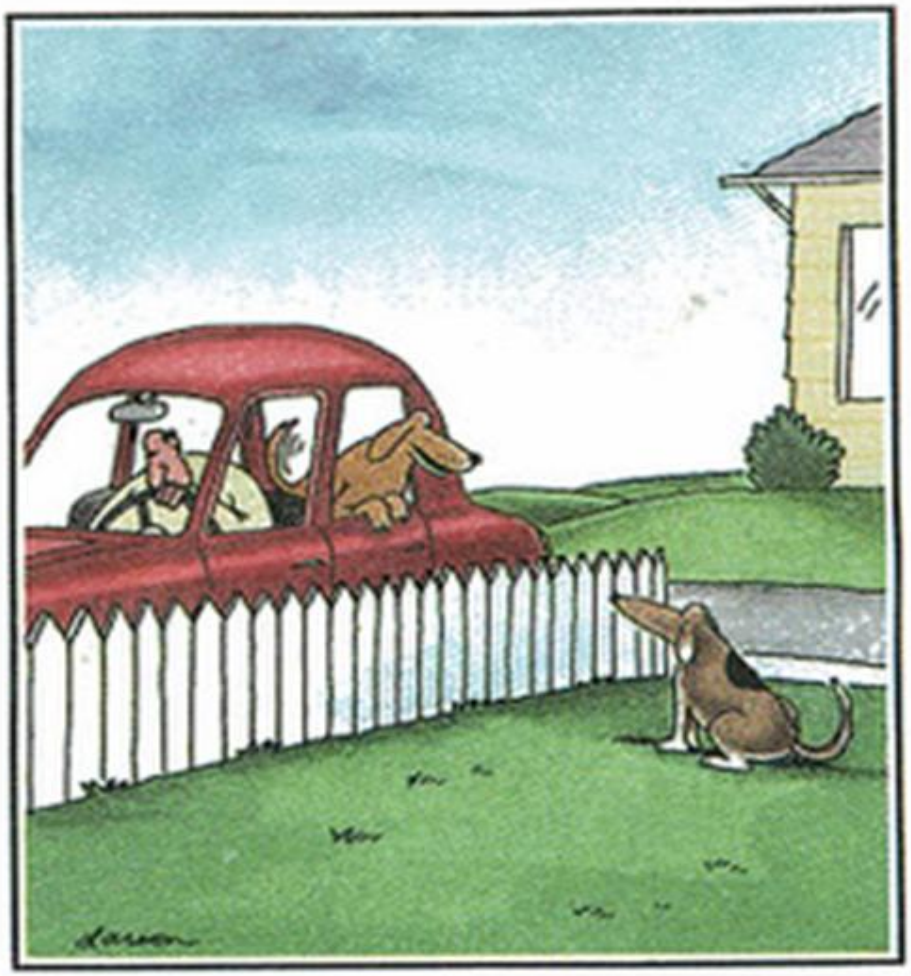
Addressing PCI w/Capitalware

A Customer Perspective



"Ha ha ha, Biff. Guess what? After we go to the drugstore and the post office, I'm going to the vet's to get tutored."

About Chris Hanna :

38 Years in IT

19 Years working w/ IBM MQ

USMC
USAA
MQSoftware
Southwest Airlines

christopher.hanna@wnco.com
(214) 792-1746

- 45 years of service, serving 97 stations around the world.
- 3900+ daily departures.
- Average more than 12 million customers enplaned per month in 2015.
- Served more than 106 million peanuts and more than 45 million pretzels in 2015.
- During 2015, 76.5 percent of our passenger revenues were booked via Southwest.com and Swabiz.com.
- More than 20 million people subscribe to Southwest's weekly Click 'N Save e-mails.
- During 2015, 85 percent of Southwest Customers checked in online or at a kiosk.
- Southwest was the first airline to establish a home page on the Internet. Initially, five Employees comprised Southwest's web site development team, and the site took about nine months to create.
- The "Southwest Shortcut" feature on Southwest.com is the first online tool that helps Customers find the lowest fare based on availability across an entire month.
- In addition to flights, Customers are able to make car, hotel, and complete vacation package reservations on Southwest.com.
- Southwest first launched an iPhone app in December 2009 and an Android app in 2011. New versions of both the mobile site and the apps were launched in 2013. In 2014, Southwest launched the capability for Customers to use a mobile boarding pass when traveling on Southwest flights.

SWA and IBM MQ

- Southwest Airlines Customer Service reps book 1.6 million reservations per month which represents just 23.5 percent of the 6.8 million total booked per month.
- Each booking represents a minimum of 7 MQ messages with PCI sensitive payload. This results in well over 48 million MQ PCI transactions per month.
- Beyond PCI, Southwest handles over 4 million MQ transactions per month touching things like baggage handling, aircraft departures and landings, aircraft maintenance, dispatch to cockpit communications and more.

PCI DSS and PCI Compliance

What does that mean?

