What I Did
Over Summer Vacation
(In Hursley)

Certified for IBM. WebSphere. software

Certified for IBM. Power Systems

T.Rob Wyatt
Managing Partner, IoPT Consulting
704-443-TROB (8762)
t.rob@ioptconsulting.com
https://ioptconsulting.com

End of WebSphere MQ v8.0 EAP

- Early Access Program closed out shortly after v8.0 was released.
- Workshop held at Hursley to review the final feature set in the release.
- Covered much territory including security, performance, compatibility, upgrades, documentation, and more.

This session is my summary of the highlights of that session.

Some of the results and findings may impact how you use the product and/or your plans for migration.

Look for a download on the MQTC site and/or my site at https://t-rob.net/links

You Are (Not) Here

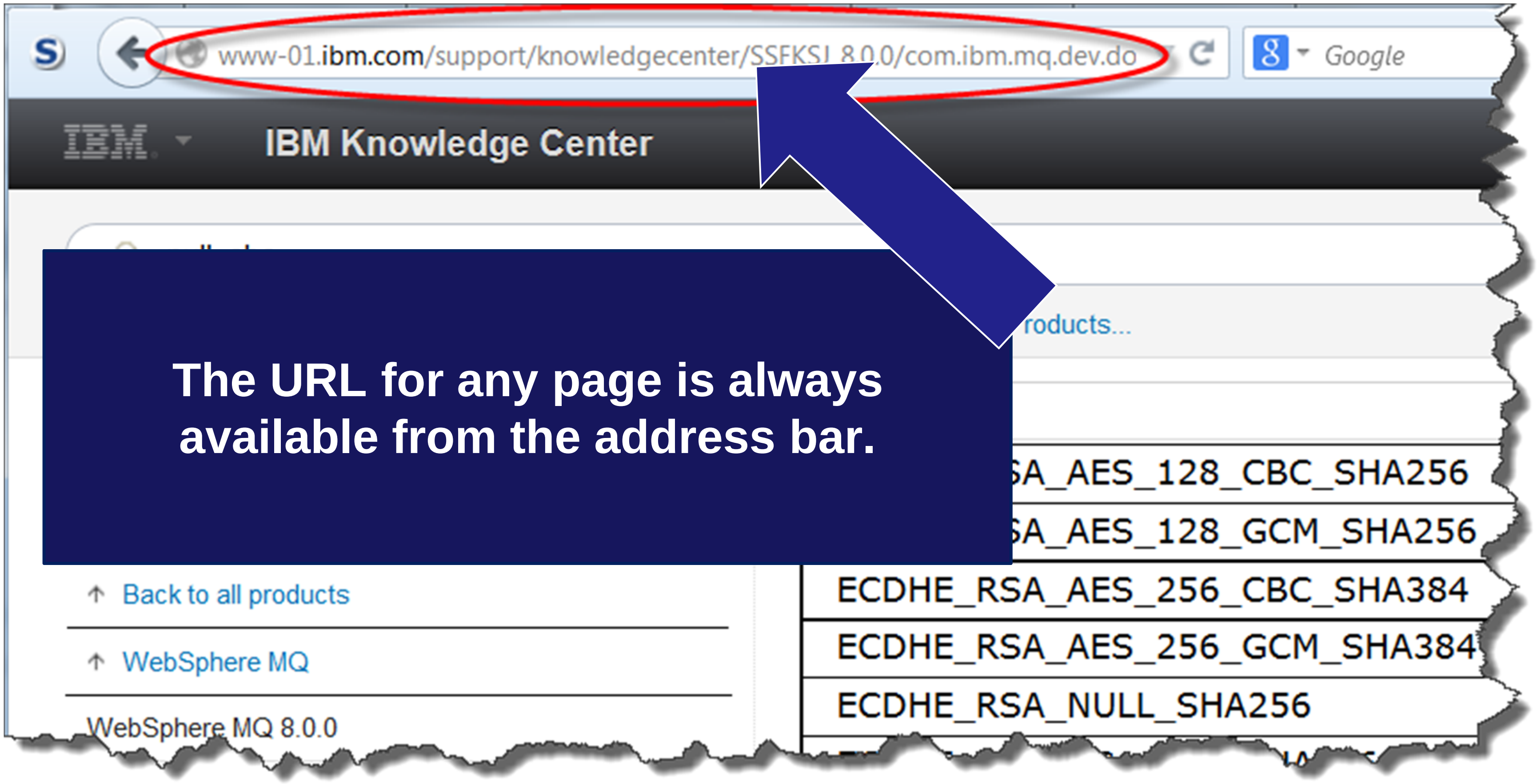
Knowledge Center: Love it or hate it?

- All of the MQ documentation for current versions has been ported to the Knowledge Center format.
- I had the opportunity to have an in-depth meeting with the manager of the tech writers who manage the KC.
- Note that the people who *program* the KC are a different group.
- Some of the things you will learn here REQUIRE your participation to get fixed. These generally fall into the categories of content defects, indexing and tagging.
- Some we hope will be resolved on their own. These generally fall into the category of mechanical and software defects.

idcrf@hursley.ibm.com

(Because sometimes the built-in reporting fails.)

KC Love: Sharing links

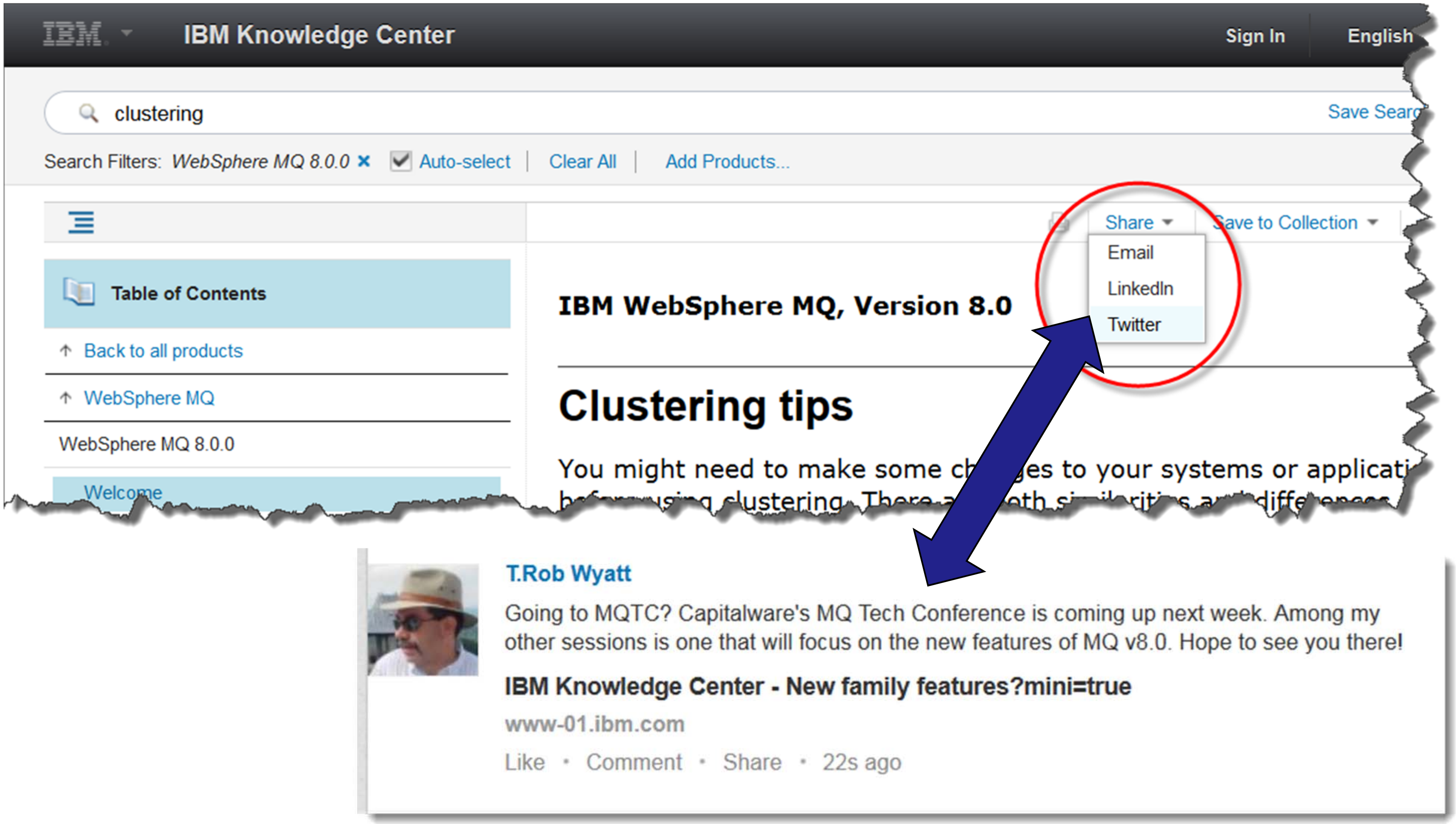


www-01.ibm.com/support/knowledgecenter/SSFKSJ_8.0.0/com.ibm.mq.dev.do

SA_AES_128_CBC_SHA256
SA_AES_128_GCM_SHA256
ECDHE_RSA_AES_256_CBC_SHA384
ECDHE_RSA_AES_256_GCM_SHA384
ECDHE_RSA_NULL_SHA256

