MediCal QAWeb Security Architecture

1.1. MEDICAL QAWEB CONCEPT

QAWeb consists of three components: QAWeb Server, QAWeb Relay and QAWeb Agent. The security architecture influences local and remote users interacting with QAWeb. The security of each component is discussed in this document. The critical part of the security is the communication through the internet and the authenticity of each individual component. Secured communication with https and certificates are the primary components of the security system.

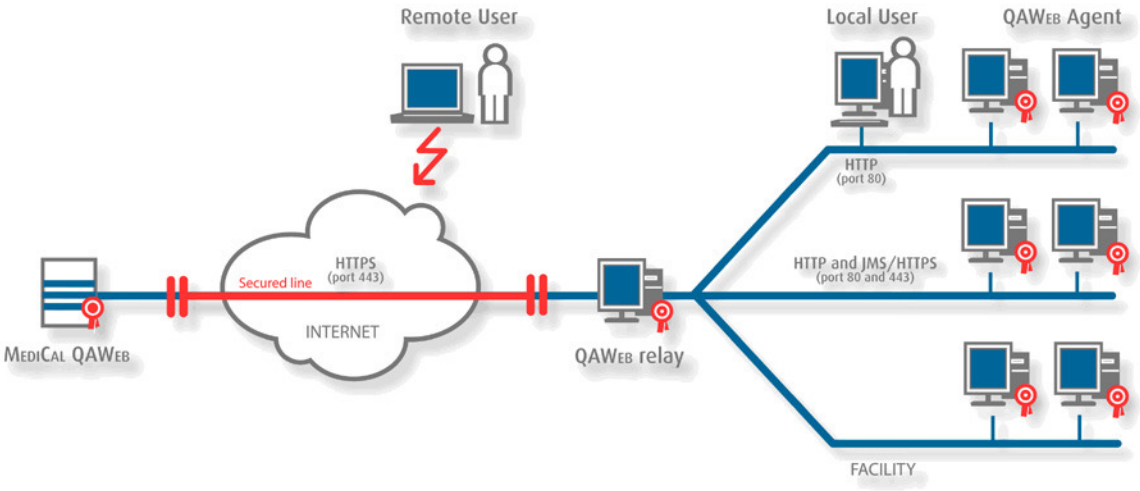

Figure 1 – Concept Overview of QAWeb Server, Relay and Agent

1.2. MEDICAL QAWEB SERVER

The MediCal QAWeb Server is hosted by Barco and is available on the internet. Through https://service.medical.barco.com you can browse to the QAWeb Server (e.g see remote user in figure 1). At that time a secure connection (128 bit encryption) is made through https (port 443) and a digital certificate is used. It is not possible to browse through the live QAWeb Server by using the http (port 80) protocol.
When accessing the QAWeb Server, a CA (certificate authority) issued certificate is used. Because the certificate is signed by a trusted authority (like VeriSign), there is no warning message in the browser of the user. Every facility also has its own unique certificate and its own user accounts. This prohibits access to other facility data.
The MediCal QAWeb Server is located in a secured environment and is only physically accessible by authorized Barco personnel.

1.3. MediCal QAWeb Relay

The QAWeb Relay is the central point for QAWeb in a facility. It is a software application running on a PC responsible for secure Internet communication with the QAWeb Server; it acts as a gateway for all QAWeb Agents in a facility. From within the facility, the QAWeb Relay allows access to the QAWeb Server through http (port 80), even when local workstations are not connected to the internet. The application framework also uses http and https in the communication between Agent and Relay.

The QAWeb Relay always takes initiative to contact the QAWeb Server, so no real remote access is enabled. The QAWeb Relay polls on a regular time base for new messages at the QAWeb Server.

The only prerequisite for the firewall between the Relay and internet is that https outbound traffic (on port 443) is allowed.

It is however recommended that the Relay is online and connected to the internet 24/7.

Although the application does not transmit any PHI (Personal Health Information), the Relay also contains an application data filter and a logging trail, so all data transferred by this machine can be traced afterwards and it should not generate any HIPAA (Health Insurance Portability and Accountability Act) concerns.