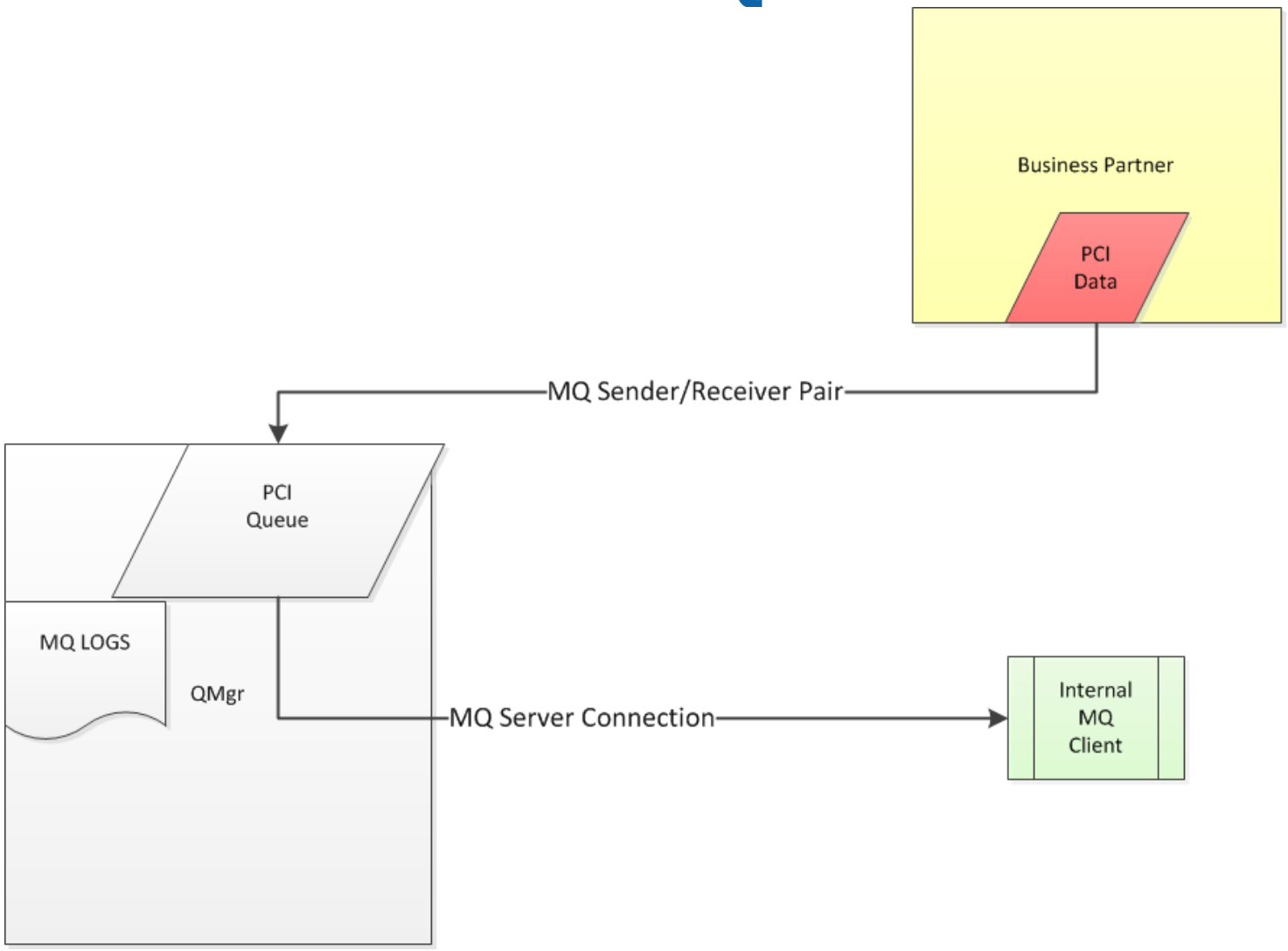
- **Payment Card** Industry Data Security Standard
  - A widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against the misuse of their personal information.

- **PCI Compliance**
  - PCI Compliance means the conformance of an organization to the PCI DSS through the following 6 tenets or objectives:
    - A secure network.
    - Protection of cardholder information wherever it is stored.
    - Protection of systems and servers against the activities of malicious hackers.
    - Access control to system information and operation.
    - Routine monitoring and testing of all networks to ensure that security measures and processes are in place, up-to-date and functioning properly.
    - A formal security policy must be defined, maintained and followed at all times and by all parties.

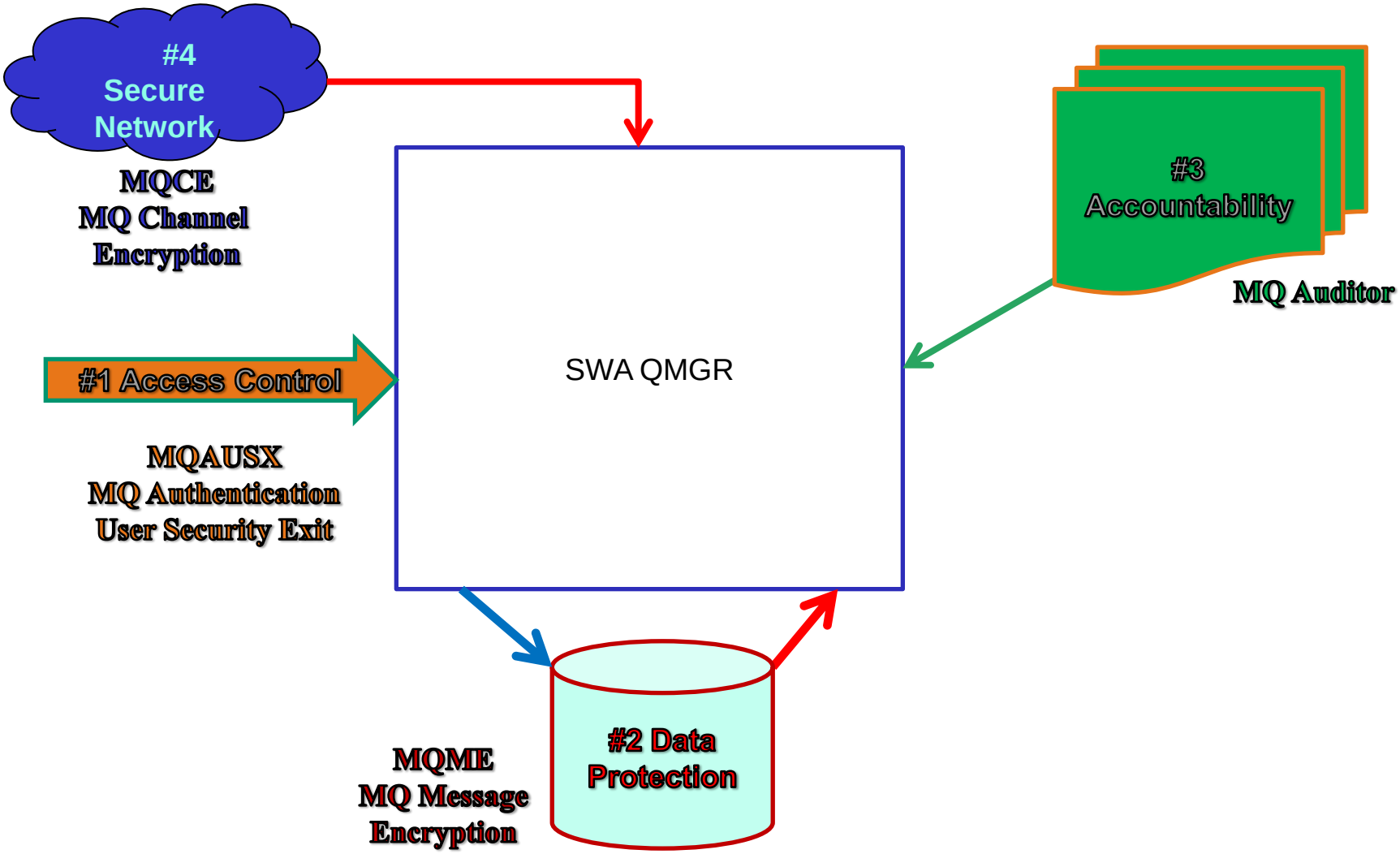
Why Capitalware?

