WebSeal (Secure End-to-End)

BLUE FORTRESS

End-to-End Encryption

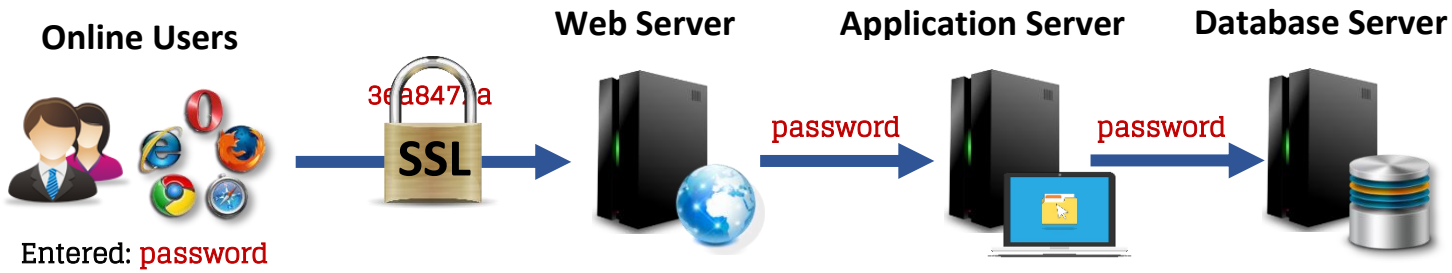
With many organizations moving their businesses to the internet, many rely heavily on SSL to protect customers' data. While SSL performs encryption on transactions between the browser and server, data remain vulnerable as soon as it ends at the web server. Hence, valuable and sensitive information is vulnerable to security threats such as sniffing, interception, theft and alteration while travelling across the network. Therefore, WebSeal was designed to ensure that sensitive data remain encrypted from the point of data entry to the application server where data is being processed.

WebSeal End-to-End Encryption also helps organizations to manage keys to encrypt new data in a secure environment (SafeNet ProtectServer HSM) before storing it in the database. Hence, the actual data is never exposed anywhere but inside the FIPS 140-2 level 3 hardware security module where data needs to be processed. End-to-End Encryption of WebSeal running inside the SafeNet ProtectServer HSM is responsible for all cryptographic operations which results in better performance in organizations' business operations on the application server.

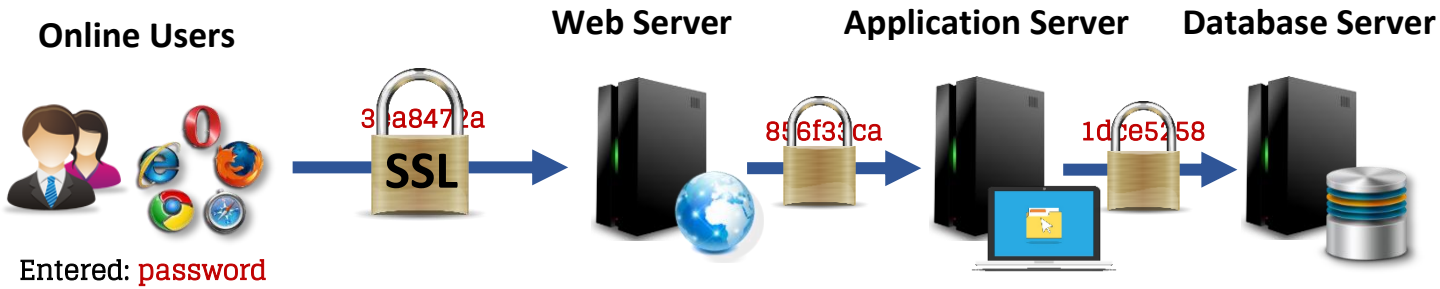
Benefits of End-to-End Encryption

- Prevents sensitive data from being exposed throughout business operation.
- Ensures data is inaccessible in plaintext at any point.
- Defend against any attempts of external and internal hacking .
- Provides highest level of security to organizations without sacrificing any performance of business operations.
- A secure environment to perform cryptographic operations and platform to manage encryption keys.

Web Services with SSL only



Web Services with **End-to-End Encryption**



WebSeal (Secure End-to-End)

BLUE FORTRESS

1 Secure E2EE

WebSeal – Secure E2EE

WebSeal (Secure End-to-End Encryption) is a solution deployed inside SafeNet ProtectServer HSM (Hardware Security Module) to aid applications to achieve a true end to end encryption, from the web browser to the webserver, application server and database server, offering a level of security unavailable from software alternatives. WebSeal ensures that no sensitive data is accessible in clear while travelling over the network throughout an application's operation cycles.

WebSeal serves as a bridge between the web browser, web server, application server and the database server to securely transmit data over the network by performing cryptographic operations inside a secure environment without sacrificing the performance of business operations. This allows developers to secure sensitive data without having to become cryptographic experts as all crypto operations are done by WebSeal.

