MO04: WebSphere MQ SSL Wizard
User Guide
Version 2.0.0.1

January 2010

Ian Vanstone
MP160,
IBM UK Laboratories Ltd.
Hursley
Winchester
Hants, SO21 2JN
United Kingdom
ivans@uk.ibm.com

Changes

Version	Released	Changes
V1.0	August 2005	-
V1.1	November 2005	- Added support for generating certificate requests. - Fixed RACDCERT CONNECT incorrectly using CERTAUTH for self signed certificates. - Fixed instructions save adding ".html" as suffix if suffix already exists - Changed certificate CN fields to combo box containing QMName and certificate label name on first pass. - Show the certificate label names (greyed out) on certificate panels. - Added ST and (single) OU distinguished name attributes. - Fixed Sender CA Properties panel field alignment problem. - Fix File->Save As exceptions caused by blank entry fields. - Change Windows commands to use runmqckm instead of gsk7cmd. - Allow spaces in Windows and UNIX key database paths.
V1.2	May 2006	- Support for C, Java and JMS clients. - Only CN, O and C are required by GSKit. - Other misc. changes.
V1.3	November 2006	- Various fixes to client support - Added new extra CipherSpecs - Added CipherSpec to CipherSuite mapping for Java/JMS clients
V2.0	November 2009	- Improved CA model - Improved GUI layout - Improved script formatting - Updated client samples for WebSphere MQ V7.0.1 - Added diagrams to each GUI page - Added gsk7capicmd command option - Added SSLFIPS support with restricted SSLCIPH values - Added FIPS/Sigalg for gsk7capicmd support - Added basic multiple OU support - Added full SSLPEER to channel definitions - Added certificate expiry - Added sample build instruction examples to doc. - Removed all MD5 hashing algorithms - Removed backwards compatibility of data files (sorry, let me know if this is a major problem for you) - Changed SSLCAUTH so that it now defaults to REQUIRED - Changed sample passwords to be unique for each key database - Documentation updates - Bug fixes - Many internals updates
V2.0.0.1	January 2010	- Fixed quoting of SSLPEER strings - Fixed italics font in instructions

V2.0.0.1 Edition, January 2010

This edition applies to Version 2.0 of *WebSphere MQ SSL Wizard* and to all subsequent releases and modifications until otherwise indicated in new editions.

Take Note!

Before using this User Guide and the product it supports, be sure to read the general information under "Notices".

Notices

The following paragraph does not apply in any country where such provisions are inconsistent with local law.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore this statement may not apply to you.

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates.

Any reference to an IBM licensed program or other IBM product in this publication is not intended to state or imply that only IBM's program or other product may be used. Any functionally equivalent program that does not infringe any of the intellectual property rights may be used instead of the IBM product. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, New York 10594, USA.

The information contained in this document has not be submitted to any formal IBM test and is distributed AS IS. The use of the information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item has been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:
WebSphere MQ
IBM
z/OS
The following terms are trademarks of the Microsoft Corporation in the United States and/or other countries:
Windows 95,98,Me
Windows NT, 2000,XP

Chapter 1. WebSphere MQ SSL Wizard

Overview

The WebSphere MQ SSL Wizard is a utility designed to ease the administration of a basic TLS/SSL channel. The WebSphere MQ SSL Wizard takes input in series of entry panels and then generates a set of instructions to enable the user to define and start a TLS/SSL channel. The instructions generated include both the platform specific commands for creating the certificates (e.g. using RACF or GSKit) and the MQSC commands used to define and start the WebSphere MQ channel.

The WebSphere MQ channel can either be an MCA channel between two queue managers or a client connection channel to a queue manager. Sample source and binaries are shipped with the WebSphere MQ SSL Wizard for clients written in C, Java and JMS.

The WebSphere MQ SSL Wizard generates instructions for z/OS, UNIX and Windows, although some instructions (e.g. MQSC) may be run on other platforms.

WebSphere MQ SSL Wizard Pre-requisites

Java 2 Runtime Environment 1.4 and above.

Output Pre-requisites

The WebSphere MQ MQSC commands generated by the WebSphere MQ SSL Wizard can be run on WebSphere MQ V6 and above. The certificate creation commands generated by the WebSphere MQ SSL Wizard are for RACF on z/OS and GSKit on UNIX and Windows.

Installation

To install the WebSphere MQ SSL Wizard simply decompress *mo04.zip* into a directory of your choice.

Quick Beginnings

Run the WebSphere MQ SSL Wizard from a command prompt, as follows: *java -jar wmqsslwizard.jar*.
Note: The '*-jar*' parameter may not be required.

Chapter 2. Using the Wizard

Basic operation

Enter data in each field displayed and press the *Next* button, until the *Generated instructions* page. The *Previous* button can also be used to go back. The generated instructions list the instructions and commands required to create the certificates and define the WebSphere MQ TLS/SSL channel.
Note: Several features are given sensible defaults. If you don't understand the meaning of a field, leave the default value. If a required field is omitted, a message will be displayed.

Page diagrams

Each page contains a diagram indicating the component to which the page entry fields relate. The diagrams each contain the components involved to that point and the specific component relating to the page is highlighted in red. See Appendix E for examples of the diagrams.

Saving/Opening user data

The *File->Open* menu option is used to restore the data for all entry fields from a data file. The *File->Save* menu option is used to save the data for all entry fields to a data file.
Note: Data files from previous versions of the WebSphere MQ SSL Wizard are not compatible with WebSphere MQ SSL Wizard V2.0.x.

A file can be opened on startup of the WebSphere MQ SSL Wizard by adding the data filename to the command line, as follows: *java -jar wmqsslwizard.jar sample_client.data*
Note: The '*-jar*' parameter may not be required.

Two sample data files, *sample_client.data* (for a client channel) and *sample_mca_channel.data* (for a queue manager to queue manager channel), are shipped in *mo04.zip*.

A data file can be used to store defaults values, where the supplied defaults are not suitable.

Saving/Copying the generated instructions

The *Save Instructions* button is used to save the generated instructions text to an html file (Firefox. The Edit->Copy menu item will copy either entire generated instructions text or the selected generated instructions text to the clipboard.

The SSL Client and SSL Server

The SSL Client is the channel which initiates communication - the client for a client/server connection channel and the sender for a sender/receiver channel.

The SSL Server is the channel which responds to a request from an SSL Client - the server for a client/server connection channel and the receiver for a sender/receiver channel.

Accessibility

Each button and entry field can be accessed in turn by pressing the TAB key. The File menu can be activated with Alt+F, the Edit menu with Alt+E and the Help menu with Alt+H. Once a menu is activated the menu items can be selected with the keys noted below.

Menu Item	**Key**
File-> New	N
File-> Open…	O
File-> Save As…	A
File-> Exit	X
Edit-> Copy	C
Help-> Help	P
Help-> About	T

The generated instructions text can also be copied to the clipboard using Ctrl+C. Data files can be opened using Ctrl+O. Data files can be saved using Ctrl+S.

Chapter 3. Entry Fields

This chapter holds information about each wizard page and information about the entry fields on those pages.
Note: Page order depends on user entry and not all pages are necessarily made visible. See Appendix A for details of page order.

SSL Client Properties

Note: The SSL Client is the channel which initiates communication - the client for a client/server connection channel and the sender for a sender/receiver channel.

The fields on this page hold information relating to the client or queue manager that will host the sender channel.

Field	**Description**
Client User	Select the radio button to create a client connection (rather than an MCA channel). Enter the user id of the client (e.g. user1) in the text field.
Java/JMS	Select the radio button to create a Java or JMS client (rather than a C client). This is the default.
Other	Select the radio button to create a C client connection (rather than a Java/JMS client).
QMGR Name	Select the radio button to create an MCA channel (rather than a client connection). This is the default. Enter the queue manager name (e.g. QM1) in the text field.
Host	The hostname (e.g. machine1)
Platform	The platform type (z/OS, UNIX or Windows)

SSL Client z/OS Properties

The fields on this page hold information relating to the z/OS queue manager that will host the sender channel.

Field	**Description**
Keyring	The name of the RACF keyring that will be created (e.g. QM1RING)
SSL Tasks	The number of SSL Tasks for the channel initiator (e.g. 5)
Chinit ID	The userid under which the channel initiator runs (e.g. VANSTON1)

SSL Client UNIX/Windows Properties

The fields on this page hold information relating to the client or the UNIX/Windows queue manager that will host the sender channel.

Field	**Description**
Key Database	The name of the key database file that will be created (e.g.

	/var/mqm/qmgrs/QM1/ssl/my.kdb)
Command	The GSKit command (runmqckm, gsk7cmd or gsk7capicmd). See Appendix B for more information.

SSL Client gsk7capicmd Properties

The fields on this page hold information relating to the parameters used on the gsk7capicmd command on the SSL client machine.

Field	**Description**
FIPS	If set, the “-fips” parameter is used on gsk7capicmd commands. See Chapter 5 for more info on FIPS.
Sigalg	Sets the “-sigalg <value>” parameter used on gsk7capicmd commands.

SSL Server Properties

Note: The SSL Server is the channel which responds to a request from an SSL Client - the server for a client/server connection channel and the receiver for a sender/receiver channel.

The fields on this page hold information relating to the client or the queue manager that will host the receiver or server connection channel.

Field	**Description**
QMGR Name	The queue manager name (e.g. QM2)
Host	The hostname (e.g. machine2)
Port	The TCP port for the listener (e.g. 1414)
Platform	The platform type (z/OS, UNIX or Windows)

SSL Server z/OS Properties

The fields on this page hold information relating to the z/OS queue manager that will host the receiver channel or server connection channel.

Field	Description
Keyring	The name of the RACF keyring that will be created (e.g. QM2RING)
SSL Tasks	The number of SSL Tasks for the channel initiator (e.g. 5)
Chinit ID	The userid under which the channel initiator runs (e.g. VANSTON2)

SSL Server UNIX/Windows Properties

The fields on this page hold information relating to the client or the UNIX/Windows queue manager that will host the receiver channel or server connection channel.

Field	Description
Key Database	The name of the key database file that will be created (e.g. */var/mqm/qmgrs/QM2/ssl/my.kdb*)
Command	The GSKit command (runmqckm, gsk7cmd or gsk7capicmd). See Appendix B for more information.

SSL Server gsk7capicmd Properties

The fields on this page hold information relating to the parameters used on the gsk7capicmd command on the SSL server machine.

Field	Description
FIPS	If set, the “-fips” parameter is used on gsk7capicmd commands. See Chapter 5 for more info on FIPS.
Sigalg	Sets the “-sigalg <value>” parameter used on gsk7capicmd commands.

Channel Properties

The fields on this page hold information relating to the channel.

Field	Description
Channel name	The name of the channel (e.g. QM1.TO.QM2)
SSLFIPS	If set the SSLFIPS queue manager attribute is set to YES (else NO) and restricts the list of SSLCIPH values. See Chapter 5 for more info on SSLFIPS.
SSLCIPH	The cipher specification (e.g. DES_SHA_EXPORT)
SSLCAUTH	Tick for client authentication (i.e. The receiver channel will attempt to authenticate the sender channel's certificate). This is checked by default.

SSL Client Certificate Properties

The fields on this page hold information relating to the TLS/SSL certificate for the client or queue manager that will host the sender channel.