- **Time and cost to develop and maintain supplementary MQ code**
  - Avoid the hassle of monitoring every security patch and fix pack coupled with the coding and testing tied with each patch that requires code changes.
  - Avoid regression testing and code changes for every new full release.
- **The solutions work**
  - Well documented.
  - Easy to implement.
  - Easy to maintain.
- **Excellent support**
  - Timely and appropriate response.
  - Receptive to customer needs and desired direction.
  - Effective communication regarding updates and new releases.
- **Cost, cost and cost**

The SWA MQ Picture



How Do We Achieve Our PCI Goals?



Capitalware for IBM MQ

A Deeper Dive

SWA utilizes four Exits from Capitalware

Two Channel Exits :

MQAUSX - for access control at the channel level

MQCE - for encryption of the data over the MQ channel

Note that Channel Exits are invoked at channel initialization.

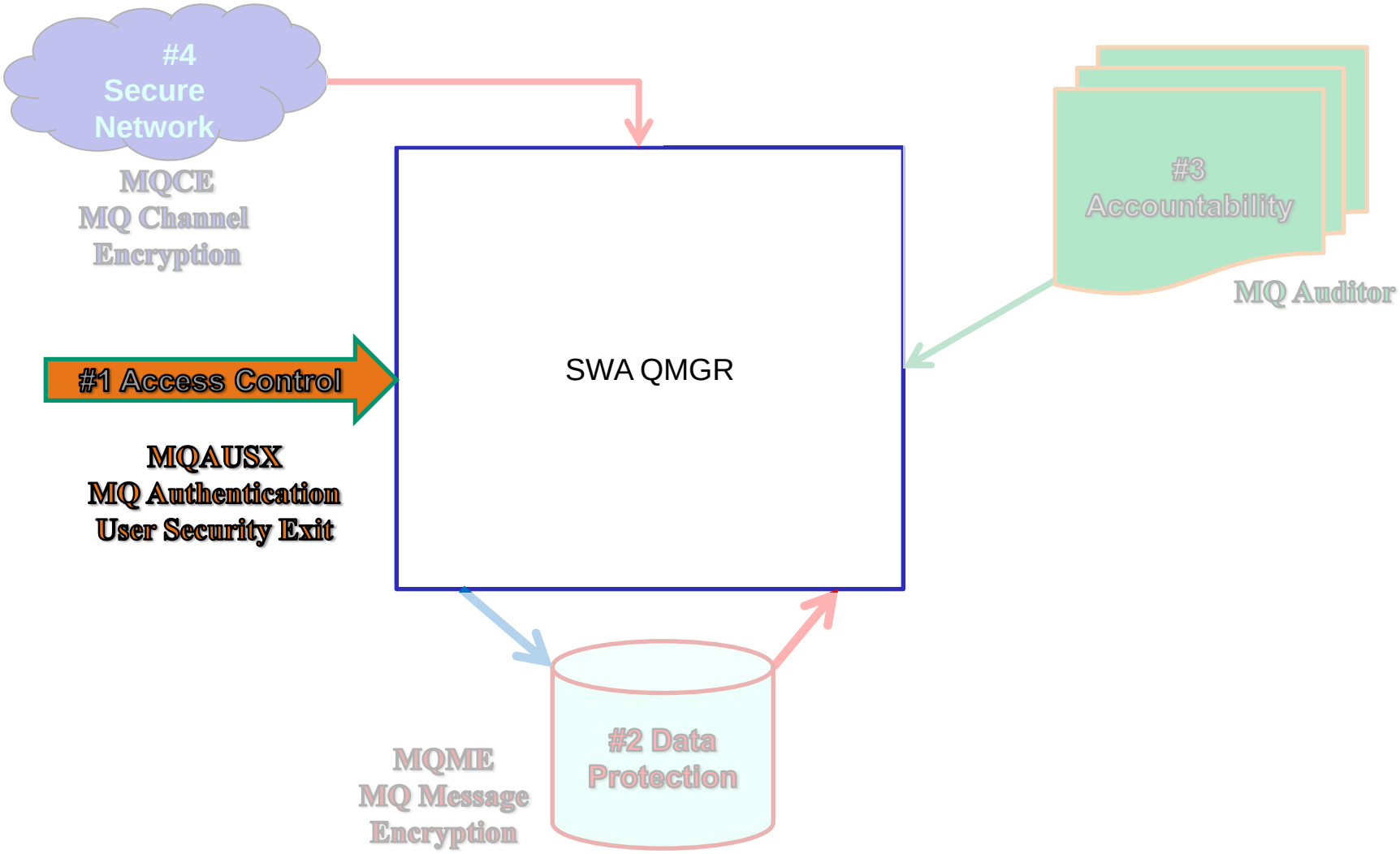
Two API (Entry Point) Exits:

MQME - for MQ Message Encryption

MQA - for Auditing specific API calls to specific queues

Note that API (Entry Point) Exits are loaded at Queue Manager startup via qm.ini or mqs.ini.