The URL for any page is always available from the address bar.

KC Love: Sharing links



IBM WebSphere MQ, Version 8.0

Clustering tips

You might need to make some ch[...]es to your systems or applicati
before using clustering. There a[...]oth similarities and differences

T.Rob Wyatt

Going to MQTC? Capitalware's MQ Tech Conference is coming up next week. Among my other sessions is one that will focus on the new features of MQ v8.0. Hope to see you there!

IBM Knowledge Center - New family features?mini=true

www-01.ibm.com

Like · Comment · Share · 22s ago

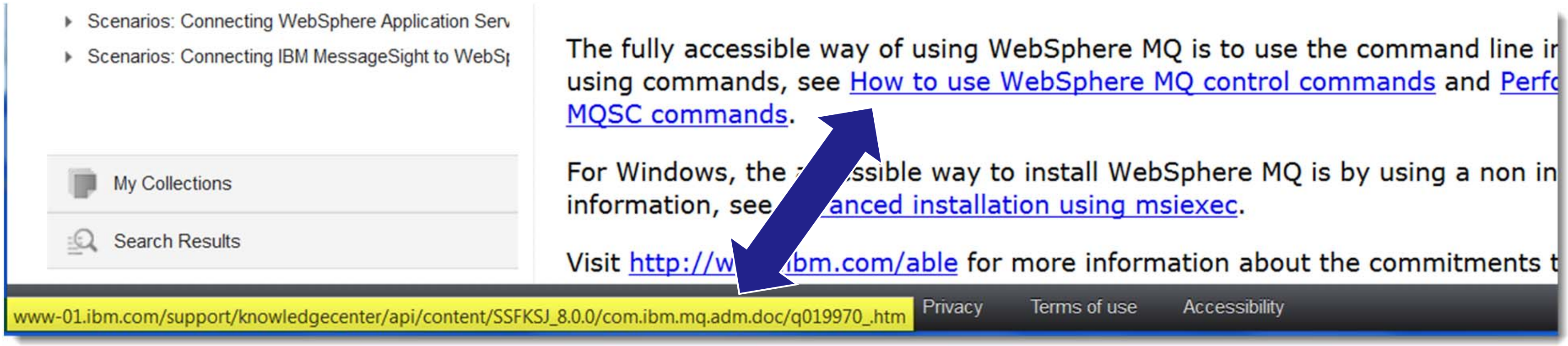
KC Hate: Sharing links

- **No more right-click on a TOC link to get the URL.**
  - All TOC links are Javascript
  - Right click to new tab always opens to Infocenter home page.

- **You must render the page to get its URL from the TOC.**

- **URLs embedded in page content are (all?) hard-coded URLs**
  - These actually *do* work with right-click or open to new tab.

- **The value in the status bar lets you know what kind of URL it is.**
  - Javascript? Either blank status or `void()`.
  - Entire URL? Copy away!


Scenarios: Connecting WebSphere Application Serv
Scenarios: Connecting IBM MessageSight to WebS
My Collections
Search Results
Privacy
Terms of use
Accessibility

The fully accessible way of using WebSphere MQ is to use the command line ir using commands, see How to use WebSphere MQ control commands and Perfo MQSC commands.

For Windows, the ssible way to install WebSphere MQ is by using a non in information, see anced installation using msiexec.

Visit http://w ibm.com/able for more information about the commitments t

www-01.ibm.com/support/knowledgecenter/api/content/SSFKSJ_8.0.0/com.ibm.mq.adm.doc/q019970_.htm

KC Ambivalence: Sharing links

- **The slug at the bottom of each content page has been unreliable.**
  - Missing
  - Wrong URL
- **Mostly with content migrated from Infocenters.**
- **Manually inserted by page author.**
- **Candidate to be generated dynamically so always correct.**
- **Now that the URL is in the address bar, not as critical.**
- **Appears to have been fixed.**

If you find this, please report it!

KC Love: Search enhancements

- Now possible to search across multiple collections.
- Narrow search by platform, keyword.
- Search results find sections within a page.
- Large result sets are paginated. (OK, this is more of a “like”.)
- Keyword type-ahead

KC Hate: Search enhancements

- **Filtering entirely dependent on manual authoring to add tags, keywords.**
- **Total number of search results not displayed.**
- **No sort of search results.**
- **Search results return duplicate pages.**
- **Search results return same page under different titles.**
- **Pages often do not sync to TOC. Sync button removed. Damn.**
- **Search results do not provide enough context.**
  - Multiple pages with same heading, no way to tell which section they are in.

Running into these issues? Please send in corrections!

Security Love: ID & Password

- **Now possible to natively authenticate an ID & Password on connect.**
- **ID & Password encrypted if client & server are BOTH >= v8.0.**
- **Encryption is session-based, not replayable.**
- **Does not require TLS channels to keep credentials confidential.**

Security Hate: ID & Pwd *may* be plaintext

- **The only case in which the ID & password are encrypted is when both client & server are at v8.0.**
  - Older version of client does not encrypt the password.
  - Possible to set WMQ to not connect if password in the clear.

- **Need to use TLS channels if any client < v8.0.**
  - Potentially use server-only authentication.
  - Make sure to use TLS/SHA ciphers.

- **Alternatively, use MQAUSX from Capitalware**
  - (i.e. the folks running this conference.)
  - Unsolicited, unpaid endorsement.

Security Love: SSLCERTI

- **SSLCERTI is now available in CHLAUTH rules.**
  - Formerly only available to exits.
  - Filters on the Distinguished name of the *issuer* of the cert.
  - CA-signed certs the issuer is the CA who signed the cert.
  - Self-signed certs are their own issuer. (IssuerDN=SubjectDN)
- **Ensures that cert originates with the intended CA or entity.**
- **Needed when there are multiple root certs in the KDB, especially when one or more of them is from a business partner or internal CA.**
- **Prior to SSLCERTI, the Distinguished Name could only be guaranteed to be globally unique if the KDB contained only one trusted cert.**
- **With SSLCERTI, the combination of Subject DN within Issuer DN creates a globally unique name.**
  - Assuming, of course, that all trusted certs in the KDB are from reliable sources.
  - Does not address problem of admins accepting non-authoritative signer certs.

New features – Love!

- **64-Bit on all platforms.**
  - Windows 7 or better.
- **AMS & MFT now integrated on z/OS & iSeries.**
- **Delete ACL record based on Windows SID**
  - No more orphaned ACLs when an ID or group is deleted.
- **Topic hosting in a cluster**
  - Control routing of publications in a cluster.
  - Design topology to prevent netstorm of publications in a large cluster.
  - All participating nodes must be v8 or higher.
  - Detects hierarchy & proxy subscription loops.

New features - Hate

- **Possible to configure OAM to use user ID rather than group.**
  - Requires QM.ini stanza edit, or crtmqm switch.
  - Once set, no longer gets primary group during setmqaut.

- **Use DNS names instead of IP addresses in CHLAUTH records.**
  - DNS subject to DOS, spoofing, poisoning attacks.
  - Even legitimate DNS may resolve to different addresses, FQDNs, etc.
  - DNS lookup latency – which can be very long.
  - The paradox of using unsecure (in most cases) DNS to make a security control easier, thereby weakening the achieved security to less than without the control.

JMS Enhancements - Love

- **WMQ Now supports JMS 2.0!**
- **Very highly requested features:**
  - Delayed message delivery.
  - Shared subscriptions. Messages round-robin across multiple consumers sharing a single subscription.
- **Prior to JMS 2.0, lots of code and configuration contortions were required to achieve these behaviors.**
  - Increased skill requirement.
  - Lots of moving parts.
  - Brittle.
- **As of JMS 2.0, these are now native behaviors.**
  - Slightly increased skill requirement but…
  - Few moving parts.
  - Reliable. Fully supported functionality of the product.

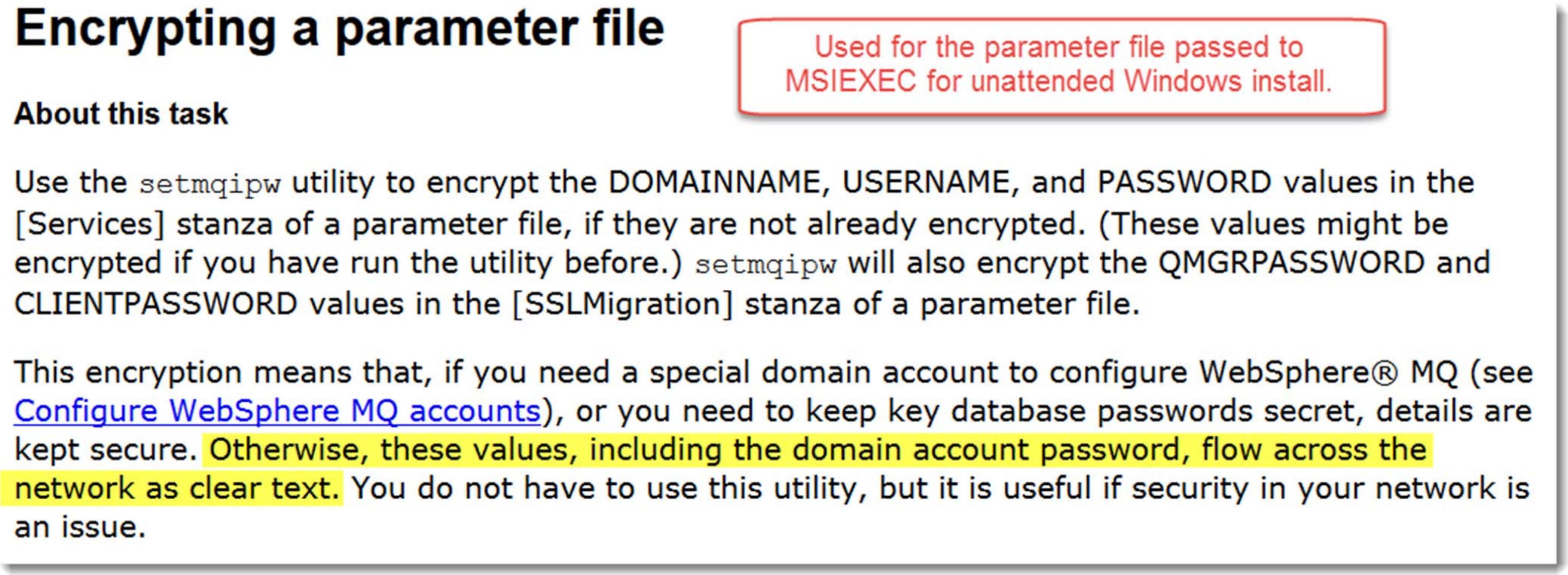
JMS Enhancements - Hate

THIS PAGE INTENTIONALLY LEFT BLANK

Old features - Hate

- **The setmqipw command remains unchanged.**
  - Subject to replay attack.

- **Limited, normally 1-time use during unattended Windows install.**
  - And how often does that happen, really. Generally either zero or a whole lot.



Encrypting a parameter file

Used for the parameter file passed to MSIEXEC for unattended Windows install.

About this task

Use the `setmqipw` utility to encrypt the DOMAINNAME, USERNAME, and PASSWORD values in the [Services] stanza of a parameter file, if they are not already encrypted. (These values might be encrypted if you have run the utility before.) `setmqipw` will also encrypt the QMGRPASSWORD and CLIENTPASSWORD values in the [SSLMigration] stanza of a parameter file.

This encryption means that, if you need a special domain account to configure WebSphere® MQ (see Configure WebSphere MQ accounts), or you need to keep key database passwords secret, details are kept secure. Otherwise, these values, including the domain account password, flow across the network as clear text. You do not have to use this utility, but it is useful if security in your network is an issue.

Per-channel certificates - Love

- **Allows the QMgr to present different personal certificates depending on which inbound channel is used.**
- **For example, internal channels present an internally signed certificate whilst external channels present a cert signed by a commercial CA.**
- **Uses the TLS Server Name Indication extension.**
  - Which means the cipher used *must* be a TLS variant. SSL ciphers don’t work.
- **Improved error messages. Since the channel name is passed with the connection request the QMgr can display it rather than ???????.**
- **Requires both ends of the connection to be at MQ v8.0 or above.**
- **The channel name is sent in the clear.**
  - Previously, channel names not exposed on the wire.
  - A case of balancing pros/cons of two security controls.
  - Ability to use multiple personal certs offsets exposure of channel name.

Questions & Answers