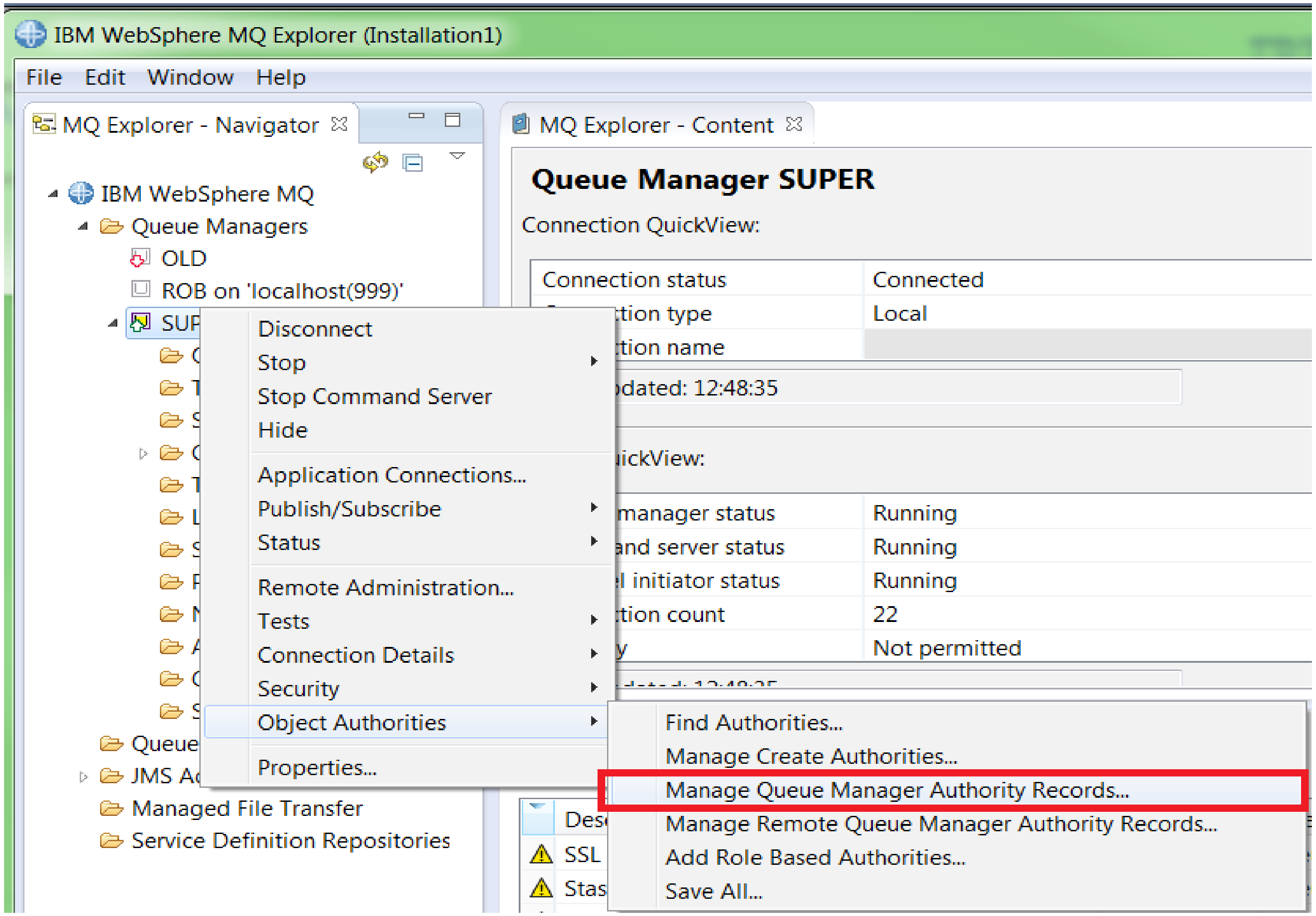

I'm Bob and here's my password
Only Let People with B in their name put messages to Q1
Hey Guys
Bob
QMGR
Q1..Qn
I'm Tim and here's my password
Tim

Authorization – Use Case



Authorization – MQ Explorer

- Right click on the QMGR or object to edit authorities for (For Example: Queue)



IBM WebSphere MQ Explorer (Installation1)

File Edit Window Help

MQ Explorer - Navigator

- IBM WebSphere MQ
  - Queue Managers
    - OLD
    - ROB on 'localhost(999)'
    - SUP
  - Queue
  - JMS A
  - Managed File Transfer
  - Service Definition Repositories

MQ Explorer - Content

Queue Manager SUPER

Connection QuickView:

Connection status	Connected
...tion type	Local
...tion name	

...dated: 12:48:35

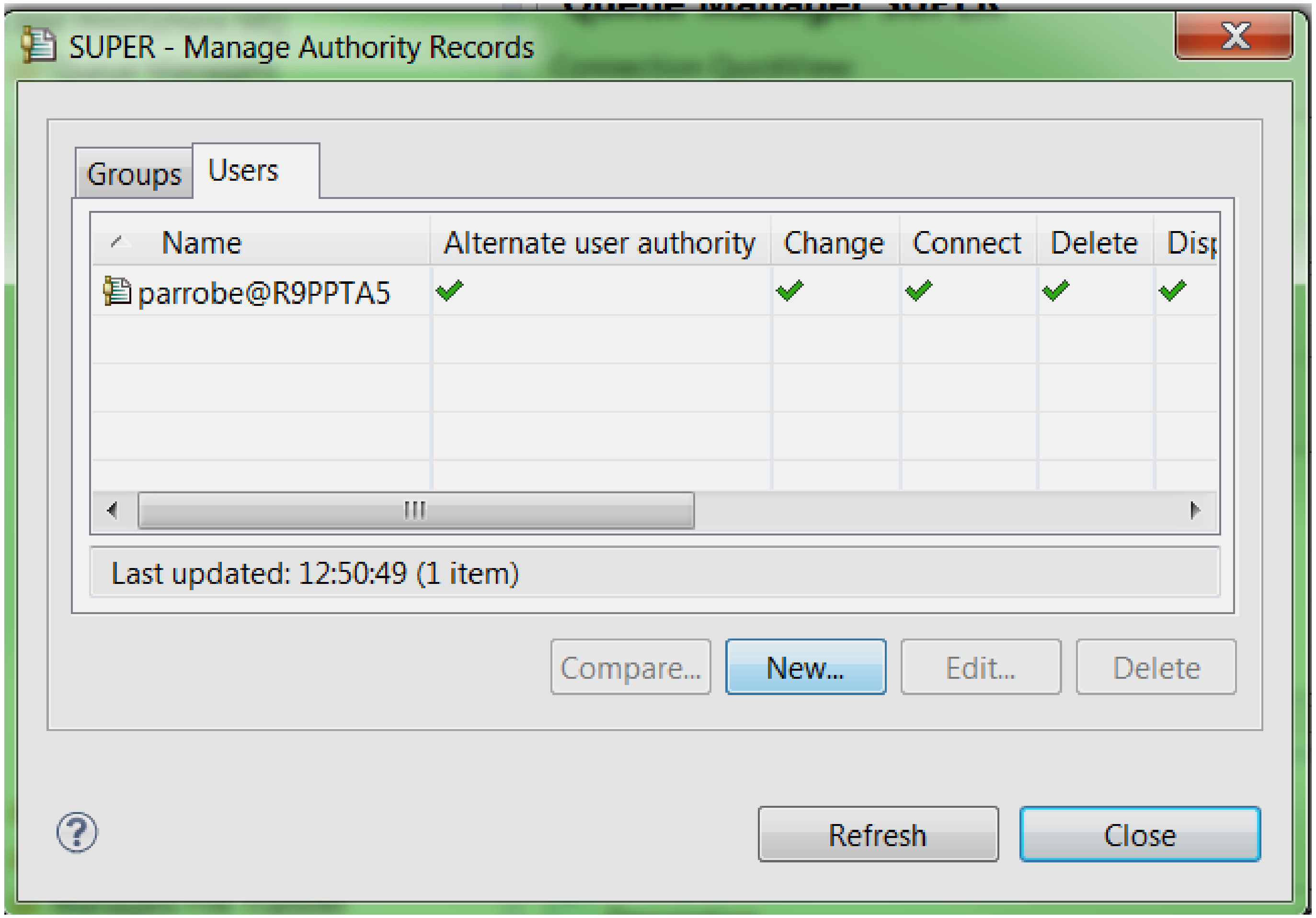
...ickView:

...manager status	Running
...and server status	Running
...l initiator status	Running
...tion count	22
...y	Not permitted

Desc
SSL
Stas

Authorization – MQ Explorer

- Choose the Groups or Users tab depending on which you are editing:
- Select New or an edit an existing



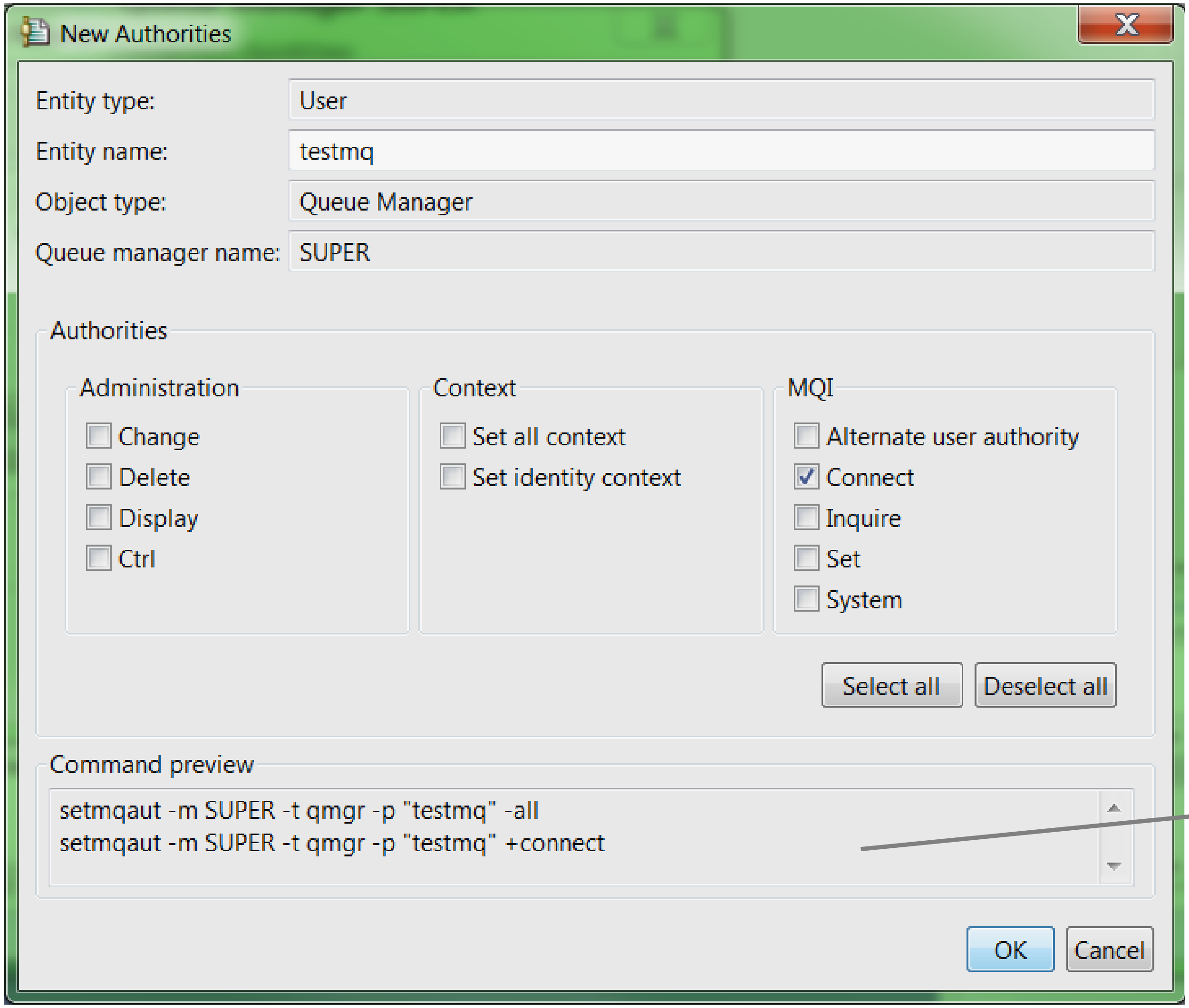
SUPER - Manage Authority Records

Name	Alternate user authority	Change	Connect	Delete	Disp
parrobe@R9PPTA5	✓	✓	✓	✓	✓

Last updated: 12:50:49 (1 item)

Authorization – MQ Explorer

- Select the authorities to give the user or group and click OK.



Entity type:	User
Entity name:	testmq
Object type:	Queue Manager
Queue manager name:	SUPER

Authorities

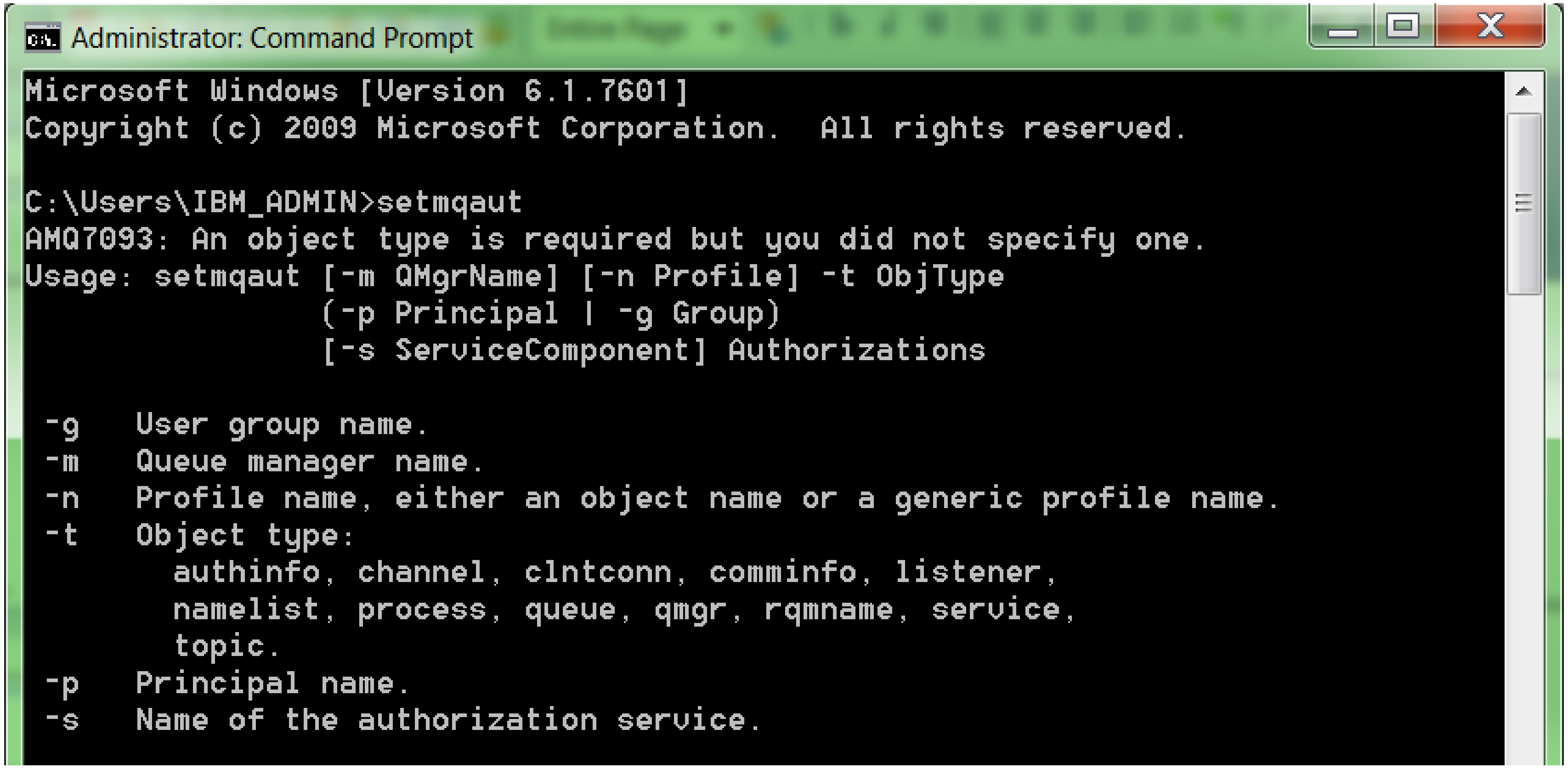
Administration	Context	MQI
☐ Change	☐ Set all context	☐ Alternate user authority
☐ Delete	☐ Set identity context	✓ Connect
☐ Display		☐ Inquire
☐ Ctrl		☐ Set
		☐ System

Command preview

```
setmqaut -m SUPER -t qmgr -p "testmq" -all
setmqaut -m SUPER -t qmgr -p "testmq" +connect
```

Example **setmqaut** commands here

Authorization – Command Line

- 

Administrator: Command Prompt

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IBM_ADMIN>setmqaut
AMQ7093: An object type is required but you did not specify one.
Usage: setmqaut [-m QMgrName] [-n Profile] -t ObjType
                (-p Principal | -g Group)
                [-s ServiceComponent] Authorizations

