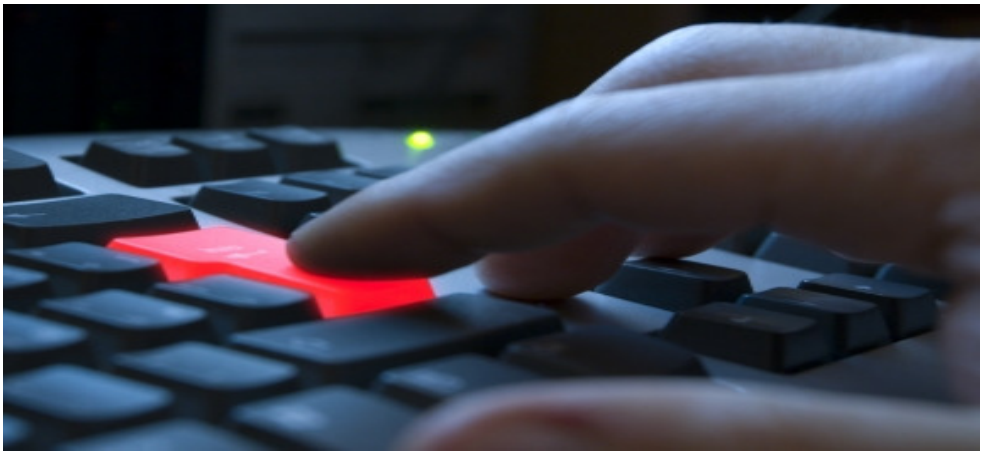
SUNNIC®

E-Trust Guard

End to End Encryption for Credentials



Security Inadequacies of SSL

- It only secures the connection to the web server, thus securing transactions partially.
- Data flowing across the web server are vulnerable to internal risks
- Does not prevent system administrator from replacing one user password with one of another user

Advantages of End-to-End Encryption

- Selective Encryption Only sensitive data needs to be encrypted . Thus only a small data packet need to be secured during transmission.
- Small file size client library for download
- Light weight processing. The client and server components employs the minimum but sufficient set of encryption and security features — AES and RSA key.
- Cost savings. No need for SSL certificates
- Flexible changing of key. For better security , the key can be changed when required.

"... the encryption security pertaining to the customer's PIN and other sensitive data should be maintained end-to-end where possible. This means the encryption process is kept intact from the point of data entry to the final system destination where decryption and/or authentication takes place."

MAS Internet Banking Technology Risk Management Guidelines , Version 2.0

The Challenge

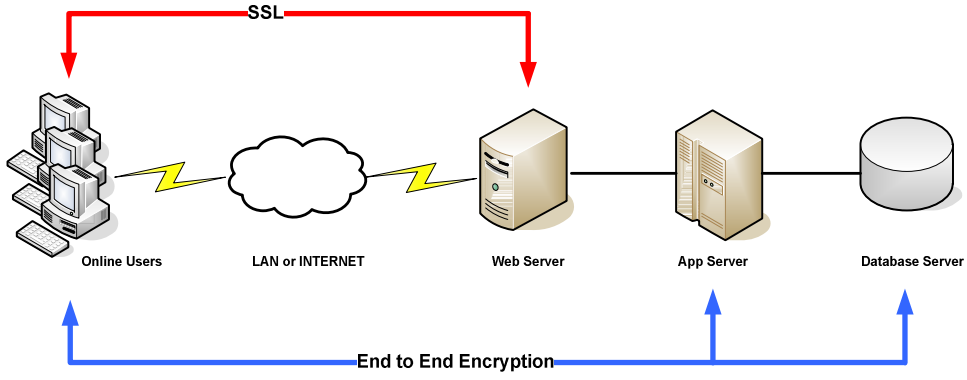
The rise of the internet has changed the way organizations conduct their business. Organizations can now leverage on the internet to access new clients, open new markets and provide a new cost-effective channel for service delivery and, partners and customers communications. Services like on-line banking, stock-broking, electronic commerce and marketplaces, telecommuting accesses and electronic mail, are prime examples of this potential. The foremost factor preventing many organizations from taking advantage of these business opportunities in this prevalent e-Economy are customer concerns over the security risks and exposures in the Internet. Data transmitted over uncharted network, such as the Internet, is vulnerable to interception, electronic vandalism, theft and alteration. Security mechanisms are required to protect these high -value data from all malicious attempts across the open network.

What is End to End Encryption (E2EE) ?

Sensitive data that travels over a network are securely encrypted from the point of data entry to the point where the data is processed. Sensitive data may be user name, password, credit card number, etc. The network can be the Internet, wireless, WAN and local LAN. Data are normally entered via the browser or a client application and the data will be processed in secure environment (via Hardware Secure Module) and be finally stored with encrypted form in the database.

Why SSL is not enough ?