Channel Exit - MQAUSX



#1 Access Control

MQAUSX
MQ Authentication
User Security Exit

- MQ Authenticate User Security Exit (MQAUSX) allows us to fully authenticate a user who is accessing a WebSphere MQ resource.
- We utilize LDAP authentication, explicit IP address lists and explicit user lists in various combinations to control access via MQAUSX.
- We also limit the number of incoming channel connections based on the Server Connection channel name via MQAUSX.
- MQAUSX application or robotic id connectivity can be tested from command prompt via: testldapssl –u pcifeed –p xxxx –f pcifeed.ini (password needs to be checked out from appropriate cyberark safe).

#1 Access Control

MQAUSX
MQ Authentication
User Security Exit

- IBM MQ server connection channel requests are directed through MQAUSX via the SCYDATA and SCYEXIT properties in the channel definition.

  SCYDATA(/var/mqvnd/mqausx/ini/mqmgt.ini)

  SCYEXIT(/var/mqvnd/exits64/mqausx(SecExit))

- SCYDATA specifies the security data or details that should be used as input to the program/code specified in SCYEXIT, mqausx(SecExit).
- The .ini file provides the configuration specifics to be applied to the individuals or applications being authenticated.
- MQAUSX logs all attempts whether successful or not.

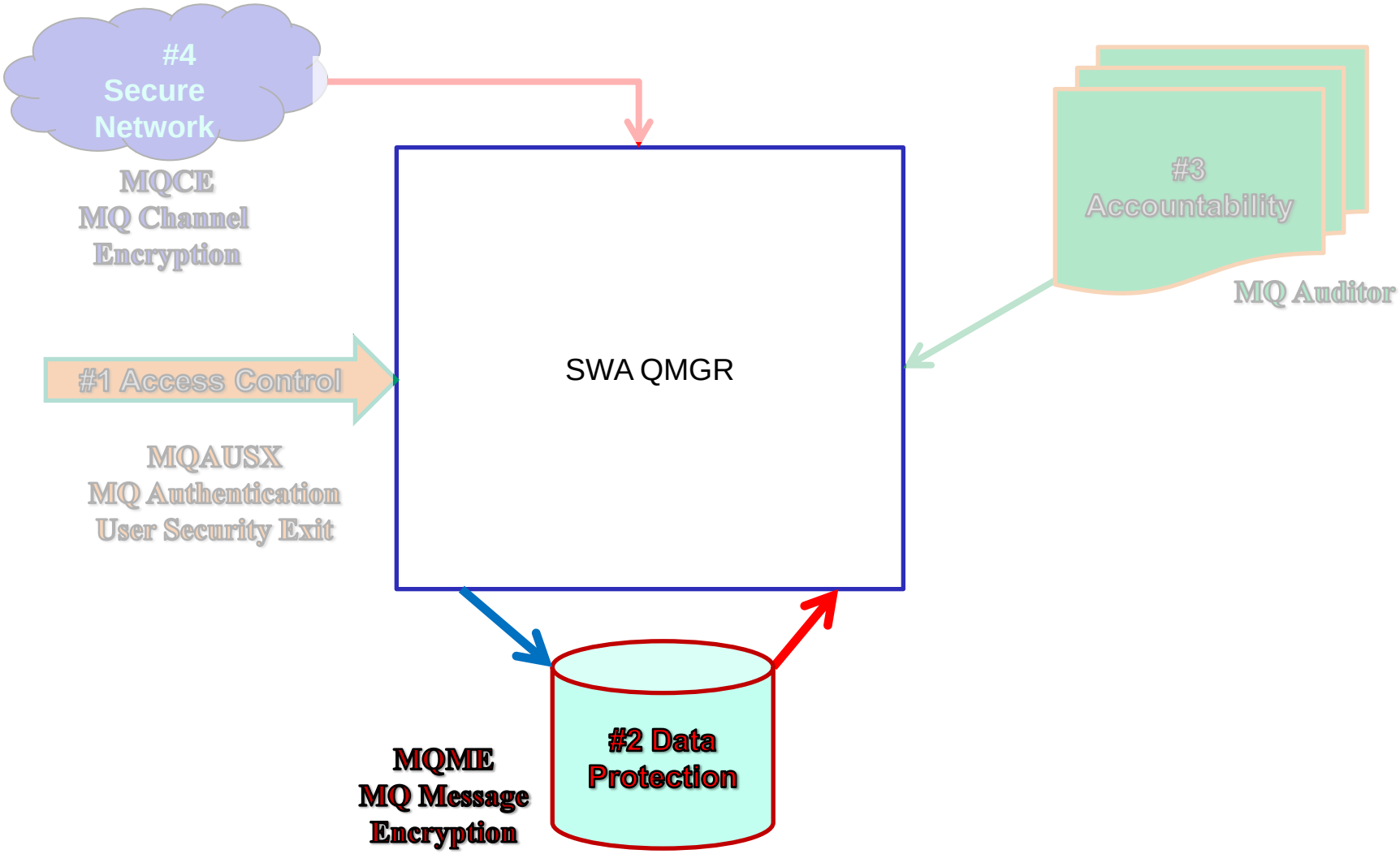
Sample .ini file for MQAUSX (LDAP Authentication)

