QlikView

QLIKVIEW MOBILE SECURITY

QlikView Technical Brief

Published: March, 2011

qlikview.com

QlikView Mobile Security

Mobile devices are convenient, versatile and, for many employees, they are indispensable. High adoption rates and reliance on mobile devices makes safe mobile data analysis a critical concern. However, mobile devices can easily be lost and that's why QlikView mobile clients have robust security means to secure sensitive business data.

QlikView's mobile clients leverage the entire security infrastructure of a typical QlikView enterprise deployment. This Technical Brief takes a look at the security features of the QlikView iPad touch-enabled Ajax client and uses an example implementation to explain some of the technical details.

This Technical Brief is a companion document to the QlikView Security Overview Technology White Paper, which deals in detail how a typical QlikView deployment addresses the question of security.

This brief will discuss the QlikView iPad client's security at these levels:

- Device
- Transmission
- Authentication and Authorization

It also includes an example implementation using Double Authentication

Device Security

One of the main security considerations for mobile BI solutions is not to store any business data on the device. QlikView mobile clients do not store data on the device. As such, there is no local copy to lose if the mobile device is stolen and the data only resides on QlikView servers within a secure enterprise environment, with access permitted only over the network for the correctly authenticated and authorized users.

Transmission Security

Transmission security refers to protection of data from unauthorized interception. The QlikView iPad client supports VPN connections where the communication between the client and the QlikView server, including the username and password, are encrypted.
The QlikView iPad client also supports HTTPS/SSL communication protocols. In the implementation example described below, HTTPS and Secure Sockets Layer (SSL) is used with server certificates installed on the IIS web server. In this specific case, tunneling is also enabled to encrypt the communication between IIS web server and QlikView server.

Authentication and Authorization

Authentication refers to the act of establishing or confirming the user as true or authentic. Authorization refers to the act of specifying access rights to control access of information to users. The QlikView iPad client leverages the existing authentication and authorization methods provided by QlikView Server (as described in the QlikView Security Overview Technology White Paper). There is nothing different from the iPad experience from a security perspective than a desktop browser.

For Authentication, the QlikView Server requires that users be authenticated by some external process, and that credentials granted by that process be communicated to the QlikView Server. QlikView supports authentication via Active Directory, third-party single sign-on (SSO) solutions (such as CA Site Minder or IBM WebSeal), as well as via digital certificates.

Once the user is authenticated, there are two authorization modes available: NTFS & DMS. NTFS mode relies on security features built in with Windows on the server side to secure access to QlikView documents through the iPad client. In NTFS mode, administrators control access to QlikView documents from the operating system itself rather than from QlikView. By contrast, DMS mode allows administrators to control access to QlikView documents centrally, within QlikView. (A detailed description of the differences between NTFS and DMS modes is contained within the QlikView Security Overview Technology White Paper).

Example Implementation — Double Authentication

The implementation example below demonstrates a real use case where security was applied to a QlikView deployment covering iPad devices. The security requirement is to achieve double authentication (i.e. using both user certificates and basic authentication against Microsoft Active Directory) with HTTPS/SSL connection. This is just one way to achieve a secure iPad implementation. There are other methods that could be used based on other security requirements. Figure 1 illustrates the Double Authentication example described below.

First Authentication

iPad supports digital certificates, giving business users secure access to corporate services. A digital certificate is composed of a public and private key pair, along with other information about the user and the certificate authority that issued the certificate. Digital certificates are a form of identification that enables authentication, data integrity, and encryption.

In this implementation example, digital certificates are used to securely authenticate users to corporate services. A Microsoft IIS web server in the ‘De-Militarized Zone’ (DMZ) domain is setup to provide one-to-one certificate mapping. When a user connects to the IIS site, IIS will request a user certificate which is already created on the iPad. The user will be prompted for a certificate and its public key is then submitted to the IIS server. The IIS server will compare this public key with the available public keys of which the administrator has granted access. Based on the result, IIS will either allow or disallow the user access to the QlikView Server.

If the user is allowed, IIS will encrypt the contents using a user public key and sends it back to the user. Now that the user has both keys, they will decrypt the contents sent by IIS using their own private key and will be able to start communication with the IIS server.