The MediCal QAWeb Relay is normally configured in one of the following two possible set-ups:

1.3.1. Set-up the MediCal QAWeb Relay in the PACS network

This is the default set-up and indicates there is no firewall between the PACS workstations (and thus the QAWeb Agent) and the Relay. This easily allows remote installation for the QAWeb Agent: the Agent installer is downloaded once, resides on the QAWeb Relay and is distributed from there to the PACS workstations connecting to QAWeb.

1.3.2. Set-up the MediCal QAWeb Relay in the DMZ

This set-up can be selected when there is no or limited access of the PACS network to internet. In this case, the IT department has to enable https traffic from the Relay to the server and should also make the Relay available for the PACS workstations (http and https). Additional adjustments are necessary to enable Remote installation.

1.4. MediCal QAWeb Agent

The QAWeb Agent runs on every workstation as a Windows Service. The QAWeb Agent contains links to the QAWeb Server by opening a browser window to the Relay, through http (port 80). The application framework uses http and https to communicate with the QAWeb Relay.

1.5. Summary of installation conditions

- Set-up a QAWeb Relay with continuous internet access for https port 443 to
  - 194.107.82.249 [service.medical.barco.com] and
  - 194.107.82.250 [secureservice.medical.barco.com]
- Enable outbound https (port 443) traffic on the firewall from the QAWeb Relay to the internet.
- Set-up a continuous connection between the PACS workstations and the QAWeb Relay (port 80 and port 443).
- Extra for remote installation support on the PACS workstations:
  - Enable remote desktop (My Computer => Properties => Remote => Remote desktop)
  - Disable Windows Firewall (Control Panel => Windows Firewall)
  - Enable the File and printer sharing exception in the Windows Firewall (Control Panel => Windows Firewall => Exceptions)
  - Disable simple file sharing (Explorer => Tools => Options => View)
- The minimum requirements for the QAWeb Relay are:
  - a Pentium 4 PC (3GHz)
  - 1GB of memory
  - hard disk of 80GB
  - Supported OS: Windows XP Professional or Windows 2003 Server
  - Pre-requisites (if you want to run the QAWeb Relay on an existing PC):
    - No Java Runtime Environment (JRE) already installed (verify this in the Add/Remove Programs section of Windows)
    - Ports 80 and 443 must be available, so no current web server should be running. So if you open a browser and run http://localhost:80 no valid page should be shown.
      Therefore, on Windows 2003 Server the service "World Wide Web Publishing service" must be stopped and set to manual.
    - If all conditions are not met, you can not use this PC for the MediCal QAWeb Relay software.
  - Be also aware that a pre-configured QAWeb Relay PC (hardware and software) can be ordered.

1.6. Conclusions

The MediCal QAWeb security architecture is based on feedback from a survey of IT and PACS administrators in medical facilities around the world. Its unique approach ensures the highest level of security for the facility itself and still enables a fast response time in case a service issue occurs by 'controlled' remote access.
It is set-up like a continuous VPN connection, but initiating the connection from within the facility. It can therefore be trusted for the transportation of fleet, asset and quality assurance management data (mainly display, graphic controller and test information) about the installed display base in the facility.

Explanation of used terms:

http **Hypertext Transfer Protocol** (**HTTP**) is the method used to transfer or convey information on the World Wide Web.

https **Hypertext Transfer Protocol Secure** (**HTTPS**) – is similar to http but provides authentication and encrypted communication ; it is widely used on the Web for security-sensitive communication, such as payment transactions, …

VPN A **virtual private network (VPN)** is a private communications network usually used within a company, or by several different companies or organizations, to communicate over a public network.

HIPAA The **Health Insurance Portability and Accountability Act (HIPAA)** was enacted by the U.S. Congress in 1996, one of the things it addresses, is the security and privacy of health data (important within the scope of this document).

CA In cryptography, a certificate authority or certification authority (CA) is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CA's are characteristic of many public key infrastructure (PKI) schemes.

PHI **Personal health information (PHI)** is all the information about an individual's health and health care, ranging from self-reported information about diet and exercise to clinical records and administrative/financial information. It also includes prescription information and test results. Health information liquidity is the ability of that information to move around, relatively friction-free, to where it is most useful and relevant.

DMZ Short for **demilitarized zone (DMZ)**, a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet