

Qatar Central Bank

SafeNet Hardware Security Modules selected to protect the state of Qatar's financial communications and transactions.

"In addition to the successful installation and deployment of the entire PKI infrastructure solution, we were more than pleased with the integration of Global Forte's time stamping authority with the Luna SP. We are now able to digitally sign any type of transaction in any impressive amount of time, and do it security"

Customer Profile

- The most advanced central bank in the GCC.

Business Challenge

- Looking for a solution for securing financial transactions, communications and digital identities between the QCB and the local banks in Qatar.

Solution

- SafeNet Luna PCI Hardware Security Module for securing the root key.
- SafeNet Luna SP Hardware Security Module used with Global Forte TSA for java based date and time non-repudiation.

Customer Profile

The Qatar Central Bank, is one of the most advanced central banks in the Gulf Cooperation Council (GCC) countries and is the regulatory authority for banks, exchange houses, investment companies, and financial companies within the state of Qatar.

Business Challenge

Qatar Central Bank was looking for a solution for securing financial transactions, communications, and digital identities. Existing MPLS networks resulted in the lack of secure communication between QCB and the local banks in Qatar for financial bank transfers. Additionally, there was no way to secure and manage the identities of the system users, in order to create reliable and secure non-repudiation characteristics.

Qatar Central Bank was looking for a complete end-to-end solution for their infrastructure that would secure the inter-bank network and provide:

- Secure local money transactions between local banks
- Provide local banks with a means for trusting and securing communications
- Offer users a single sign-on feature for local applications
- Have a reliable PKI based infrastructure for future applications that need security, integration, and non-repudiation

Solution

After reviewing several solutions in the market, QCB selected SafeNet. They chose SafeNet because they could get a complete end-to-end solution from one vendor that provided the most secure products available and could be easily integrated into the current infrastructure.

"When looking for a solution to handling the local money transactions of a country like Qatar, we felt we had to use the most advanced solution. We wanted it to be easy to integrate, manage, and the most secure. SafeNet was chosen because they were able to secure the root key of QCB Certificate Authority and provide the local banks' operators with a true end-to-end secure connection with two-factor authentication. This enabled the local banks' operators to securely submit their customers' transactions," said Global Forte partner for the QCB project.



SafeNet and its regional partner, Global Forte, deployed a complete PKI infrastructure using Microsoft Certificate Authority, SafeNet Luna Hardware Security Modules (HSMs), and the Time Stamping Authority. This infrastructure enabled QCB to issue certificates to system users for authentication, signing, and securing communications between local banks by signing and encrypting financial transactions, payments, and email communications. The PKI infrastructure deployed included:

- SafeNet Luna PCI HSM- the fastest, most secure HSM on the market, used for securing the QCB's Certificate Authority root key.
- SafeNet Luna SP HSM- the most secure, and easiest to manage and integrate HSM that is a web server embedded HSM that is used along with Global Forte's java based Time Stamping Authority (TSA) to achieve date and time non-repudiation.
- SafeNet High Assurance 2000 with SMC- hardware based solution for managing VPN connectivity providing secure VPN connectivity with two-factor authentication tunnels established between QCB and the Local Banks true end to end communication security.
- SafeNet iKey Tokens-provide strong authentication for securely generating user keys pairs and two-factor authentication for VPN connectivity as well as for signing transactions and exchanged data.
- SafeNet Axis- used for establishing single sign-on capabilities.

Conclusion

Shortly after deploying the SafeNet PKI Infrastructure, Global Forte realized immediate results including:

- A secure communication line between QCB and the local banks in Qatar
- The successful deployment of a Microsoft Certificate Authority to secure and validate system users and digital identities.
- A trusted means for the banks to time-stamp financial and payment transactions.
- A complete set of integrated solutions providing application integration.
- The convenience of a single sign-on option that allows the users to log-on into any application they specify automatically.
- The ability to launch a new service for local inter-bank transactions that was more cost effective compared to other alternatives, and provided for secure communications between banks.

In addition to the successful installation and deployment of the entire PKI infrastructure solution, the Qatar Central bank was more than pleased with the integration of Global Forte's TSA with the Luna SP. They are now able to digitally sign any type of transaction in an impressive amount of time, and do it securely.

About SafeNet

SafeNet is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property, and digital identities, and offers a full spectrum of products, including hardware, software, and chips. ARM, Bank of America, Cisco Systems, the Departments of Defense and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit www.safenet-inc.com/