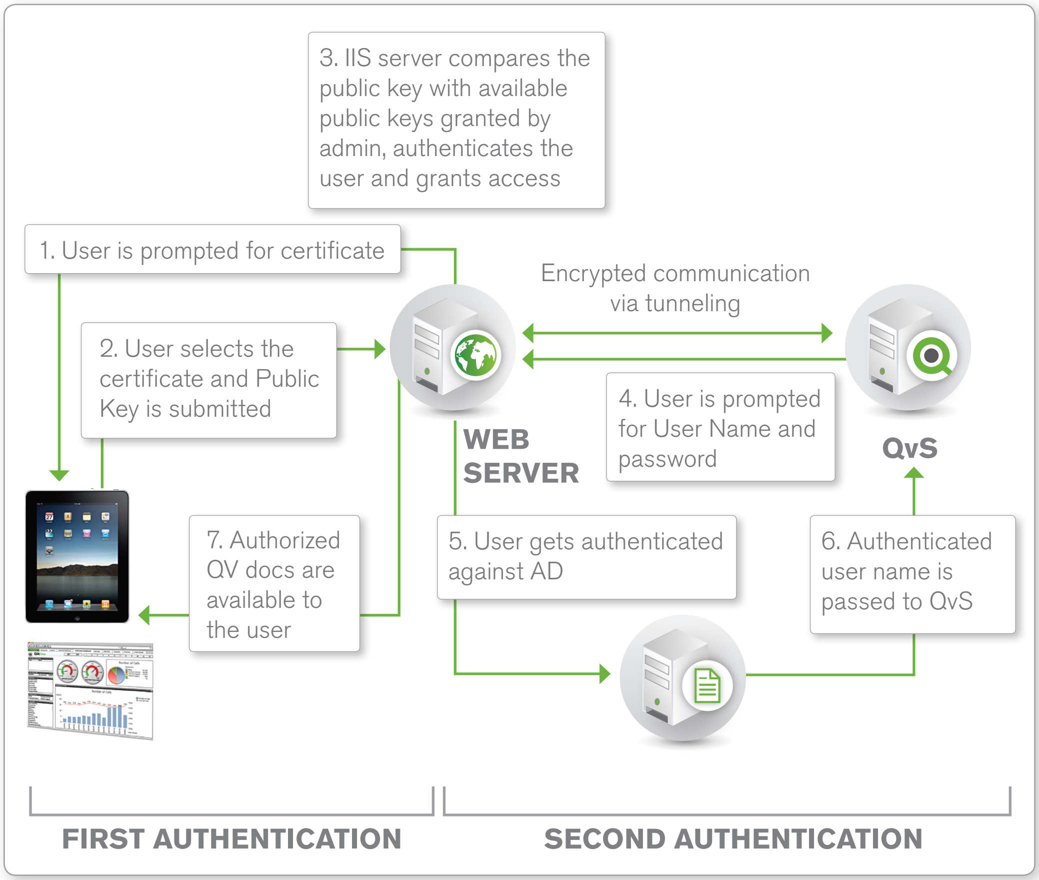
Second Authentication

The next step in this example is the second authentication. QlikView can be configured to provide a second layer of authentication to make sure that the user requesting access to the QlikView Server can be authenticated against the corporate security system (such as Active Directory or another LDAP, for example). As is normal, the user gets challenged for their credentials to be authenticated against the security system.

Authorization

The final step in the process is to give the authenticated user access to the authorized documents. This process is handled by the QlikView Server and is described in detail in the QlikView Security Overview Technology White Paper.

Figure 1: Double Authentication in a Mobile Environment


3. IIS server compares the public key with available public keys granted by admin, authenticates the user and grants access
1. User is prompted for certificate
Encrypted communication via tunneling
2. User selects the certificate and Public Key is submitted
WEB SERVER
4. User is prompted for User Name and password
QvS
7. Authorized QV docs are available to the user
5. User gets authenticated against AD
6. Authenticated user name is passed to QvS
FIRST AUTHENTICATION
SECOND AUTHENTICATION

Source: QlikTech