 -g    User group name.
 -m    Queue manager name.
 -n    Profile name, either an object name or a generic profile name.
 -t    Object type:
         authinfo, channel, clntconn, comminfo, listener,
         namelist, process, queue, qmgr, rqmname, service,
         topic.
 -p    Principal name.
 -s    Name of the authorization service.
```

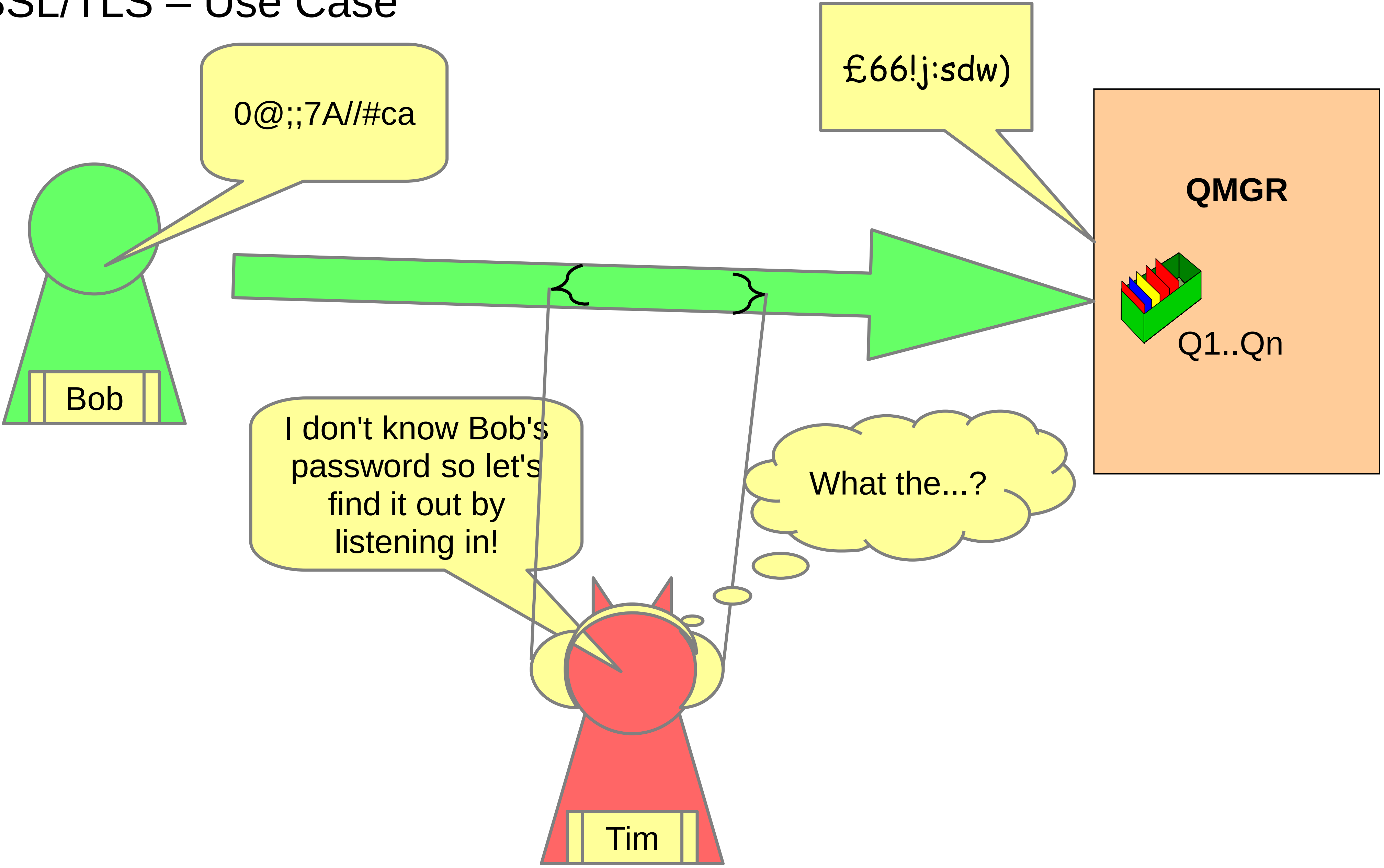
SSL/TLS

SSL/TLS – Use Case

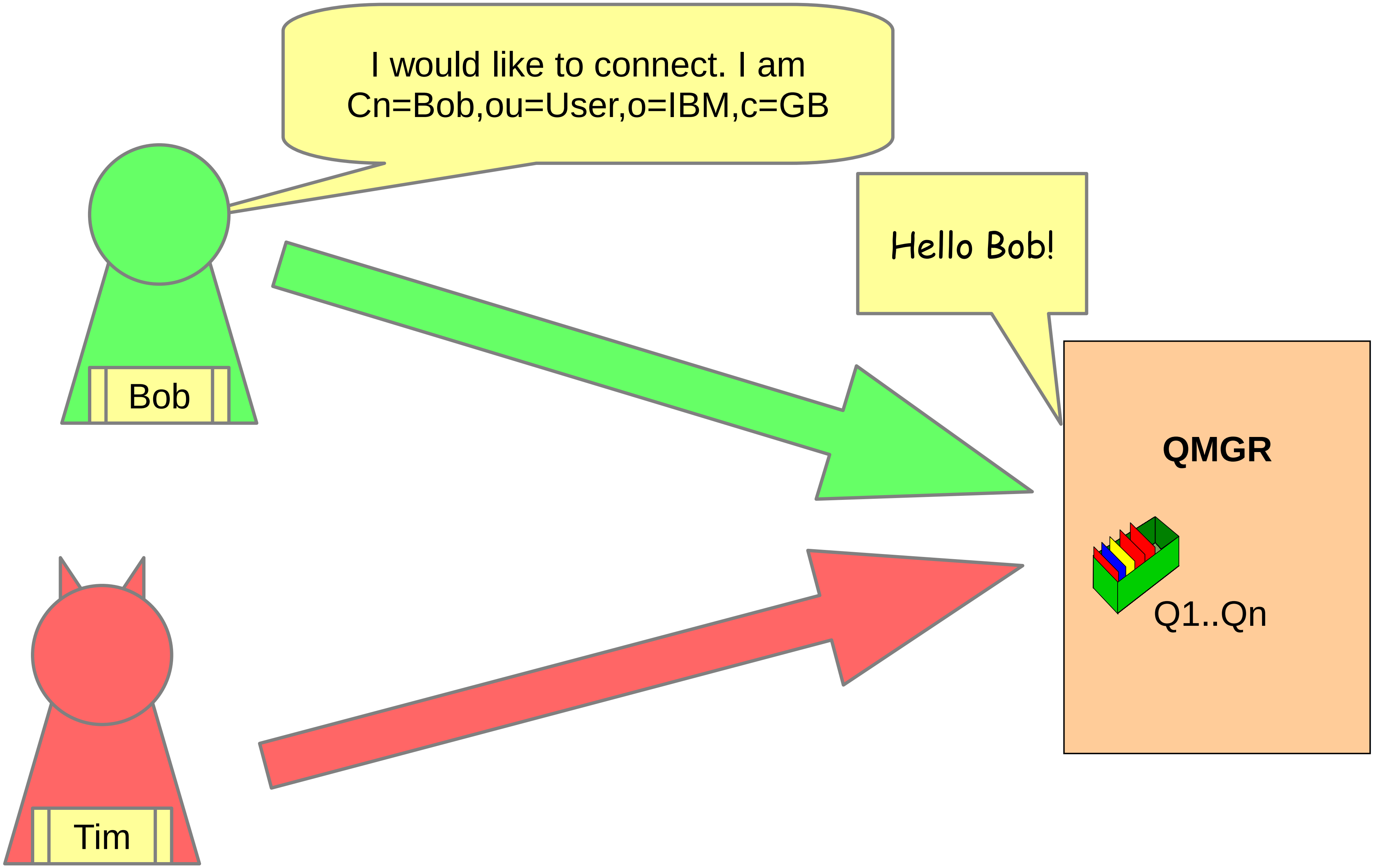
- There are two reasons to use SSL/TLS with MQ.
  - Encryption of transmissions between Client/QMGR to QMGR
  - Authentication with a QMGR.

- SSL/TLS uses Private-Public asymmetric keys to exchange symmetric keys used to encrypt data.
  - The symmetric keys exchanged are referred to as “session keys”.

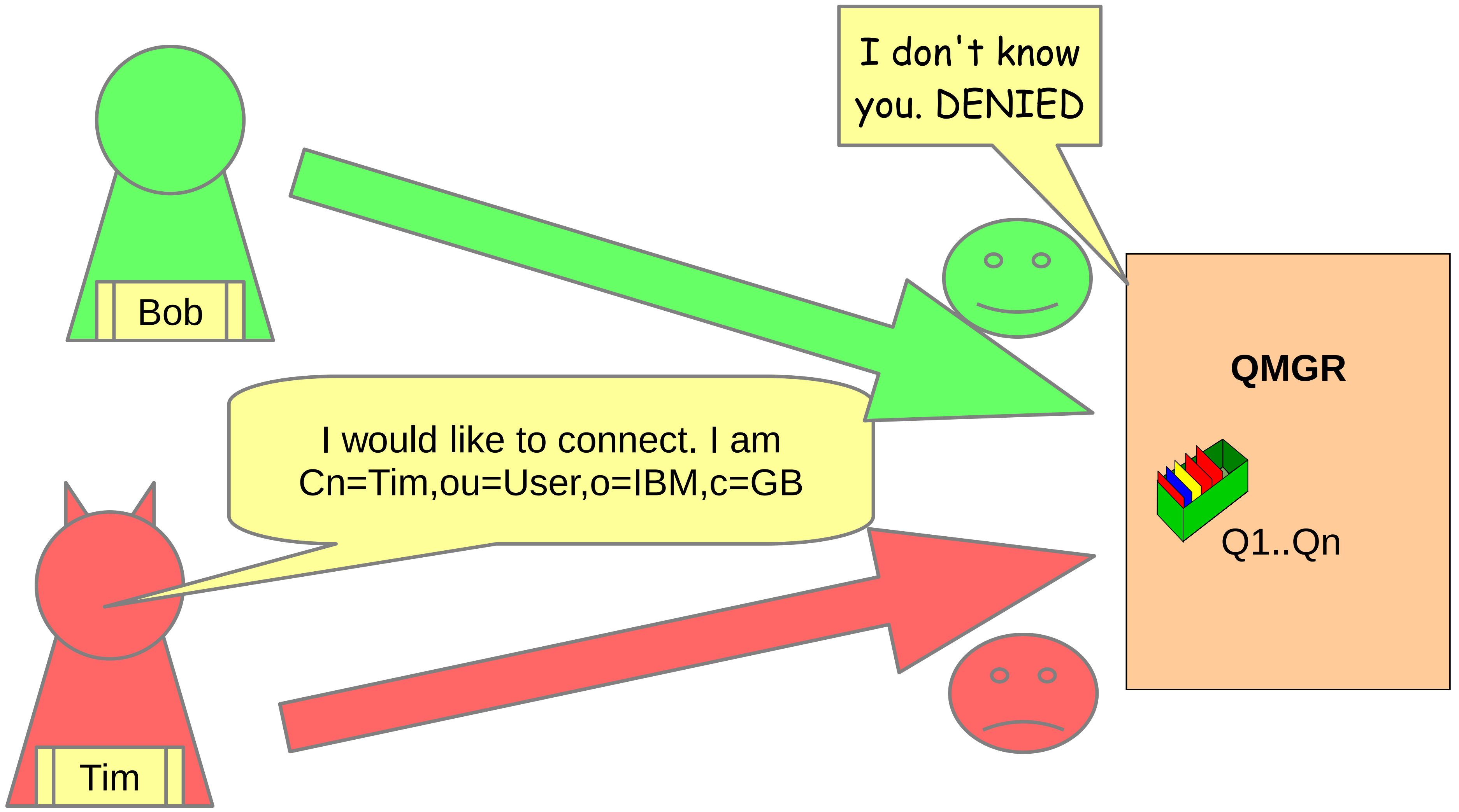
SSL/TLS – Use Case


0@;;7A//#ca
£66!j:sdw)
QMGR
Q1..Qn
Bob
I don't know Bob's password so let's find it out by listening in!
What the...?
Tim