SafeNet ProtectServer Hardware Security Module

SafeNet ProtectServer (PSE) HSM is a Hardware Security Module that allows customized application to be executed within the secure environment of the HSM. Its programmable flexibility became the perfect option for WebSeal to carry out a true end to end encryption to protect sensitive data and credentials such as password, credit card numbers, PIN, etc.

SafeNet PSE HSM is tamper resistant security module and generates true random numbers based on factors that are non-reproducible. SafeNet PSE HSM is capable of performing up to 1500 RSA signings per second.

Cryptographic Algorithms

- Any hashing and encryption algorithm supported by the SafeNet PSE HSM

Type of Application

- Executable Functional Module hosted by the SafeNet PSE HSM

Database

- Database hosted by existing server

Performance

- Up to 1500 RSA signings per second

Operating System Supported

- Any OS with a browser to access web application

End-to-End Encryption

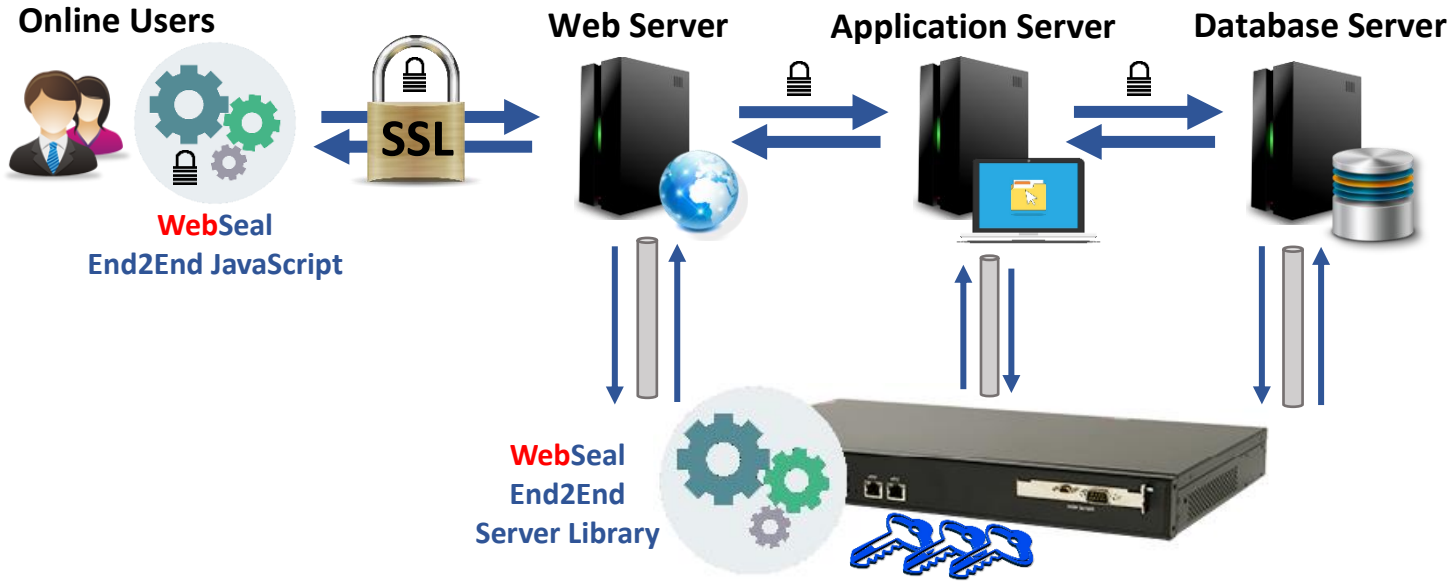
- Every sensitive data involved will remain encrypted throughout the business operation

Keys Management

- Keys generated by the Hardware Security Module solely for WebSeal which is unexportable from the appliance
- Allows key rotation to further improve security

2 How it Works?

- When users access the web application via SSL, e.g. Online Banking, a RSA public key inside a Hardware Security Module (HSM) loaded from the back-end server will be embedded into the web page to encrypt the password/PIN entered.
- Encrypted data will travel through the internet via SSL from the web browser to the web server.
- Upon receiving the encrypted data in the web server, the data will be sent to the HSM to be decrypted along with a random session key which was generated and encrypted in the web browser.
- Once the session key is verified by the HSM, decryption of the actual data will happen and application will receive the plaintext to be processed.
- When user requests for data to be retrieved from the database, eg. bank credit details, photos, videos, etc, the same session key stored in the HSM will be used to encrypt the data back to the web browser.
- All sensitive data and information remains encrypted throughout the entire process, immediately after data entry and data retrieval from the database.



enquiry@blue-fortress.com

www.blue-fortress.com

© Blue Fortress 2016. All rights reserved.