SSL does not performs completed end to end data encryption in most critical deployment. SSL performs information encryption on a standard browser-to-server transaction. It only secures the connection to the web server. Unfortunately, securing the network borders is not enough. Data flowing across the web server remains vulnerable to internal risks or third-party risks in case of an outsourced web service. The use of SSL alone without application layer security therefore creates a false sense of security



SSL-based Web Deployment Vs End to End Encryption –based Web Deployment

SPECIFICATIONS

E-Trust Guard

Cryptographic Algorithms

- AES-128,256 RSA 1024 2048 Triple DES 192
- Compatible with major HSM brands

Operating Systems supported

- Windows, AIX , Linux , Solaris, Unix

Applications

- iPlanet Application server, WebLogic, Tomcat, IIS etc

Mobile Platform

- Apple, Andriod, Windows Mobile, Blackberry, Symbian etc

Solution & Key benefits

The deployment of E-TRUSTED GUARD will enable organizations to secure their valuable data end-to-end and allow secure user authentication over the Internet.

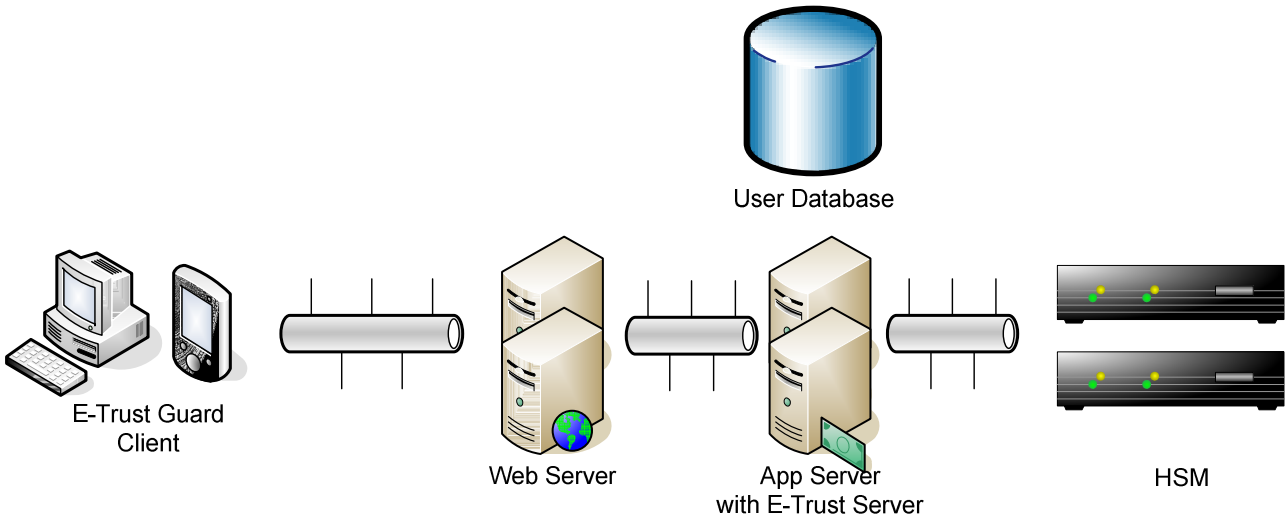
How does E-Trust Guard work ?

- When user access the login page of a web application, e.g. Internet Banking service, an client will be downloaded to the browser/mobile device together with a RSA public key to encrypt the credentials and sensitive information.
- Upon confirmation of login details, the client will encrypt the sensitive information using the downloaded RSA public key and submit the encrypted information to the server for processing.
- Once the information reached the application server, the server will retrieve the corresponding encrypted information in the application database . The pair of encrypted information will be send to the HSM for verification.
- The HSM will decrypt both set of information and compare them in the secure tamper-proof environment of the HSM.
- Upon successful verification of the credentials , the user will be allowed access to the system.
- Throughout the whole process, all credentials and sensitive information remains secure.

E-Trust Guard SDK .

The E-TRUSTED GUARD SDK enables developers to build and integrate E-TRUSTED GUARD-compliant applications with minimal efforts. Developers simply need to identify the information required to be secured and apply the relevant security application interfaces (API) available.

E-TRUSTED GUARD provides developers with an expert product that includes everything needed for delivering a TRUE end-to-end encryption security application. This means corporations can deliver the project on time without having to become cryptographic experts.



About Sunnic Pte Ltd

Founded in 2005, **SUNNIC PTE. LTD.** is the expert in protecting online identities and digital assets. The expert of core security technologies for the Internet, the company leads the way in strong authentication and encryption, bringing trust to many of user identities and the transactions that they perform.

SUNNIC has strategic partnerships with industry-leading companies that allow us to integrate our solutions into many diverse environments. Our partner network reads like a “who’s who list” of industry powerhouses, including global integrators. With the strong reputation, we already built a trusted relationship with banking and financial institutions in Asia-Pacific.

For more information , please see www.sunnic-sec.com or email to enquiry@sunnic-sec.com

Sunnic Pte Ltd

33 Ubi Avenue 3 | #08-42 Vertex Tower A | Singapore

Tel : +65 6634 8910 Fax : +65 6634 8920