Sharjah Islamic Bank was in need of two-factor authentication, specifically SMS-based One Time Password (OTP) for their Internet banking and trading applications to prevent identity thefts.

**Problem**
- Ensure minimal change to application code-base.
- Enable the bank to do a phased migration of users to the new system.
- Allow the bank to adapt to changing threat levels by being able to introduce additional authentication mechanisms easily.

**Solution**
Odyssey deployed two-factor authentication for the bank's applications using Snorkel-TX, a transaction security gateway server that can seamlessly enable additional factors of authentication for end-users.

The deployment was completed in four weeks and the solution is currently live.

**Results**
- The solution has prevented the bank's customers from falling victim to identity thefts.
- The move to two-factor authentication has increased end-user confidence in using the bank's online services. This is evident from the increased online users since the deployment of SMS-based authentication.
- The solution was cost-effective for the bank, as the deployment required absolutely no change to the application code-base and was completed in record time compared to implementation of similar solutions in the market.
- The bank was able to do a phased migration of its users to the new system as originally planned.
- The bank will be able to scale and expand its services confidently in the future without having to worrying about security mishaps.
Sharjah Islamic Bank

Sharjah Islamic Bank hosts an internet banking application for their customers to access and manage their bank accounts from any geographical location through a web browser.

The application offers the customers a variety of options like viewing account details, fund transfers, remittances and payments for online purchases.

Sharjah Islamic Financial Services is an associated concern hosting a web application for its customers to trade online.

Both applications use the traditional mechanism of requesting 'username' and 'password' for identifying and authenticating users. By establishing a secure SSL channel wherein information sent back and forth is encrypted, the information shared between the customers and the application server is protected.

The secure channel is established by a 2048 bit RSA key associated with the SSL certificate issued to the bank by a Certifying Authority. In addition, the login page to the application offers a virtual keyboard for keying in the password as an additional protection mechanism against keystroke loggers.

Need For Enhanced Security

Although both the applications used SSL for privacy, the applications and the users were still susceptible to a wide range of attacks such as phishing, Man-In-The-Middle, Man-In-The-Browser, Pharming etc, that could potentially result in identity thefts.

With a growing list of online threats, the bank felt an immediate need to take preventive action and provide Two Factor Authentication (TFA) to protect both the customers and itself.
Case Study

Solution Requirements

1. **Enabling two-factor authentication with minimal change to the application server was SIB's primary goal.**
   The bank wanted to enhance authentication mechanisms for the applications, but not at the cost of changing the existing user experience.

   Besides, the bank envisioned the security module as a separate entity similar to a firewall protecting the network behind it.

2. The bank wanted to deploy SMS-based One Time Passwords (OTP) for TFA. With changing threat levels, the solution should be able to support other types of authentication methods in the future.

3. The migration of Internet Banking users was expected to happen in phases, which meant that both users with TFA and no TFA had to co-exist until TFA could be enabled for all the users.

4. The solution should also enable end-users to self-register for the service.

Odyssey Snorkel-TX

Snorkel-TX is a powerful transaction security gateway server capable of enabling additional forms of authentication for web-based applications. It sports a range of second factor authentication mechanisms such as digital certificates, One Time Password using hardware tokens/software tokens and SMS.

Snorkel is positioned in front of the application server and intercepts requests from the user. Based on the configuration, Snorkel then enables the appropriate second factor of authentication for the user.

The solution can be deployed without any changes to the existing technology infrastructure.

Why Snorkel-TX?

The zero-touch deployment model of Snorkel was a significant factor in the bank's decision to employ Snorkel. Practically zero coordination from the application vendor is required, as there is no need for changes to the application.

Odyssey Technologies Ltd
Consequently, the deployment time is also considerably reduced. This model of deployment fulfills the bank's requirement for a separate security component that is isolated from the rest of the application infrastructure.

The solution supports the co-existing of users with different authentication levels, thus enabling the bank to migrate its users to the new model in phases, just as the bank envisioned.

The application developer is also free to upgrade or change the application code-base in the future, without affecting Snorkel. Changes in the application would require only configuration changes in Snorkel. This will ensure that the application can scale comfortably in the future without the need for changes to the security infrastructure.

Additionally, the option to upgrade users to higher-levels of authentication methods like certificate-based authentication by making simple configuration changes was attractive to the bank, since it would be advantageous when the bank expands its services in the future to include high-value transactions.

The bank could also introduce other methods of authentication like hardware/software One Time Passwords by making configuration changes in Snorkel. Again, this ensured that the solution could withstand changing needs of the bank and its users.

Since the bank was rapidly expanding, it was important that the IT infrastructure reliably support its growth. A product like Snorkel-TX that can adapt to growing needs with only a few configuration changes fit well into the bank's business strategy.

The implementation was carried out in phases and was completed in four weeks by two onsite resources.

The bank was initially skeptical about the short implementation schedule. However, the implementation proceeded on time and the system was live at the end of four weeks. Odyssey continues to provide post-production support to SIB remotely, through e-mail, phone and remote login.
Case Study

### Implementation Highlights:

Odyssey is a Chennai-based company and has no local presence at Sharjah, despite which it took only two onsite resources and 4 weeks to complete the entire implementation. This stands testimony to Odyssey's efficient planning and implementation methods.

Since going live, remote support has been more than adequate to manage post-production activities, demonstrating the company's ability to implement and support solutions world-wide.

### Results

- The solution was successfully deployed within the scheduled time frame.
- The migration of users to the new system of authentication was trivial. Since most of the bank's customers were extensive users of the mobile phone and familiar with SMS technology for sending and receiving messages, user-experience remained unchanged.
- Since the move to SMS-based OTP authentication, the bank has realized cost-savings due to more customers using the online system confidently.
- The success of the solution in preventing identity thefts, combined with the cost-effective implementation has enabled the bank to confidently explore new horizons in providing online services for its customers.

To learn more about solutions from Odyssey Technologies Limited, visit [www.odysseytec.com](http://www.odysseytec.com) or e-mail [info@odysseytec.com](mailto:info@odysseytec.com).