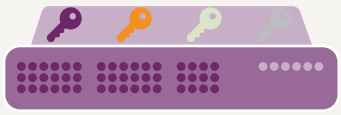
gemalto
security to be free



SOLUTION BRIEF

IBM Security Access Manager WebSEAL and Gemalto SafeNet Luna SA

Maximizing the Security and Performance of Online Communications and Business

SSL has become a fundamental requirement for securing the connections used for e-commerce, portals, Web browsing, enterprise applications, and many other purposes. However, in too many organizations, existing SSL implementations introduce unacceptable performance hits and security vulnerabilities. With IBM and Gemalto, organizations can leverage the robust solutions that enable them to maximize the security and performance of their SSL-based applications.

Introduction: Securing Online Communications and Transactions

The more businesses rely on online communications and transactions, the more they stand to lose when those channels are compromised—and today, organizations rely on these channels a great deal. For today's enterprises, transactions, communications, and applications are inextricably bound to online channels. Quite simply, many organizations stand to lose substantial revenue if their online communications are breached. Their brands, reputations, and compliance status can suffer irreparable damage. That's why, more than ever, securing Web-based communication is vital.

Today, the Secure Sockets Layer (SSL) standard is often used for securing online communications and transactions. While SSL has enjoyed broad usage, it presents several potentially significant issues:

- **Security vulnerabilities.** If the digital credentials used to authenticate the identity of a Web server are stolen or inadvertently copied to an insecure location, the SSL framework for an organization can be compromised.
- **Performance issues.** SSL requires intensive cryptographic processing, which can create significant performance issues for any associated applications and transactions.

Key Features

Through their combined solutions, IBM and Gemalto deliver the following features:

- **Robust security.** Through its capabilities for central policy enforcement, WebSEAL enables security teams to more effectively and consistently apply strong security policies across an enterprise. SafeNet Luna SA HSMs by Gemalto provide hardened security of vital assets, including certificates, cryptographic keys, and more. Further, these HSMs offer the highest level of tamper resistance and security, and have been validated to be compliant with FIPS 140-2 Level 3 and Common Criteria EAL 4+ standards.
- **Flexible interoperability.** Through GSKit, organizations can integrate approximately 200 IBM applications, including IBM WebSphere, with their Security Access Manager environments. This broad integration offers enterprises maximum flexibility in adapting their security policies and deployments to business objectives.
- **High performance.** WebSEAL is a high-performance, multi-threaded server that offers optimal throughput and responsiveness for users. SafeNet Luna SA HSMs are purpose-built, highly scalable appliances that are capable of processing up to 7,000 RSA and 1,000 ECC transactions per second. Further, by offloading resource-intensive cryptographic operations from general-purpose servers, SafeNet Luna SA HSMs help ensure that SSL operations don't compromise application performance.

The Solution: IBM Security Access Manager WebSEAL and SafeNet Luna SA

Today, IBM and Gemalto deliver integrated capabilities that enable joint customers to optimize the security and performance of online communications and transactions. With IBM and SafeNet Luna HSM by Gemalto, organizations can harness secure key and certificate storage and robust SSL acceleration. As a result, enterprises can safeguard the integrity of SSL connections, protect online presences and business applications, and secure transactions.

Following is a brief overview of each of the products and components that comprise this SSL solution:

- **IBM Security Access Manager (formerly called IBM Tivoli Access Manager).** Security Access Manager is a robust and secure centralized policy management solution for distributed applications. Security Access Manager is a unified platform that provides authentication, authorization, data security, and resource management capabilities.
- **IBM Security Access Manager WebSEAL.** WebSEAL is a high-performance Web server that enables customers to apply fine-grained security policies to their Web-based Security Access Manager environments. WebSEAL can provide single sign-on capabilities and enables customers to apply policies to back-end Web application server resources.
- **IBM Global Security Kit (GSKit).** GSKit provides libraries and utilities for SSL communication, enabling organizations to integrate SSL with a wide range of IBM applications, including IBM WebSphere.
- **SafeNet Luna SA HSMs.** SafeNet Luna SA HSMs by Gemalto are robust, high-availability, and high-performance appliances that maximize the integrity and security of cryptographic operations. SafeNet Luna SA HSMs are capable of performing thousands of cryptographic transactions per second, offering the throughput and responsiveness to support the most demanding SSL applications.

How It Works: XThe SSL Handshake and the Role of SafeNet Luna SA HSMs

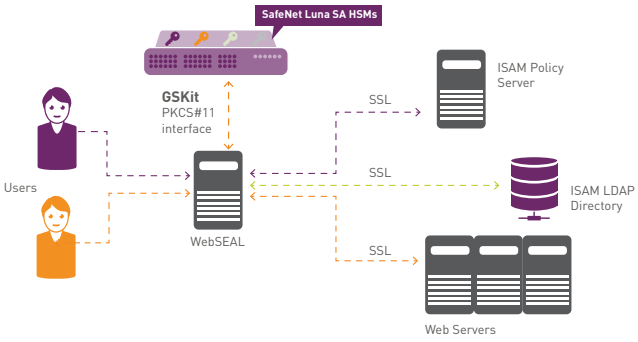
When establishing sessions between clients and servers, SSL relies on the following:

- Trusted digital credentials, in the form of an SSL private key and associated public key certificate
- Symmetric, or secret key, cryptography
- Asymmetric, or public key, cryptography

When two computers establish a new SSL session, they use digital credentials to negotiate cryptographic protocols, authenticate themselves to each other, and exchange the cryptographic material needed to create a unique session key used to encrypt subsequent communications.

During the initial SSL handshake, asymmetric key operations are used. Although the amount of data being encrypted at this point is small, the processing cost of this encryption is high. The cost of encryption at this stage makes the ability to offload processing from the WebSEAL server appealing.

Gemalto SafeNet HSM in an IBM Security Access Manager WebSEAL Environment



That's why high-performance, scalable HSMs like SafeNet Luna SA by Gemalto offer compelling advantages in SSL environments. SafeNet Luna SA HSMs can function as a dedicated SSL accelerator, which provides several benefits:

- Enables secure storage of SSL keys and certificates in a tamper-resistant appliance
- Performs both symmetric and asymmetric key functions on a single platform, which streamlines administration
- Offers a central platform for SSL acceleration that can be used by many machines
- Provides hash functions and true random number generation, providing stronger security than other solutions

About Gemalto's SafeNet Identity and Data Protection Solutions

- Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core. Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enables enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

SafeNet VERIFIED

Business Partner IBM Ready for Security Intelligence

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com
Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free