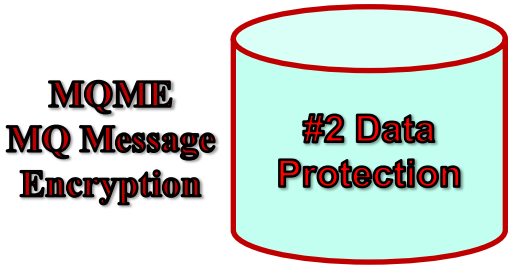
```
# /var/mqvnd/mqausx/ini/mqadmin.ini
# Last updated: 2010-01-05 13:04:37
LicenseFile=/var/mqvnd/exits64/mqausx_licenses.ini (Specifies the location of License file that contains costumer's license keys)
Description=MQAUSX user auth exit for DPCI*
LogMode=D                    (4 supported values Q/N/V/D, Quiet, Normal, Verbose or Debug)
LogFile=/var/mqvnd/mqausx/logs/mqadmin.log
UseLDAP=Y            ("Turn on" LDAP authentication)
LDAPHost=ldapsvrnm01.swadomain.com
LDAPPort=333
LDAPBaseDN=ou=employees,ou=people,o=our-ldap|ou=contractors,ou=people,o=our-ldap
LDAPTimeOut=10
UseLDAPSSL=Y         (Is your LDAP server connection over SSL?)
UseLDAPSSLCert=Y     (Does it require a CERT file?)
SSLCertFileName=/var/mqvnd/mqausx/bgsldaptr.der      (CERT file location)
SSLCertFileType=DER        (Cert file type)
```

Sample .ini file for MQAUSX (cont.)

```
Allowmqm=Y
UseMCAUser=Y
UseAllowUserID=Y                (Specify a list of allowed User IDs?)
AllowUserID=e0000;e112233;e4321;c19193                    (list of allowed IDs or patterns)
UseAllowIP=Y              (Specify a list of allowed IP addresses?)
AllowIP=172.18.66.82;172.18.66.66;172.18.66.81;172.18.66.73;172.18.66.48;172.19.169.231;172.18.66.89;172.18.66.46
 (Specifies list of IP addresses or an address pattern that will be permitted to initiate channel instance)
UseMCC=Y
DefaultMCC=30
MCCRedoMinutes=1
MCCRedoCount=1000
MCCEventWarnLevel=80
MCCGetTimeOut=3
MQAMCHL = 60
#
### The End ###
```

MQME


#4
Secure
Network
MQCE
MQ Channel
Encryption
#3
Accountability
MQ Auditor
#1 Access Control
MQAUSX
MQ Authentication
User Security Exit
SWA QMGR
#2 Data
Protection
MQME
MQ Message
Encryption



Provides encryption for MQ message data at rest, i.e. not on the wire

- Provides SWA the ability to encrypt PCI data on the queues AND stored in MQ transaction logs.
- Deployed to an MQ environment EXITS directory, /var/mqm/exits and /var/mqm/exits64, by default.
- Input to MQME is provided via an .ini file.

MQME Exit Stanza

ExitPath:

ExitsDefaultPath=/var/mqvnd/exits/

ExitsDefaultPath64=/var/mqvnd/exits64/

ApiExitLocal:

Name=MQAuditor

Sequence=1

Function=EntryPoint

Module=mqa

Data=/var/mqvnd/MQA/DTPCI.ini

ApiExitLocal:

Name=MQME

Sequence=2

Function=EntryPoint

Module=mqme

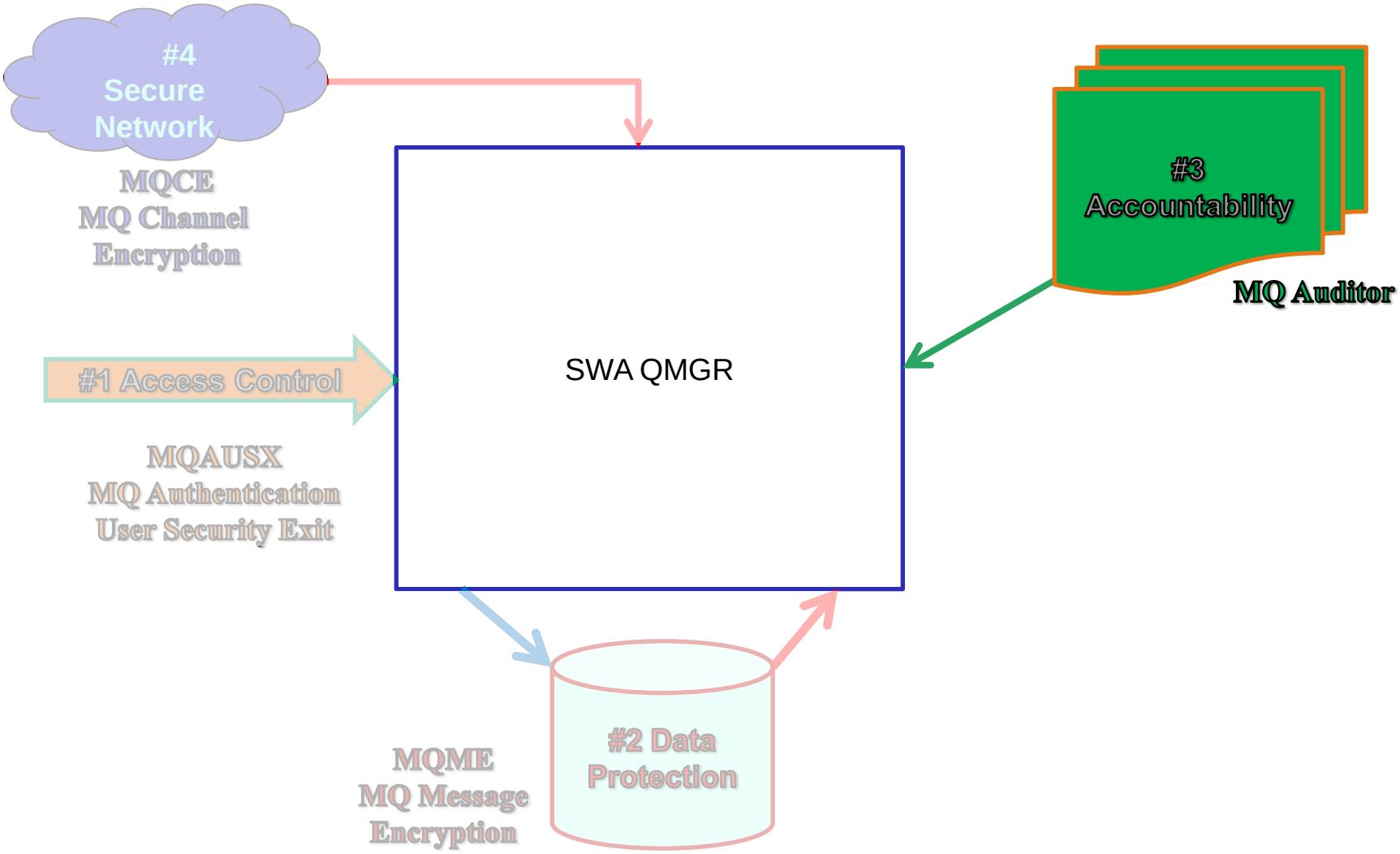
Data=/var/mqvnd/mqme/DTPCI.ini

Log:
LogPrimaryFiles=5
LogSecondaryFiles=1
LogFilePages=65535
LogType=LINEAR
LogBufferPages=0
Service:
Name=AuthorizationService
EntryPoints=13
ServiceComponent:
Service=AuthorizationService
Name=MQSeries.UNIX.auth.service
Module=/opt/mqm/lib64/amqzfu
ComponentDataSize=0
CHANNELS:
MaxChannels=1500
MaxActiveChannels=1500
Tcp:
Port=14XX
KeepAlive=yes

Sample .ini File for MQME

```
[default]
Active=Y
LogMode=D                    (4 supported values Q/N/V/D for Quiet, Normal, Verbose and Debug. Default is N)
LogFile=/var/mqvnd/mqme/DTPCI.log          (Specifies the location of the log file for this instance of MQME)
KeySize=256                  (Specifies the AES key size. Valid values are 128, 192 and 256. Default is 128)
LicenseFile=/var/mqvnd/exits64/mqme_licenses.in
#
[Q:SWA.PNRFEED.*]
UserIDs=pcifd;pcierr;xvendin
(Specifies authorized UserIDs so that MQME will decrypt the data when retrieved by an authorized user)
[Q:SWA.PCIFEED2.*]
UserIDs=pcifd;pcierr;mqm;vendin
[Q:SWA.PCIFEED1.*]
UserIDs=pcid;pcierr;mqm;vendin
# UserIDs=pcifeed
UseGroups=N
# Groups=mqm;RBTxxxx;RBTxxxx;genwasid
# GroupFile=/etc/group
#
#[Q:COH.PCIFEED.*]
#UserIDs=mqm;pcifd;pcierr
#
### The End ###
```

MQ Auditor


#4
Secure
Network
MQCE
MQ Channel
Encryption
#3
Accountability
MQ Auditor
#1 Access Control
MQAUSX
MQ Authentication
User Security Exit
SWA QMGR
#2 Data
Protection
MQME
MQ Message
Encryption

- **Audit/Track MQ API calls to any queue on any queue manager.**
- **SWA uses it to track very specific calls to very specific queues in support of PCI Compliance**
  - Specifically MQOPEN, MQINQ, MQPUT, MQPUT1 and MQGET calls.
- **Deployed to queue manager's default exit and default exits64 directory as module mqa.**
- **Input to mqa is provided via an .ini file.**
- **Audit files for MQ Auditor are located in /var/mqvnd/audit.**

MQ Auditor Exit Stanza

ExitPath:

ExitsDefaultPath=/var/mqvnd/exits/

ExitsDefaultPath64=/var/mqvnd/exits64/

ApiExitLocal:

Name=MQAuditor

Sequence=1

Function=EntryPoint

Module=mqa

Data=/var/mqvnd/MQA/DTPCI.ini

ApiExitLocal:

Name=MQME

Sequence=2

Function=EntryPoint

Module=mqme

Data=/var/mqvnd/mqme/DTPCI.ini

Log:
LogPrimaryFiles=5
LogSecondaryFiles=1
LogFilePages=65535
LogType=LINEAR
LogBufferPages=0
Service:
Name=AuthorizationService
EntryPoints=13
ServiceComponent:
Service=AuthorizationService
Name=MQSeries.UNIX.auth.service
Module=/opt/mqm/lib64/amqzfu
ComponentDataSize=0
CHANNELS:
MaxChannels=1500
MaxActiveChannels=1500
Tcp:
Port=14XX
KeepAlive=yes