Field	Description
Cert. label	Read-only. The certificate label (e.g. ibmWebsphereMQQM1) NOTE: Labels are case-sensitive.
Common Name	The distinguished name common name (e.g. QM1)
Org. Unit	The distinguished name organizational unit (e.g. WebSphere MQ). Use a comma separated list for multiple OUs.
Org.	The distinguished name organization (e.g. IBM)
Locality	The distinguished name locality (e.g. Hursley)
State	The distinguished name state (e.g. Hampshire)
Country	The distinguished name country (e.g. UK)
Expiry	Certificate expiry in days. Defaults to 365.

SSL Server Certificate Properties

The fields on this page hold information relating to the TLS/SSL certificate for the client or the queue manager that will host the receiver channel or server connection channel.

Field	Description
Cert. label	Read-only. The certificate label (e.g. ibmWebsphereMQQM2) NOTE: Labels are case-sensitive.
Common Name	The distinguished name common name (e.g. QM2)
Org. Unit	The distinguished name organizational unit (e.g. FIT Team). Use a comma separated list for multiple OUs.
Org.	The distinguished name organization (e.g. IBM)
Locality	The distinguished name locality (e.g. Hursley)
State	The distinguished name state (e.g. Hampshire)
Country	The distinguished name country (e.g. UK)
Expiry	Certificate expiry in days. Defaults to 365.

Certificate Setup Choice

The fields on this page hold information relating to whether a Certificate Authority (CA) is used.

Field	Description
Self signed certificates	Create self signed certificates
CA signed certificates	Create certificate requests to be signed by CA (and optionally create the CA)

CA Setup Choice

The fields on this page hold information relating to how a Certificate Authority (CA) is used.

Field	Description
Use an existing CA	Create certificate requests, send them to an existing CA, and receive the signed certificates.
Create a CA	Create a CA, create certificate requests, sign the certificate requests, and receive the signed certificates.

CA System

The fields on this page hold information relating to the Certificate Authority (CA).

Field	Description
Host	The hostname (e.g. machine3)
Platform	The platform type (z/OS, UNIX or Windows)

CA z/OS Properties

The fields on this page hold information relating to the z/OS queue manager that will host the Certificate Authority (CA).

Field	Description
Keyring	The name of the RACF keyring that will be created (e.g. WMQCAKR)
CA ID	The userid which owns the keyring (e.g.WMQCAUSR)

CA UNIX/Windows Properties

The fields on this page hold information relating to the client or the UNIX/Windows queue manager that will host the receiver channel or server connection channel.

Field	Description
Key Database	The name of the key database file that will be created (e.g. */var/mqm/wmqca.kdb*)
Command	The GSKit command (runmqckm, gsk7cmd or gsk7capicmd). See Appendix B for more information.

CA gsk7capicmd Properties

The fields on this page hold information relating to the parameters used on the gsk7capicmd command on the CA machine.

Field	Description
FIPS	If set, the “-fips” parameter is used on gsk7capicmd commands.
Sigalg	Sets the “-sigalg <value>” parameter used on gsk7capicmd commands.

CA Certificate Properties

The fields on this page hold information relating to the TLS/SSL certificate for the CA that will sign the TLS/SSL certificates for the SSL client and SSL server.

Field	Description
Label	The certificate label (e.g. WMQCertAuth) NOTE: Labels are case-sensitive.
Common Name	The distinguished name common name (e.g. WMQ CA)
Org. Unit	The distinguished name organizational unit (e.g. Security Ops). Use a comma separated list for multiple OUs.
Org.	The distinguished name organization (e.g. IBM)
Locality	The distinguished name locality (e.g. Hursley)
State	The distinguished name state (e.g. Hampshire)
Country	The distinguished name country (e.g. UK)
Expiry	Certificate expiry in days. Defaults to 365.

Generated Instructions

The main field on this page holds the generated instructions.

Note: The WebSphere MQ SSL Wizard assumes that objects (e.g. the WMQ channel and TLS/SSL artifacts) are being created for the first time. Be aware that this will negate the need for some commands if objects already exist.

Chapter 4. Further tasks

There are many other tasks that should be carried out when using the WebSphere MQ SSL Wizard and WebSphere MQ SSL in general. Some of these are summarized below.