SSL/TLS – Use Case

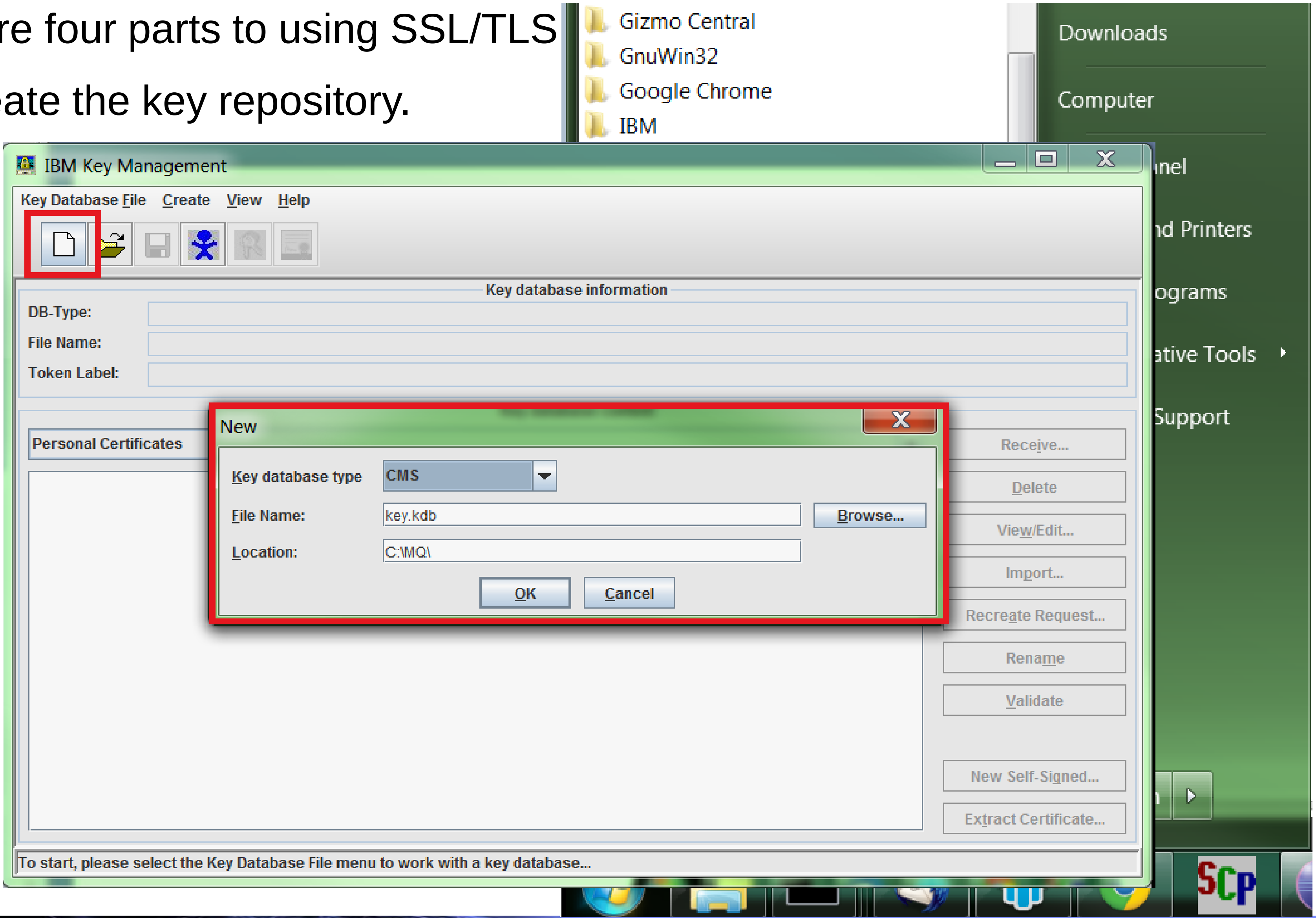


SSL/TLS – Use Case



SSL/TLS – Setting up QMGR

- There are four parts to using SSL/TLS
- First create the key repository.



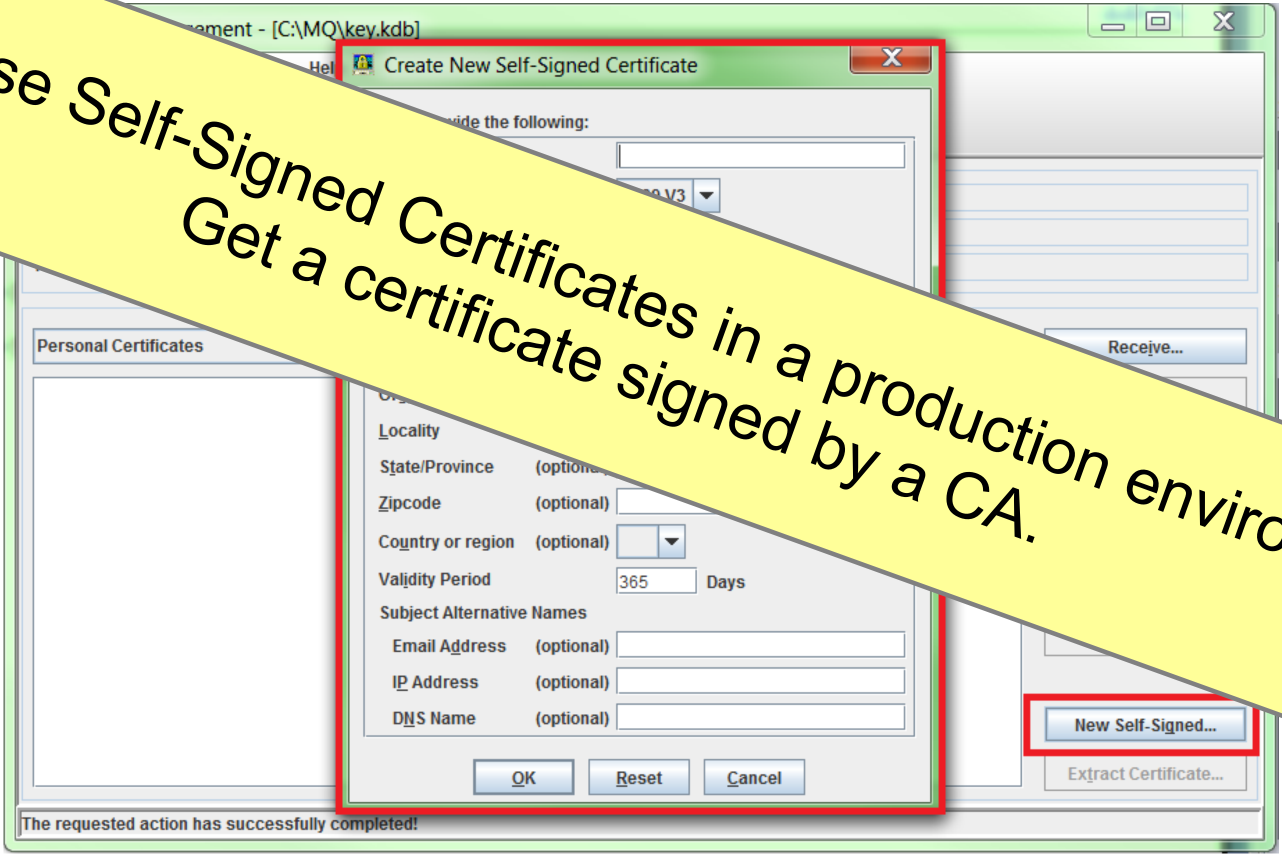
DB-Type:
File Name:
Token Label:

Key database type: CMS
File Name: key.kdb
Location: C:\MQ\

To start, please select the Key Database File menu to work with a key database...

SSL/TLS – Setting up QMGR

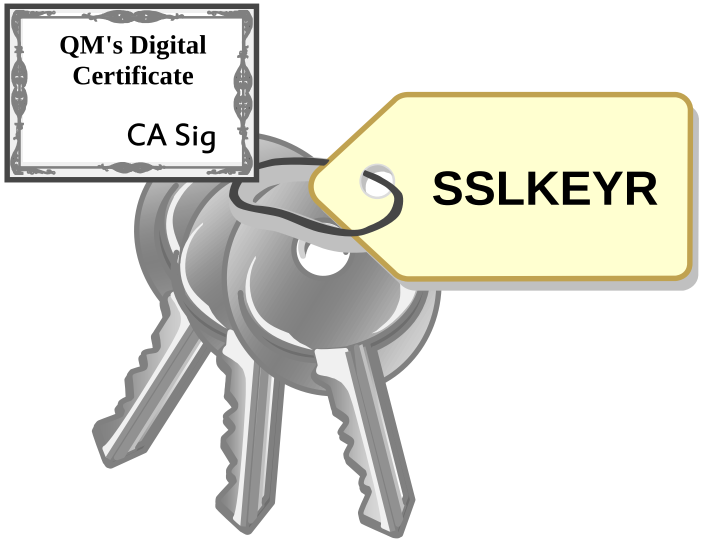
- There are four parts to using SSL/TLS
- First create the key repository.
- ...t Create the QMGR Certificates.



The requested action has successfully completed!

Don't use Self-Signed Certificates in a production environment!
Get a certificate signed by a CA.

SSL/TLS – Setting up QMGR

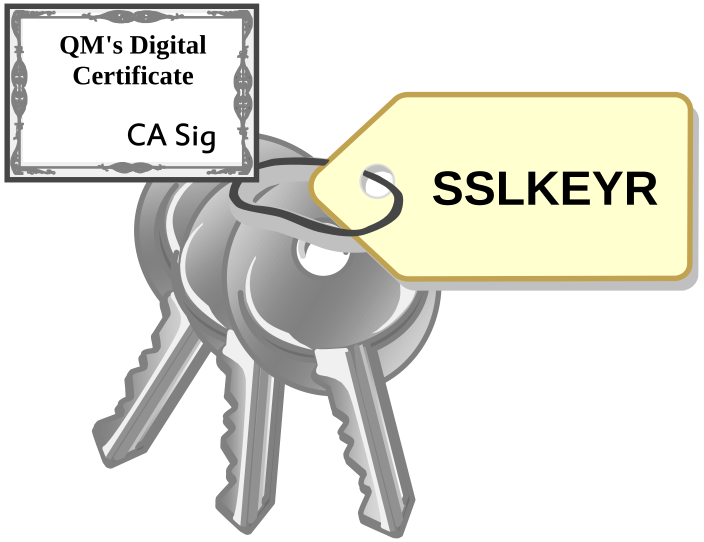


- There are four parts to using SSL/TLS
- First create the key repository.
- Next Create the QMGR Certificates.
- Now set up the QMGR to use it.

```
ALTER QMGR
SSLKEYR('var/mqm/qmgrs/QM1/ssl/key')
CERTLABL(‘QM1Certificate’)

REFRESH SECURITY TYPE(SSL)
```

SSL/TLS – Setting up QMGR



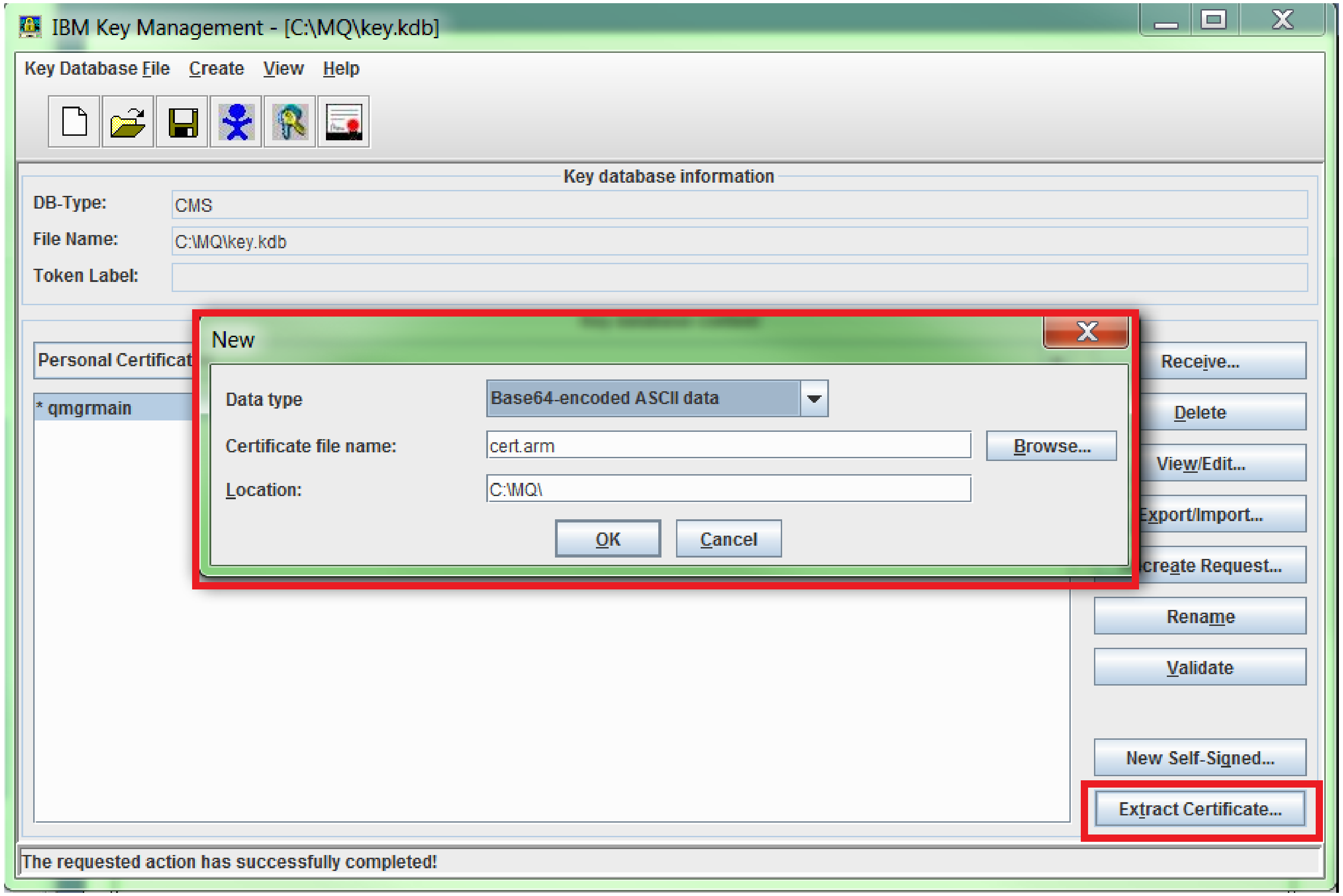
- There are four parts to using SSL/TLS
- First create the key repository.
- Next Create the QMGR Certificates.
- Now set up the QMGR to use it.
- Finally set up the Channel to use SSL

