Odyssey Snorkel-TX

Odyssey Snorkel – TX is a robust and powerful transaction security server, deployed to protect web applications. The server instantly enables two-factor authentication, access control, non-repudiation and integrity for web applications, regardless of application vendor, architecture, or technology.

Need for Security

Businesses are increasingly adopting web-based transactions, resulting in a wider target market, lower cost of business, and increased profits.

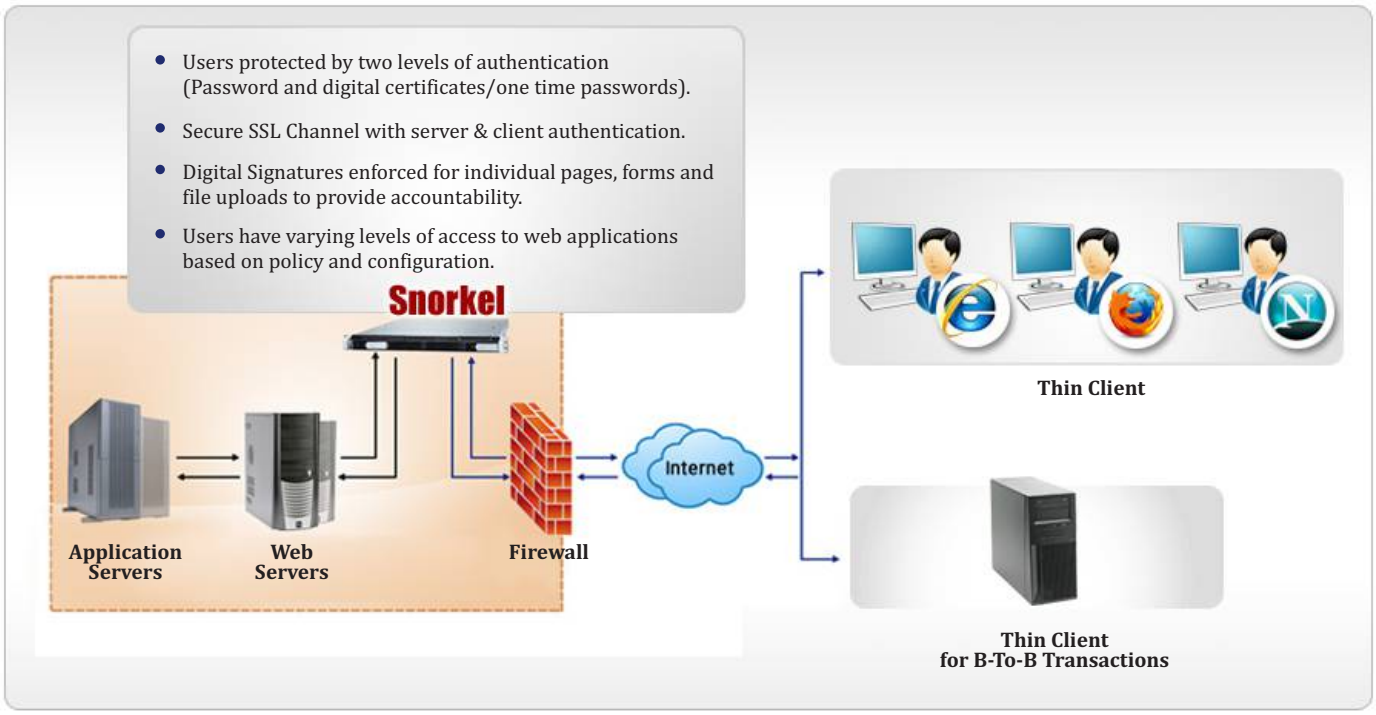
Unfortunately, online transactions are rife with security threats. With the availability of powerful password cracking software, even novice users can now crack thousands of passwords in a very short time, typically hours.

Other attacks that enable unauthorized access to web applications and result in identity thefts include phishing attacks, pharming attacks, and various social engineering techniques. The existence of such threats behooves web applications to use defense in depth and implement at least a second factor of authentication to protect against intruders.

