ODYSSEY
cryptic by intent

Odyssey Snorkel FAQ

Odyssey Technologies Ltd

Odyssey Snorkel FAQ

1. What is Odyssey Snorkel-TX?

Snorkel-TX is a PKI-based transaction security server that enables two-factor authentication, access control, privacy and digital signature capabilities for web applications.

2. What security functionality does Snorkel provide?

- Snorkel enables the highest form of authentication using digital certificates. Customers can also opt for One Time Passwords.
- Snorkel provides intricate page-level access control.
- Snorkel establishes a secure client and server authenticated SSL channel to protect the privacy of transactions.
- Non-repudiation of transactions is achieved by enabling the end user to digitally sign the transactions, form submissions and file uploads.
- Data integrity is achieved using hashing algorithms.

3. Why should I buy Snorkel-TX? I already use password-based authentication for my web application(s)?

Password based authentication is not strong enough. Users generally choose a weak password which is easy for them to remember; this makes the passwords susceptible to attacks. There are many cheap password cracking software and services available online. So even amateurs can make use of them to hack into the websites easily.

A second or even third authentication factor helps to secure the application more strongly.

Snorkel first identifies the user by crosschecking his identity with that of the backend application. Snorkel then provides additional authentication factors using digital certificates and/or OTP. The customer can choose authentication factors depending on the risk profile of the various users. Migrating to a higher level of authentication can be achieved just by a few configuration changes.

Currently, Public Key Certificates for authentication is the most secure form of authentication technology available. Services which need authentication on a smaller scale can opt for OTP, because such situations do not justify the cost of digital certificate based authentication.

One Time Passwords, which cannot be reused or replayed offer a simple and elegant alternative to digital certificates and can be easily deployed using Snorkel-TX.

Snorkel's OTP options include hardware tokens that comply with OATH standard, mobile phones, desktop applications, and SMS.

Benefits:

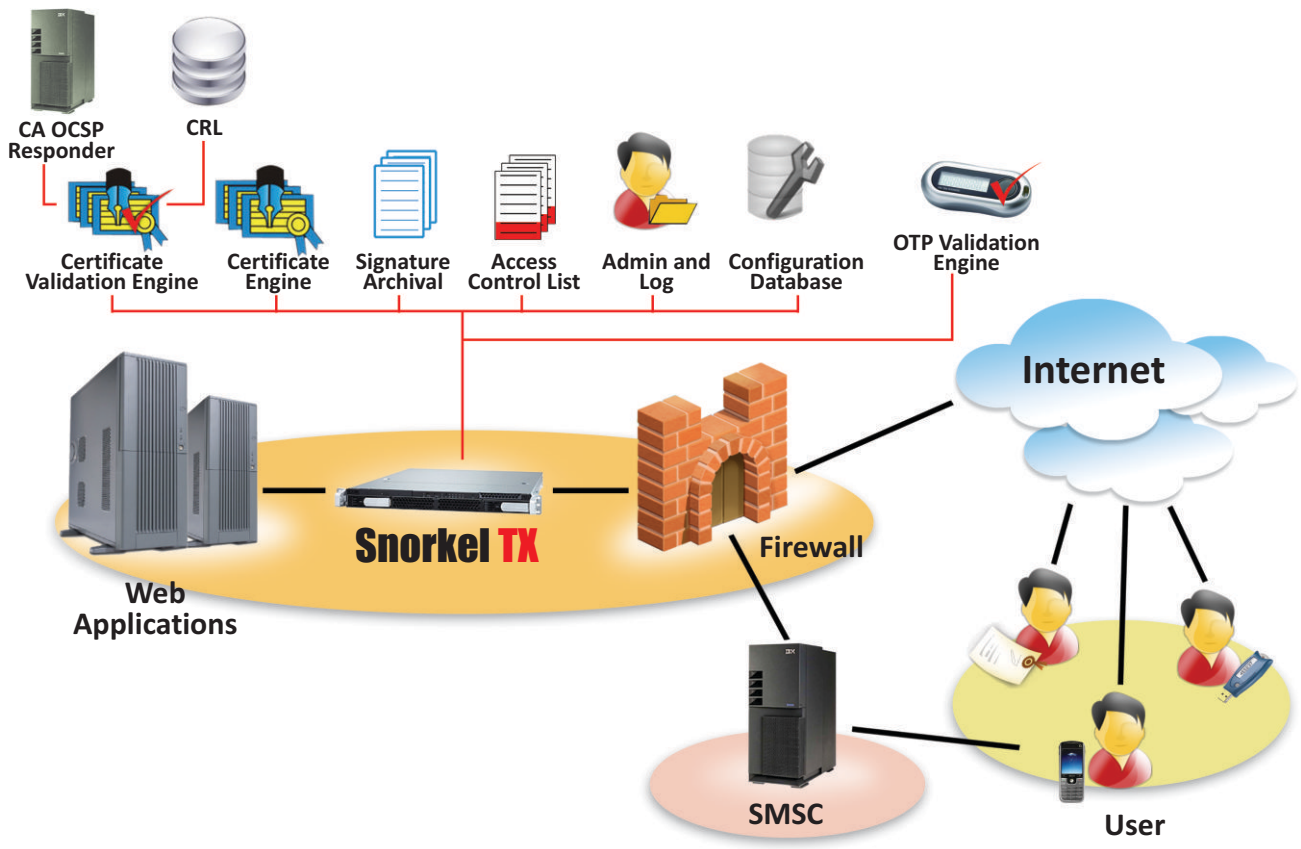
- High performance
- Able to seamlessly handle multiple kinds of authentication for very large volumes of users
- Enhances trust in the applications

