Fusebox Switch’s Use of Certificates and Testing Schemas v1.1

Server Certificates – Server Certificates are used for Server authentication from the Client Side, in a similar fashion of the “https” moniker in a browser. It ensures that the client (a client as used here is either a Point of Sale (POS), a Property Management System (PMS) or an e-Commerce application) is connected to the host that it intends to connect to and that the server says that it is who the client thinks it is connected to.

Presently, Fusebox uses a Symantec certificate. We are migrating to an Entrust provided certificate. This entails testing on the client (merchant) side to ensure that the certificate support structure on the client can support the Entrust server certificate.

Stunnel Implementations

Stunnel has already been tested, no further action is required.

Other Implementations

Normally, most clients reside on an OS (operating system) that encompasses an Internet Certificate Trust Store structure that has the common root and intermediate certificates and that the client uses this store for authentication.

Some clients, either run on an OS that does not have an Internet Certificate Trust Store or does not use the OS’ store. These clients normally use their own “Trust Store” or uses a PEM file (a file that has the server, intermediate and root certificates inside it).

Testing Protocols

The Elavon UAT environment has two (2) setups:

sha2.gatewaydemomoc.elavon.net – This URL uses an Entrust Server Certificate (all ports).

gatewaydemomoc.elavon.net – This URL uses a Comodo Server Certificate (all ports).

The essence of merchant (POS and PMS) testing is:

1. If the POS/PMS is using the OS’ Internet Certificate Store, the POS/PMS needs to be able to connect to URLs that use the current Symantec Server Certificate and the future Entrust Certificate.
    a. This is accomplished by sending test transactions to gatewaydemomoc.elavon.net (BAU) and then sending transactions to sha2.gatewaydemomoc.elavon.net. You will need to get your UAT Locator Values from your Solution Engineer.
        i. If both can be done with no changes (other than changing the endpoint URL), your POS/PMS implementation is ready for the certificate provider change.
        ii. If the first URL works and the second fails, then there problem with your OS’ Internet Certificate Trust Store and you will need to have a process to update your merchant’s computer to have the Entrust Certificate chains inserted in that

Certificate store. The certificate key file with the server certificate and chain is available from Elavon upon request.

2. If the POS/PMS uses a self-contained Internet Certificate Store (like a Java Key Store (jks) file), the POS/PMS needs to be able to connect to URLs that use the current Symantec Server Certificate and the future Entrust Certificate.
    a. This is accomplished by sending test transactions to gatewaydemomoc.elavon.net (BAU) and then sending transactions to sha2.gatewaydemomoc.elavon.net. You will need to get your UAT Locator Values from your Solution Engineer.
    b. If both can be done with no changes (other than changing the endpoint URL), your POS/PMS implementation is ready for the certificate provider change.
    c. If the first URL works and the second fails, then there problem with your self-contained Internet Certificate Trust Store and you will need to have a process to update your merchant's computer to have the Entrust Certificate chains inserted in that Certificate store. The certificate key file with the server certificate and chain is available from Elavon upon request.
3. If the PMS/POS uses stunnel to transact with Fusebox, no further action is required.