Sample .ini File for MQ Auditor

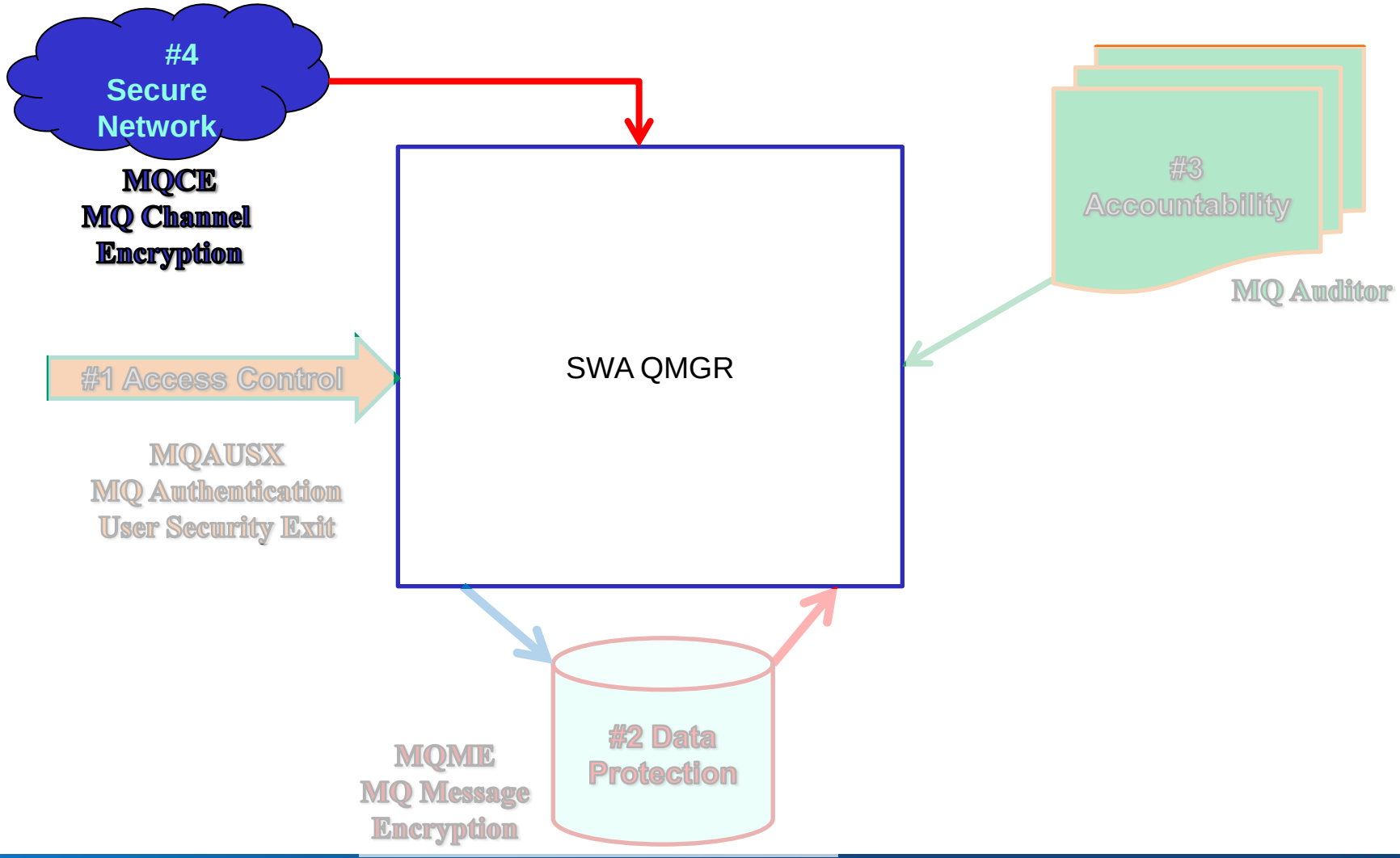
```
#
[default]
Active=Y
LogMode=Q
BackupLogFileCount=2
LogFile=/var/mqvnd/MQA/log/DTPCI.log
MonitorType=A                    (A=After API call, the other available option, B=Both before and after the API call)
MsgDataAsHex=Y                   (Display payload data specified in MsgDataLength, as hexadecimal)
MsgDataLength=25                 (Specifies some portion of the message payload to be included in the audit record)
LicenseFile=/var/mqvnd/exits64/mqa_licenses.ini
AuditPath=/var/mqvnd/audit/
AuditFileMaxSize=250
AuditArchivePath=/var/mqvnd/audit/archive/
ArchiveDays=90
ExcludeRC=2033;2009
ExitPath=/var/mqvnd/exits64/
ShowAPI=MQOPEN;MQGET;MQINQ;MQPUT;MQPUT1
Queues=*.FROM.VENDIN;*.FROM.VENDIN.*
#
### The End ###
```

Sample MQ Auditor Report Entry

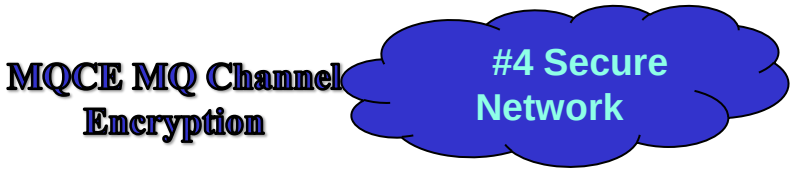
2013/01/23 06:35:26.149, MQXF_GET, A, PID=8907, TID=9, CC=0, RC=0,
UserId=mqm, HConn=20971549, HObj=4,
GMO_Options=MQGMO_NO_WAIT+MQGMO_NO_SYNCPOINT+MQGMO_BROWSE_NEXT+MQGMO_ACCEPT_TRUNCATED_MSG+MQGMO_PROPERTIES_FORCE_MQRFH2, GMO_WaitInterval=0,
GMO_ResolvedQName=COH.PNRFEED.FROM.RESVEND,
GMO_MatchOptions=MQMO_MATCH_MSG_ID+MQMO_MATCH_CORREL_ID,
MD_PutDate=2013/01/23, MD_PutTime=12:32:39.97,
MD_MsgId=414D512044544B303320202020202020018DFF650196A1420,
MD_Format=MQSTR, MD_MsgType=MQMT_DATAGRAM,
MD_Persistence=MQPER_PERSISTENT, MD_ReplyToQMgr=DPCI03,
MD_UserId=mqm, BufferLength=1000, DataLength=84,
MsgDataAsHex=6F6820776169742C20676F74206361727269656420617617 9,

The MsgDataAsHex string above, when converted="oh wait, got carried away"

MQCE


#4
Secure
Network
MQCE
MQ Channel
Encryption
#3
Accountability
MQ Auditor
#1 Access Control
MQAUSX
MQ Authentication
User Security Exit
SWA QMGR
MQME
MQ Message
Encryption
#2 Data
Protection

MQCE



- We initiate encrypted channel connections by employing the MQCE exit via the MSGDATA and MSGEXIT properties in a channel definition.