```
ALTER CHANNEL(X) SSLCAUTH(REQUIRED)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
```

SSL/TLS – Final Steps for SSL/TLS

- Once the QMGR is ready you need to exchange public keys.

–**Never give out your Private keys!**



IBM Key Management - [C:\MQ\key.kdb]

Key database information

DB-Type: CMS
File Name: C:\MQ\key.kdb
Token Label:

Personal Certificat
* qmgrmain

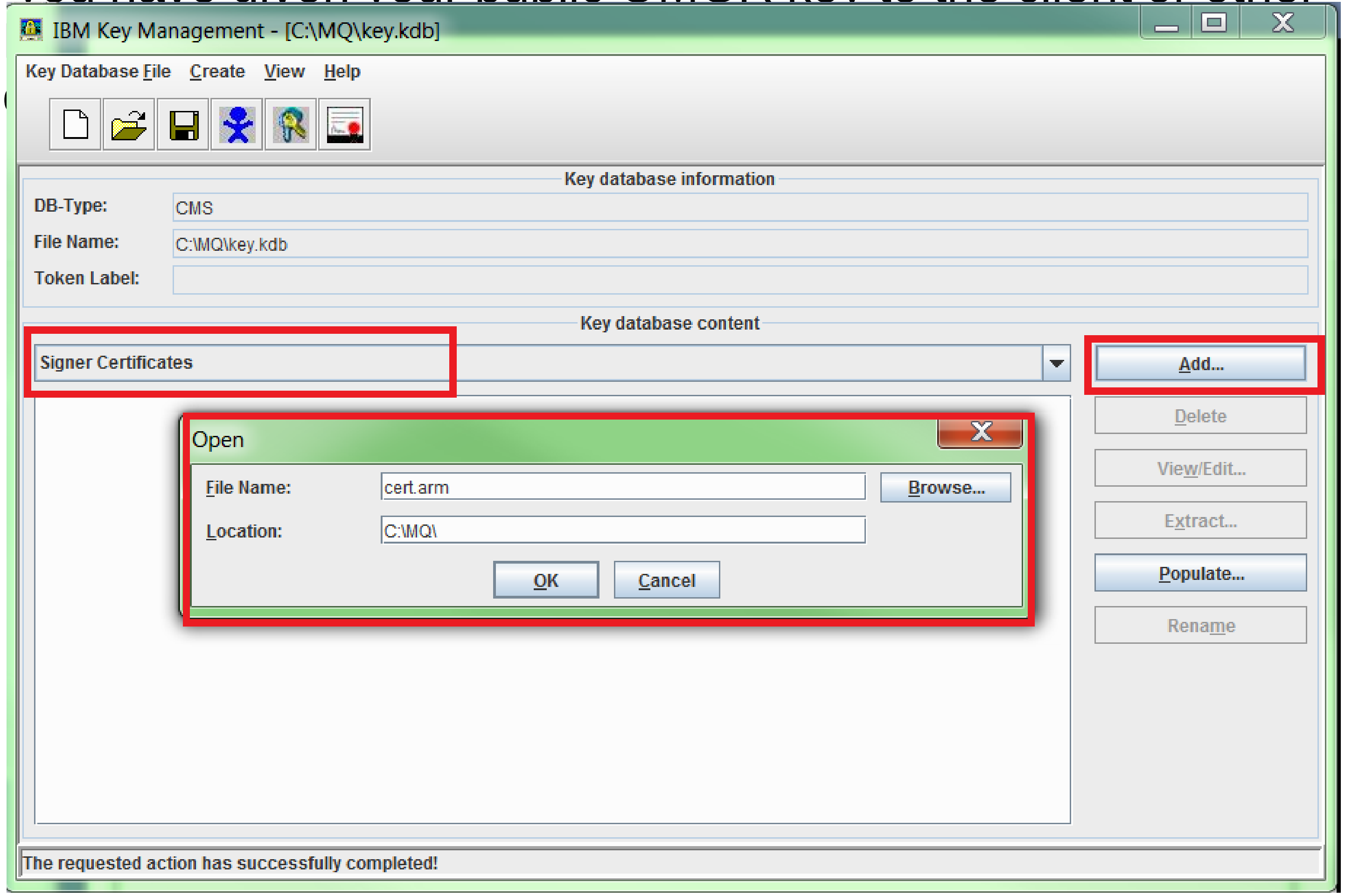
New

Data type: Base64-encoded ASCII data
Certificate file name: cert.arm
Location: C:\MQ\

The requested action has successfully completed!

SSL/TLS – Final Steps for SSL/TLS

- Once you have given your public QMGR key to the client or other QMG certifi



DB-Type: CMS
File Name: C:\MQ\key.kdb
Token Label:

Signer Certificates

File Name: cert.arm
Location: C:\MQ\

The requested action has successfully completed!

Channel Authentication

Channel Authentication – Use Case

- CHLAUTH rules are basically filters.
- We create rules that will allow or block a connection that matches the filter.
- The filter can be either very specific or generic.
- Types of filters:

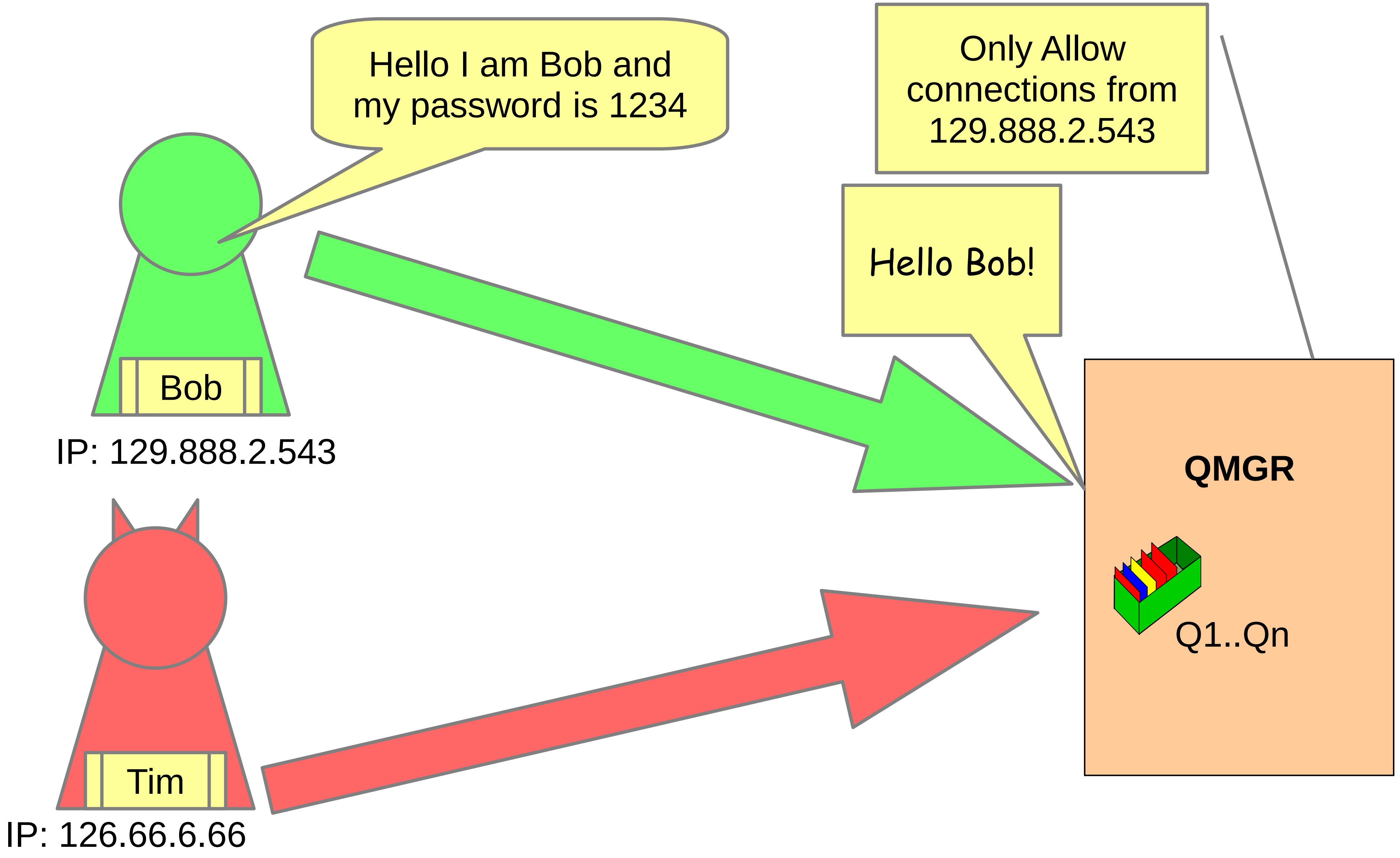
–SSL Distinguished name (Issuer and Subject)

–Client User ID name

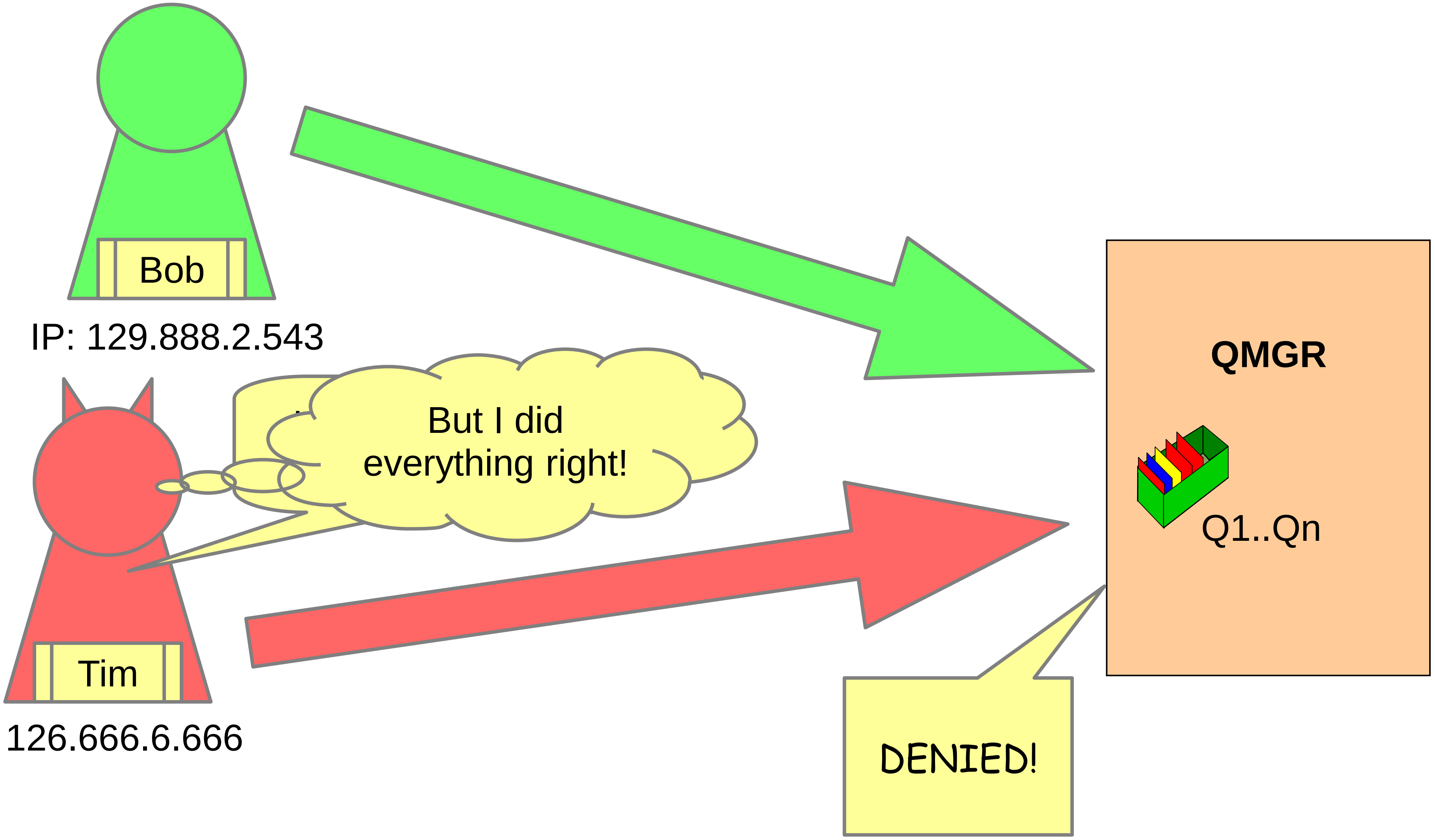
–Remote Queue Manager name

–IP/Hostname

Channel Authentication – Use Case


Hello I am Bob and my password is 1234
Only Allow connections from 129.888.2.543
Hello Bob!
Bob
IP: 129.888.2.543
QMGR
Q1..Qn
Tim
IP: 126.66.6.66

Channel Authentication – Use Case



Channel Authentication – Side note

- Channel Authentication rules have an order of checking:

1) ADDRESSMAP

2) BLOCKADDR

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 used to work out what to do.

- For example two ADDRESSMAP:

- 1, Block where address=*

- 2, Allow where address=129.12.9.9

- Connection from 129.12.9.9 will be allowed through.

Channel Authentication – USERSRC

- 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

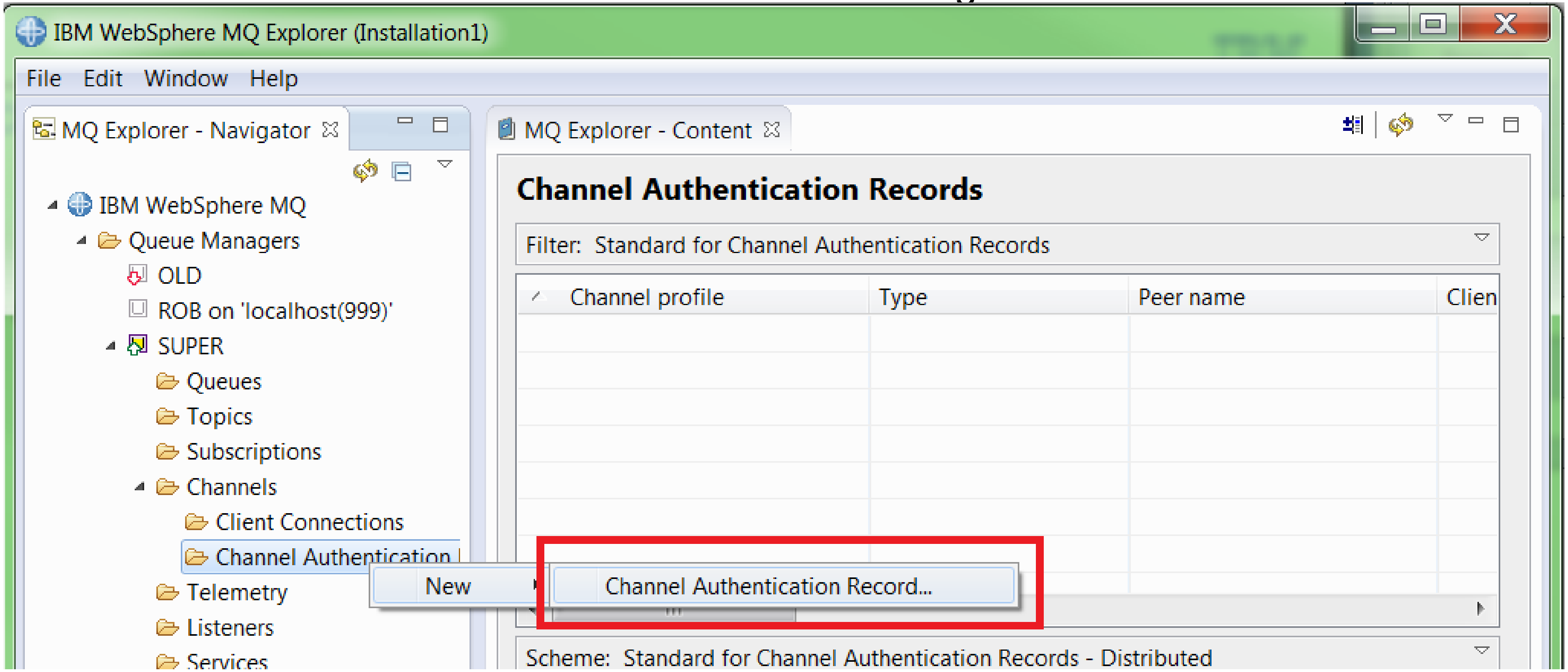
- In addition you can raise the security of the channel by setting a higher CHCKCLNT value on the CHLAUTH.

–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.

Channel Authentication – MQ Explorer

- To create a new Channel Authentication rule right click on the channel



Channel Authentication – MQ Explorer

- Next follow the steps to set up your channel authentication rule.
- In the Channel profile screen you can put the name of a channel or a generic name

–For example: “INCOMING.CHANNEL” or “System.*”

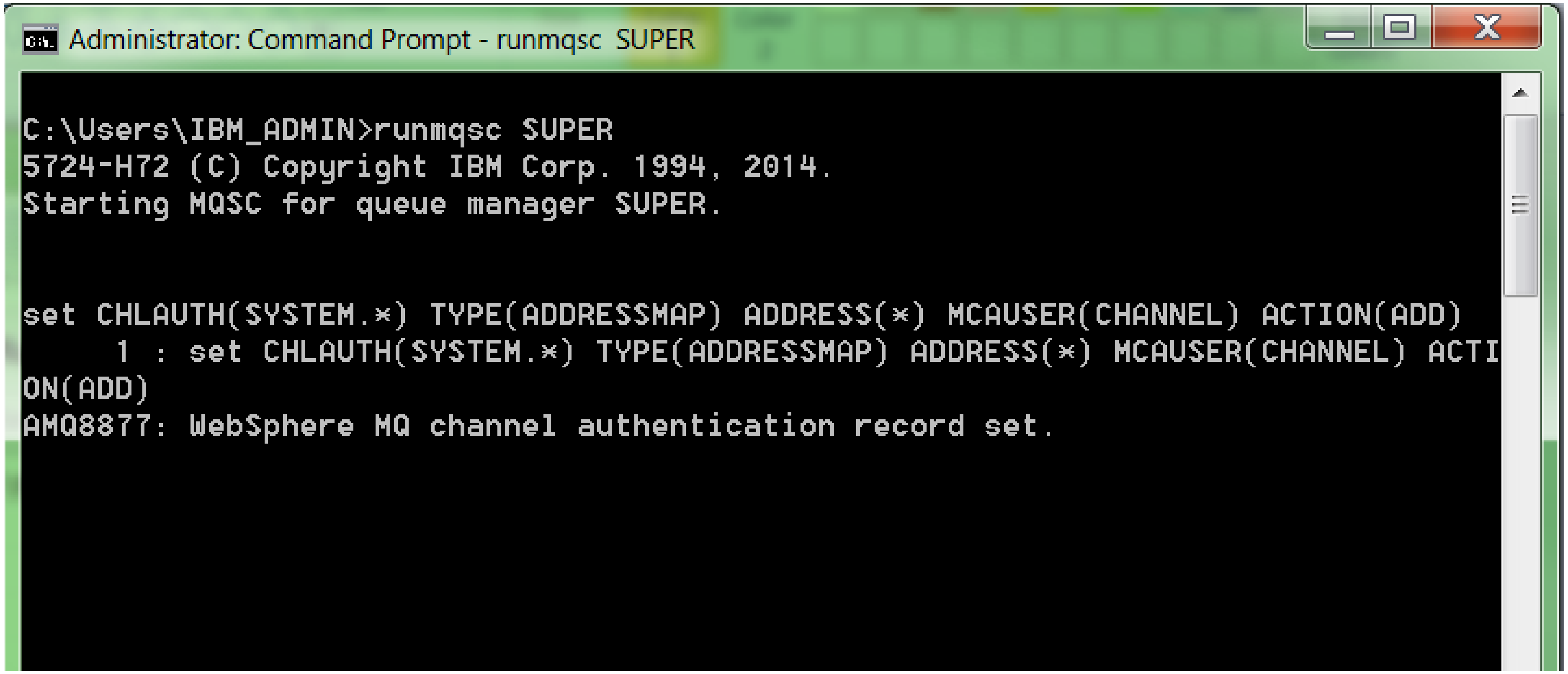
- The next screens allow you to put the filter rules in for the CHLAUTH rule which will cause the rule to trigger.

–For example In a CHLAUTH rule of type ADDRESSMAP putting address=* will cause the rule to trigger for all addresses.

Channel Authentication – Command Line

- CHLAUTH rules are added and removed using the SET command in RUNMQCS.

–The difference between adding and removing is what ACTION(x) is set to.



```
C:\Users\IBM_ADMIN>runmqsc SUPER
5724-H72 (C) Copyright IBM Corp. 1994, 2014.
Starting MQSC for queue manager SUPER.


set CHLAUTH(SYSTEM.*) TYPE(ADDRESSMAP) ADDRESS(*) MCAUSER(CHANNEL) ACTION(ADD)
     1 : set CHLAUTH(SYSTEM.*) TYPE(ADDRESSMAP) ADDRESS(*) MCAUSER(CHANNEL) ACTI
ON(ADD)
AMQ8877: WebSphere MQ channel authentication record set.
```

Security Exits

Security Exits

- Security exits are bespoke, customer created exists that are ran during the security checking.
- MQ comes with an API that means a security exit can interact with MQ to provide extra security that a customer wishes.
- 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 were used to provide Connection Authentication.

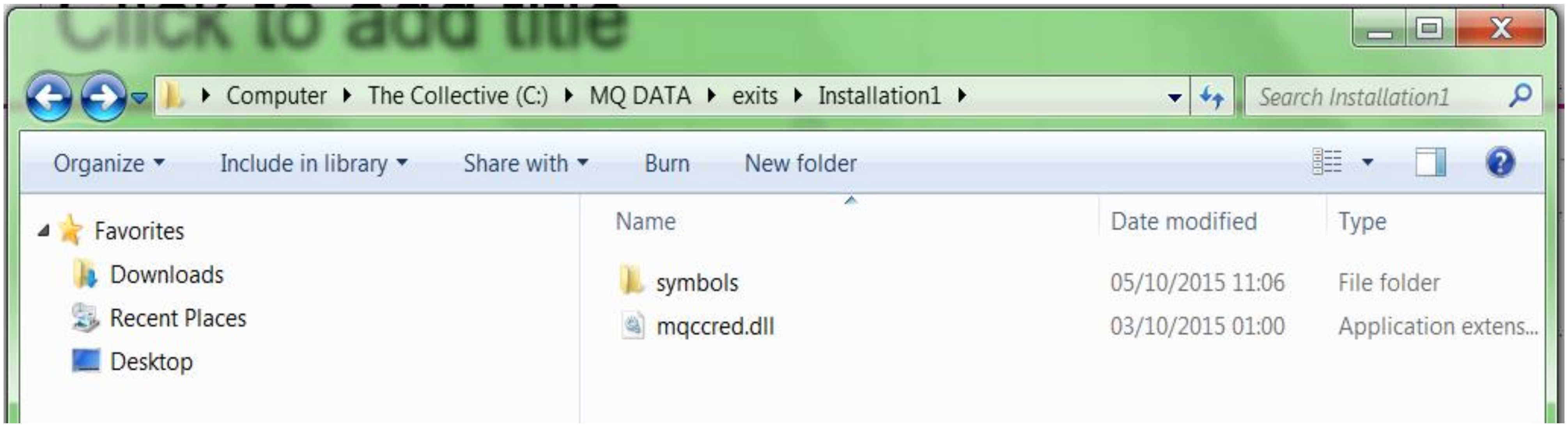
Security Exits

- First write a C Application with the following skeleton Code

```
void MQENTRY MQStart() {;}
void MQENTRY EntryPoint (PMQVOID pChannelExitParms,
                         PMQVOID pChannelDefinition,
                         PMQLONG pDataLength,
                         PMQLONG pAgentBufferLength,
                         PMQVOID pAgentBuffer,
                         PMQLONG pExitBufferLength,
                         PMQPTR pExitBufferAddr)
{
  PMQCXP pParms = (PMQCXP)pChannelExitParms;
  PMQCD pChDef = (PMQCD)pChannelDefinition;
  /* TODO: Add Security Exit Code Here */
}
```

Security Exits

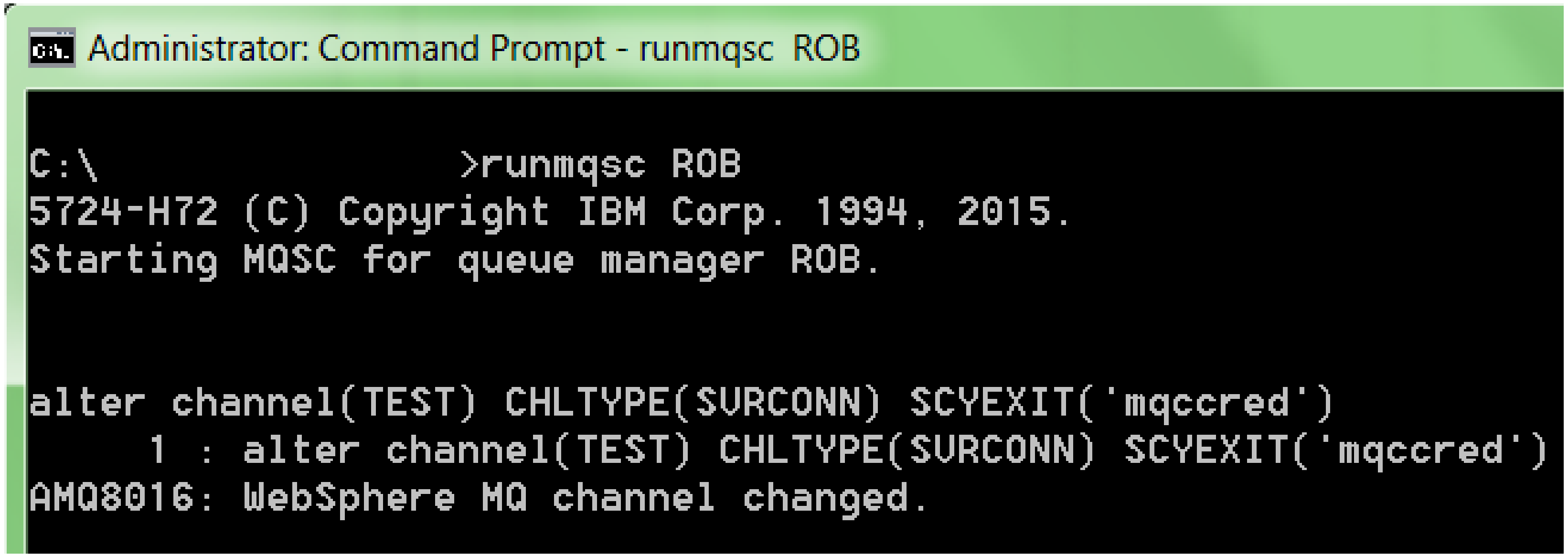
- Compile it into a dll and place the dll in:
- <MQ Data Root>/exits/<Installation Name>



Name	Date modified	Type
symbols	05/10/2015 11:06	File folder
mqccred.dll	03/10/2015 01:00	Application extens...

Security Exits

- Alter the channel you want to run the exit:
- SCYEXIT('<name of dll>')
- SCYDATA('<Data to pass to the Security Exit>')



```
C:\                 >runmqsc ROB
5724-H72 (C) Copyright IBM Corp. 1994, 2015.
Starting MQSC for queue manager ROB.


alter channel(TEST) CHLTYPE(SVRCONN) SCYEXIT('mqccred')
     1 : alter channel(TEST) CHLTYPE(SVRCONN) SCYEXIT('mqccred')
AMQ8016: WebSphere MQ channel changed.
```

AMS

AMS

- AMS stands for Advanced Message Security
- 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.
- The policies describe whether messages should be digitally signed or digitally signed + encrypted. Signing and encryption uses digital certificates, such as those used by SSL/TLS.
- AMS is an end-to-end security model, messages stay signed/encrypted through the whole lifetime of a message

AMS

- AMS does not perform any access control, it just provides privacy and integrity to messages - it is complementary - not an alternative to setting OAM authorities to determine who can access a queue
- AMS allows messages to be selectively encrypted so that even MQ administrators cannot see the cleartext content without the right certificate
- Certain types of data fall under standards compliance that requires encryption whilst 'at rest' as well as in transit - e.g. credit card numbers (PCI), healthcare (HIPAA), government data - for MQ 'at rest' means whilst data is on a queue and AMS is our strategic offering for this type of data

Useful Links

- MQ v8 information: https://www.ibm.com/developerworks/community/blogs/messaging/entry/where_can_i_find_mq_v8_information?lang=en
- MQ v8 Security Demo: https://www.youtube.com/watch?v=0aKamUTS4rs&feature=youtu.be

Click to add text

Thank you very much.

Robert Parker

IBM
IBM MQ Security Development
parrobe@uk.ibm.com