In addition to having a sound authentication mechanism, web applications have to protect transactions against privacy breeches, unauthorized changes to data, and repudiation. The lack of effective security measures can cost businesses, especially those operating in the financial and retail sectors huge fiscal losses, and also a mitigation of trust among customers.

Odyssey Snorkel-TX

Odyssey Snorkel-TX provides comprehensive security coverage to web applications by enabling reliable two-factor authentication, access control, non-repudiation, and integrity.



Two-Factor Authentication

Snorkel – TX provides multiple options for secure two-factor authentication including various One Time Password (OTP) techniques as well as certificate-based login.

OTP Options

- Mobile OTP
- SMS OTP
- Token-based OTP
- Software-based OTP

One Time Password is a convenient form of authentication technique that is ideal for low-risk transactions. User adoption of One Time Passwords is fairly easy since it makes use of familiar technologies such as mobile phones.

Certificate-based Authentication

Certificate-based authentication is currently the most secure authentication technique and is primarily recommended for high-value transactions. Snorkel-TX comes with a certificate generation engine that enables enterprises to register and issue digital certificates to customers.

With options for phased migration of end users to either type of authentication technique, Snorkel-TX provides the flexibility to handle multiple types of users and implement risk-based security.

Fine-grained Access Control

Snorkel-TX provides policy-based, fine grained access control that enables enterprises to control access to various web services. Snorkel-TX can simultaneously protect up to 11 web applications. There is hence a need for limiting end-users to specific applications. Even within specific web applications, users may have to be provided with limited access to specific services and web pages.

Snorkel provides a simple, yet powerful configuration interface that allows administrators to configure fine-grained access control rules.

Two-way authenticated SSL

Snorkel provides a secure channel for communication by enabling client and server authenticated SSL. This ensures that all communication between the application server and client is protected from unauthorized access and viewing.

Integrity and Non-repudiation

Snorkel-TX enables end-users to digitally sign transactions using their signing certificates. Snorkel verifies signatures on the transactions and also archives the signatures for offline verification. This protects the transactions from non-repudiation.

Zero Touch Implementation

Snorkel-TX brings a comprehensive set of security features to web applications without compromising business continuity. The server can be configured to work with any web application and instantly enable PKI functionality. Implementation of Snorkel-TX typically takes only a few weeks as opposed to months in the case of PKI integration.

Standards Compliance

Component	Standard
• Digital Certificates	• X. 509 V3
• Account based authentication	• ANSI X9.59
• Digital Signatures	• PKCS #1 V2
• Digital Signature Storage Format	• PKCS #7
• SSL	• SSL V3, TLS
• Public Key Algorithm – RSA	• PKCS #1 V2, RFC 2437
• Symmetric Algorithms – DES, 3DES	• FIPS 46-3, FIPS 81
• Hashing Algorithm SHA1, SHA2	• FIPS 180-1, FIPS 180 - 3
• Pseudo Random Number	• X 9.17
• Smart Cards / Readers / TokensGenerator	• ISO 7816, PC / SC 1.0

Features

- Authentication using One Time Passwords – Software, mobile, SMS, Token
- Inbuilt digital certificate issuance engine
- Authentication using X. 509 V3 Digital Certificates
- Fine-grained page-level access control
- Support for upload of signed forms and files
- Support for both thin clients (browsers) and thick clients (Snorkel-BX Servers)
- Support for crypto smart cards, tokens, and HSM (optional) for key storage
- Support for PKCS #12 files and browser stores
- Support for certificate validation using CRL and OCSP client
- Support for certificates from external CAs
- Archival of signatures for offline verification
- Hot standby deployment for failover switching
- Comprehensive backup and restore
- Comprehensive reporting
- Support for SSL V2, SSL V3, TLS

ODYSSEY
Cryptic by intent

ODYSSEY TECHNOLOGIES LTD.
A to E, 8th Floor, Gee Gee Emerald, 312, Valluvar Kottam High Road, Nungambakkam, Chennai - 600034, India.
Tel : 91 44 28222455/ 28218982, Fax : 91 44 28271559
e-mail : info@odysseytec.com