  MSGDATA(/var/mqm/exits64/mqce.ini)

  MSGEXIT(/var/mqm/exits64/mqce(CE))

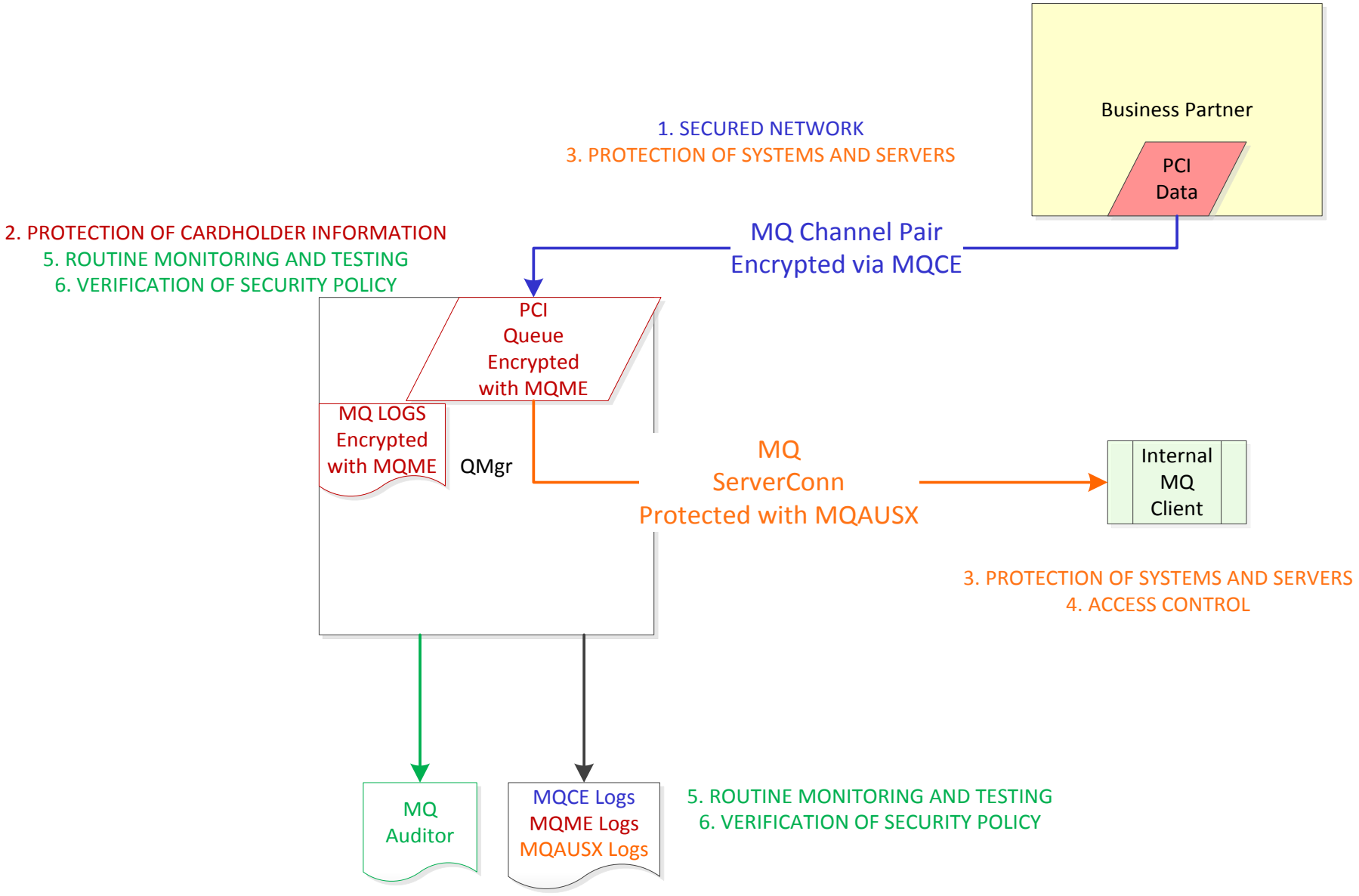
- MSGDATA specifies the exit and encryption details to be used as input to the program/code specified in MSGEXIT.
- The .ini file is an enterprise or universal configuration that will be applied to any SWA MQCE deployment.

Sample .ini File for MQCE

```
# /var/mqm/exits64/mqce.ini
# Last updated: 2016-08-16 13:04:37
LicenseFile=/var/mqex/exits64/mqce_licenses.ini

LogFile=/var/mqex/mqce/mqce.log

# What KeySize will you use? 128, 192 or 256

KeySize=256

# S, E, or B. What do you want to Perform, Sign, Encrypt or Both
Perform=E

#Debug log mode?
LogMode=N

#
### The End ###
```

Bringing It Back to PCI

1. **A secure network.**
   - MQCE
2. **Protection of cardholder information wherever it is stored.**
   - MQME
3. **Protection of systems and servers against the activities of malicious hackers.**
   - MQCE
   - MQAUSX
4. **Access Control to system information and operation.**
   - MQAUSX
5. **Routine monitoring and testing of all networks to ensure that security measures and processes are in place, up-to-date and functioning properly.**
   - MQ Auditor
6. **A formal security policy must be defined, maintained and followed at all times and by all parties.**
   - MQ Auditor


Business Partner
PCI Data
1. SECURED NETWORK
3. PROTECTION OF SYSTEMS AND SERVERS
2. PROTECTION OF CARDHOLDER INFORMATION
5. ROUTINE MONITORING AND TESTING
6. VERIFICATION OF SECURITY POLICY
MQ Channel Pair
Encrypted via MQCE
PCI
Queue
Encrypted
with MQME
MQ LOGS
Encrypted
with MQME
QMgr
MQ
ServerConn
Protected with MQAUSX
Internal
MQ
Client
3. PROTECTION OF SYSTEMS AND SERVERS
4. ACCESS CONTROL
MQ
Auditor
MQCE Logs
MQME Logs
MQAUSX Logs
5. ROUTINE MONITORING AND TESTING
6. VERIFICATION OF SECURITY POLICY

Where Can I Get This Stuff?

For more information, further documentation or trial versions of any Capitalware offerings - go to:

http://www.capitalware.com/products.html

For questions, sales or support contact:

Sales: +1-226-980-7307

sales@capitalware.com

support@capitalware.com

Questions & Answers

N

O

T

E

S