Passwords

Many GSKit commands require a password. Cryptographic security is largely dependent on password length and complexity - longer, more complex passwords are better. The commands generated by the WebSphere MQ SSL Wizard use the passwords *passclient, passserver, and passca.* You should replace the generated password strings with your own passwords.

Unreferenced Certificate Authority certificates

TLS/SSL key databases usually contain many default Certificate Authority signer certificates. All unreferenced Certificate Authority signer certificates should be deleted from key databases (e.g. *gsk7capicmd -cert -delete -label "VeriSign Class 3 Secure Server CA" -db my.kdb -pw password –fips*).

CRLs/OCSP

If using a Certificate Authority to sign certificates it is important to use CRLs or OCSP to prevent the use of revoked certificates. OCSP is generally considered a better option.

SSL key reset

SSL key reset minimizes the amount of encrypted data that can be decrypted if the secret key is discovered. The use of SSL key reset should be considered.

Certificate Name Filtering

On z/OS, message CSQX632I is output if no userid is associated with a remote certificate. This message indicates that the channel initiator userid is being used instead of a userid that relates to the remote certificate. Because the channel initiator userid is usually given a high level of access to queue manager resources, it should not usually be used by the channel. It is therefore recommended that the distinguished name of the remote certificate be mapped to a userid using certificate name filtering. See http://publib.boulder.ibm.com/infocenter/wmqv7/v7r0/topic/com.ibm.mq.csqzas.doc/sy12660_.htm

Chapter 5. Further information

Client Samples

Client application samples are supplied for the purpose of testing the SSL connection.

The client source files are found in directory *client_samples/src* and the client binaries are found in *client_samples/bin*. For examples of building the source, see Appendix C

Note: '*.exe'* binaries were built and are designed to be executed on the 32bit Windows platform.

FIPS

When FIPS is required, it applies to build-time administrative operations such as key database generation and certificate signing as well as to run-time functions such as the channel's cipherspec.

The build-time options are available only when selecting the gsk7capicmd. If gsk7capicmd is selected, the FIPS option is available on the following panels:

- SSL Client gsk7capicmd Properties
- SSL Server gsk7capicmd Properties
- CA gsk7capicmd Properties

A key database or certificate generated with non-FIPS methods cannot retroactively be made compliant. But key databases and certificates generated with FIPS-compliant methods can be used in both FIPS-compliant and non-FIPS-compliant systems. For these reasons the default is to always set the FIPS checkbox.

The runtime option is the SSLFIPS checkbox on the Channel Properties panel. If set, it controls restricts the list of SSLCIPH options available and sets the SSLFIPS queue manager attribute to YES.

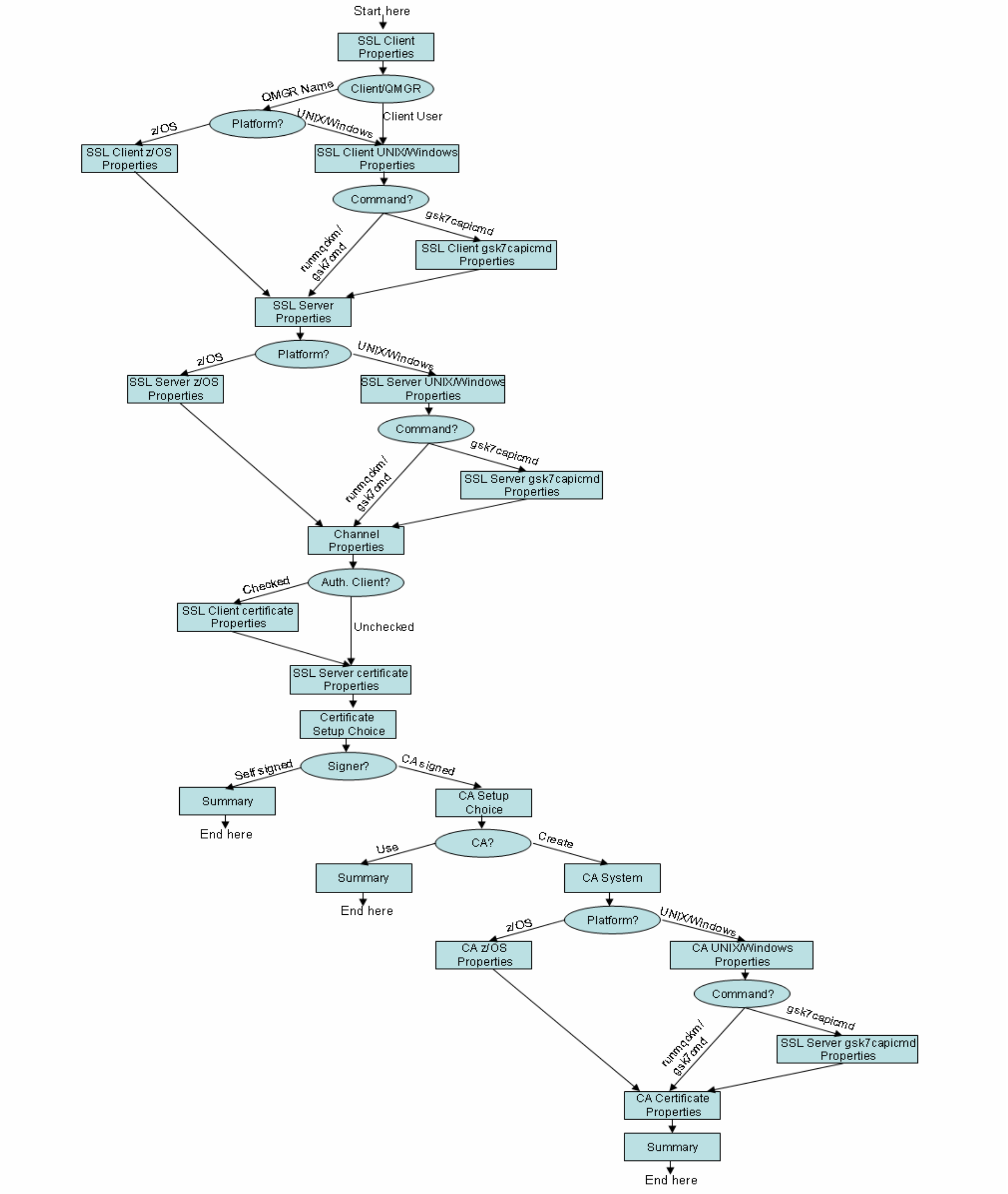
MD5

No MD5 hash algorithms are available in the WebSphere MQ SSL Wizard because they are considered cryptographically broken.

Name mangling

WebSphere MQ mangles queue manager names for directory paths (on UNIX and Windows), so the path generated for key databases may not be correct for the queue manager.

Appendix A – Page Order Diagram



Appendix B – GSKit command alternatives

Command	Platform	FIPS compliant	Notes
runmqckm	Windows	No	
gsk7cmd	Unix	No	
gsk7capicmd	Windows and Unix	Yes (using "-fips" parameter and subject to notes below*)	Supports "-sigalg"

* http://publib.boulder.ibm.com/infocenter/wmqv7/v7r0/topic/com.ibm.mq.csqzas.doc/sy11010_.htm

Appendix C – Building client samples

The following examples are included for convenience. For detailed build instructions, see the WebSphere MQ Infocenter.

Build SSLSample.java on Linux 32 bit:

```
javac SSLSample.java
```

Build SSLSampleJMS.java on Linux 32 bit:

```
javac SSLSampleJMS.java
```

Build SSLSample.c on Linux 32 bit:

```
gcc -m32 -o SSLSample.exe SSLSample.c -I/opt/mqm/inc -L/opt/mqm/lib -Wl,-rpath=/opt/mqm/lib -Wl,-rpath=/usr/lib -lmqic
```

Build SSLSample.java on Windows 32 bit:

```
javac SSLSample.java
```

Build SSLSampleJMS.java on Windows 32 bit:

```
javac SSLSampleJMS.java
```

Build SSLSample.c on Windows 32 bit:

```
cl /MT SSLSample.c mqic32.lib
```

Appendix D – Further references

Further WebSphere MQ SSL information…

- SupportPac MC6C - WebSphere MQ - How to Configure SSL: http://www-01.ibm.com/support/docview.wss?rs=171&uid=swg24006696&loc=en_US&cs=utf-8&lang=en
- SupportPac MH03 - WebSphere MQ SSL Configuration Checker: http://www-01.ibm.com/support/docview.wss?rs=171&uid=swg24014179&loc=en_US&cs=utf-8&lang=en
- WebSphere MQ Infocenter Security section: http://publib.boulder.ibm.com/infocenter/wmqv7/v7r0/topic/com.ibm.mq.csqzas.doc/sy10120_.htm
- WebSphere MQ Security in an Enterprise Environment Redbook: http://www.redbooks.ibm.com/abstracts/sg246814.html
- WebSphere MQ SSL: https://www-01.ibm.com/software/integration/wmq/ssl.html
- WebSphere MQ SSL “gotchas”: common mistakes and how to avoid them: http://hursleyonwmq.wordpress.com/2007/06/29/websphere-mq-ssl-%E2%80%9Cgotchas%E2%80%9D-common-mistakes-and-how-to-avoid-them/

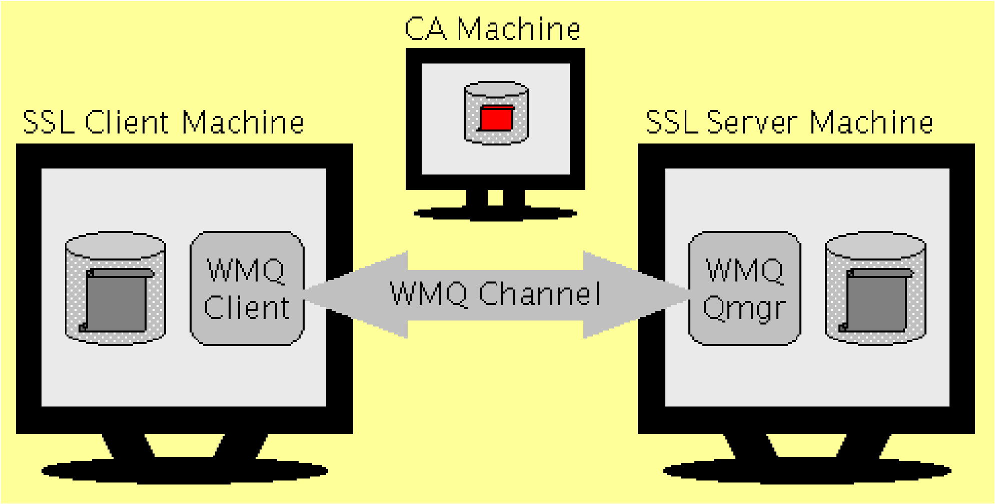
Appendix E – Example diagrams

Example 1

This diagram shows that a user has chosen…

- a WMQ client to queue manager connection (rather than a queue manager to queue manager connection).
- to authenticate the client, so there is a certificate (scroll) in the key database of the SSL Client.
- to create an internal CA (rather than use an external CA or self-signed certificates)

The diagram also shows that user is currently creating the CA certificate.

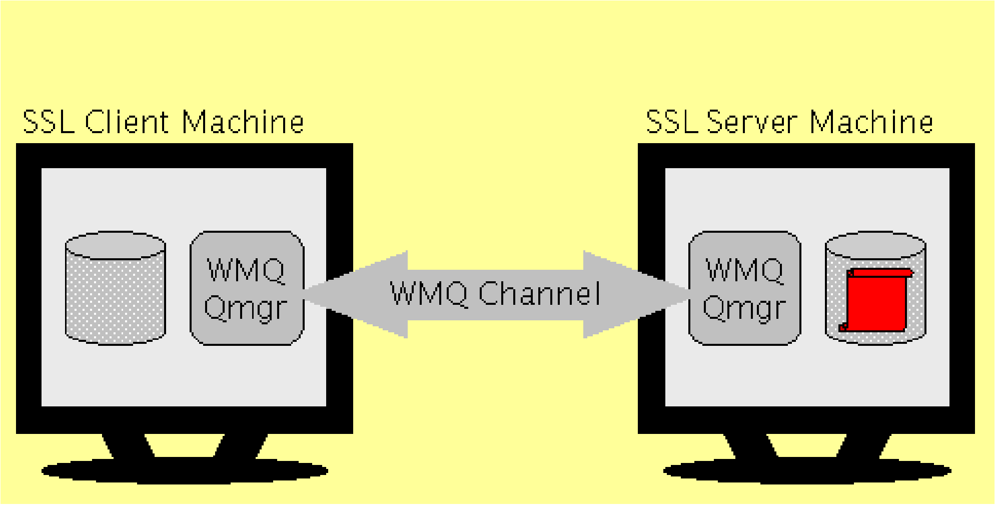


Example 2

This diagram shows that a user has chosen…

- a queue manager to queue manager connection (rather than a WMQ client to queue manager connection).
- to not authenticate the client, so there is not a certificate (scroll) in the key database of the SSL Client.

The diagram also shows that user is currently creating the SSL Server certificate.

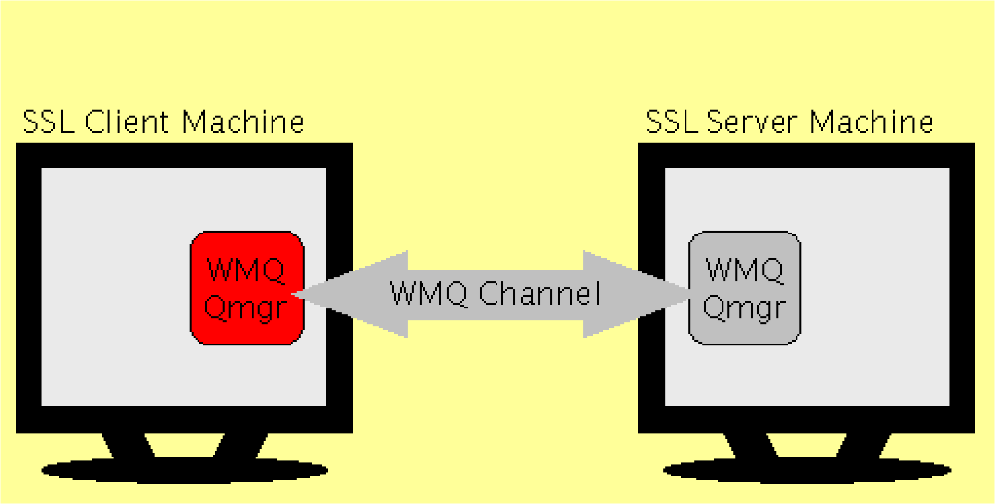


Example 3

This diagram shows that a user has chosen…

- a queue manager to queue manager connection (rather than a WMQ client to queue manager connection).

The diagram also shows that user is currently defining components relating to the SLS Client queue manager. And also that the user has not defined many components yet.



Appendix F – Acknowledgments

Many people have provided very valuable feedback on MO04, but special thanks go to Mike Horan, Neil Casey, and T.Rob Wyatt for their significant contributions made during development of V2.0.

Appendix G – Feedback

To report problems or suggest improvements please email Ian Vanstone (ivans@uk.ibm.com). When reporting problems please identify which version of MO04 you are using (See File->Help->About) and save and attach the data file (File->Save As) where possible. Note that the data file is much more useful than the generated instructions.