4. How does Snorkel benefit my business?

- Snorkel does not require integration or changes to existing web applications or databases. So there is minimal downtime in business continuity.
- The solution can be configured to suit changing business needs. New security features can be added without making huge investments.
- Snorkel is cost-effective because:
  - It has a short implementation time, being plug-configure-play.
  - It protects more than one application at a time.
  - Implementation does not depend on third party applications or databases.
  - It has a native Certification Authority to issue digital certificates.
  - Simple, intuitive user interface with a steep learning curve.

5. How is Snorkel installed/deployed?

Snorkel is positioned between the web application and internet. All requests to the application pass through snorkel.



6. How many users can Snorkel support?

Snorkel supports both certificate and OTP users based on license limits.

7. How many applications can Snorkel support?

Snorkel can support up to eleven applications.

8. How does Snorkel support security policy enforcements?

Snorkel supports security policy enforcements by allowing for policy-based configuration and management of administrators and users.

Administrators

- Snorkel supports tiered administration with varying levels of access rights.
- All administrator activities are digitally signed and logged for accountability.

Users

- User management includes user addition, deletion, suspension, and reactivation.
- Access rights for users are managed through configuration. Users can be allowed or denied access to specific pages within specific web applications.
- User transactions are digitally signed and logged for audit trail.

9. How does Snorkel bring accountability to web applications?

Snorkel does extensive logging of administrator and user activities.

- All administrator activities are digitally signed and logged along with the date, time and nature of the activity. This creates a detailed audit trail and allows for tracking and verification of administrator activities.
- All user activities including user login time, logout time, pages accessed etc. are logged along with the date and time.
- User transactions are digitally signed and archived for non-repudiation.
- The reporting module shows comprehensive reports of administrator activities, user activities, and digital signatures. The reports can be filtered using multiple criteria.

10. How is Snorkel better than other similar products in the market?

Snorkel	Other Products
Snorkel is plug-configure play and can be deployed with zero changes to the existing web application. Therefore, deployment is quick.	Most PKI products in the market require integration with the application which can be expensive and resource intensive, not to mention costly.
The solution can be configured to work with any business application regardless of the application's functionality, platform or vendor.	Usually suited only for specific business applications. Often, integration or changes to the web application may be necessary to make the solution work.

▪ Changes or upgrades in business applications can be accommodated effortlessly in Snorkel by only making configuration changes.	▪ To accommodate changes in business application, the business would need a well qualified API integration team permanently, which scales up the cost.
▪ Snorkel provides both OTP based authentication and certificate-based authentication. Users can be switched from one form to the other effortlessly.	▪ Most products currently available in the market do not support both forms of authentication. They are often fragmented in terms of the security features offered, driving up the total cost of security.
▪ Both server-to-server and server-to-client transactions can be protected easily.	▪ Mostly protect only server-to-client transactions.

11. What kind of web applications does Snorkel protect?

Odyssey Snorkel

Snorkel can be used to provide comprehensive security for almost all web applications including those employed in banking, trading, defense, dealer management, vendor management, inventory control, customer relationship management, supplier relationship management, e-mails and file sharing, ERP, education, etc.

12. What is Snorkel-BX?

Snorkel-BX

Snorkel-BX is a PKI-enabled security gateway server that facilitates secure transactions between two or more entities.

13. How does Snorkel-BX manage security?

In a typical deployment scenario, Snorkel-BX is made the front-end to the web applications involved in transactions.

Depending on the requirement, the server can either accept HTTP data from the web application or pick up data to be transferred from a folder located in the web application.

The server establishes a secure communication channel using SSL with the entity on the other end which could be either a Snorkel-TX server or a Snorkel-BX server. This makes Snorkel-BX ideal for business communications that require privacy.

Snorkel-BX authenticates itself to the other end by means of a digital certificate. Snorkel-BX authenticates the other entity by requesting for that entity's digital certificate and verifying the same.

The server can be configured to sign specific data/transaction that is being sent to the other entity. Similarly, Snorkel-BX is also capable of verifying the signature and archiving the same when it receives signed data/transaction. The archival of digital signatures enables offline verification and non-repudiation of transactions.

14. What is the difference between Snorkel-TX and Snorkel-BX?

Snorkel-BX is deployed in a server-to-server environment and is capable of acting as either a server or client, depending on what the transaction calls for. Snorkel-BX authenticates the entities on the other end using digital certificates. Snorkel-BX is typically deployed for securing B-to-B transactions.

Snorkel-TX is deployed in server-to-client instances where the client could be either a thin client like a browser or a thick client like a Snorkel-BX server. The server is capable of authenticating its clients using both digital certificates and one time passwords. Snorkel-TX is typically deployed for security B-to-C transactions.

ODYSSEY TECHNOLOGIES LTD.
5th Floor, Dowlath Towers, 63,Taylors Road, Kilpauk, Chennai – 600 010, India.
Tel : +91 44 26450082, 26450083, 43084070, 43084080
e-mail: info@odysseytec.com