CRYPTOMATHIC
www.cryptomathic.com

Crypto Service Gateway

HSM SECURITY AS A SERVICE

You can procure storage, rack space and systems monitoring as services but why not security?

Security is at system level and is pervasive, yet time and time again corporations end up duplicating the security infrastructure for various projects in order to satisfy internal audit and compliance requirements. HSMs lie redundant; application developers waste resources dealing with proprietary interfaces and auditors must trawl through the source code of each and every application to gain assurance that the systems are working correctly. The associated financial costs across multiple business units are staggering.

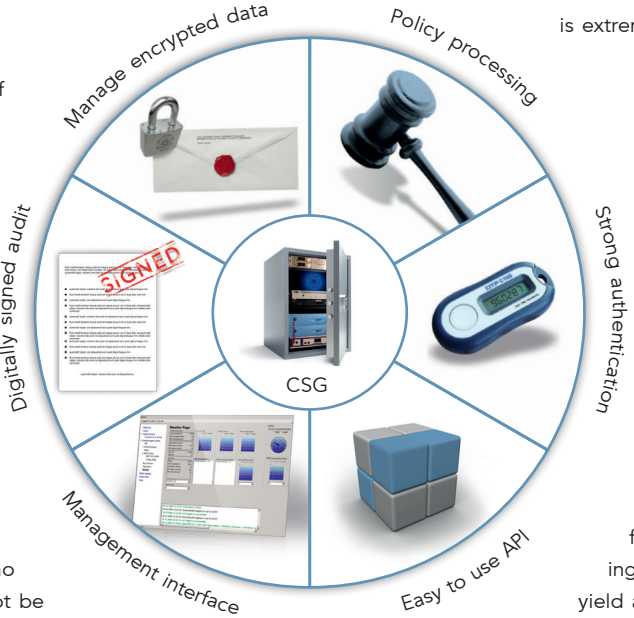
The Crypto Service Gateway (CSG) offers the world's first viable solution for providing cryptography as a service.

The CSG Concept

Project architects who design systems that utilise hardware security modules (HSMs) must invest considerable time attempting to comply with internal security policy. Often their decisions will create conflict and delay when security and risk managers come to review the system design. Instead of risking such conflicts that cause delay and sidetrack projects, the designers can procure access to a centralised HSM installation. This centralised system features key management and comprehensive compliance tools arranged around it in a secure, cloud-like environment. This allows the project designers to do what they do best – write application software, which accesses a complete and compliant security service, as and when required. We introduce the notion of a Crypto Service Gateway as the underlying software service around which a security business service can be offered.

Crypto Service Gateway

The CSG system consists of a cluster of Cryptographic Servers which sit between the HSMs and the applications. The Cryptographic Servers are managed using a dashboard allowing secure configuration, policy management and monitoring of the cluster. Operators interact with the service using two-factor smartcard authentication, and calls to the API from applications are fully authenticated (including LDAP, RADIUS etc.). Application specific cryptographic parameters and policies are all managed centrally with an easy-to-read policy language, thus ensuring that those who need to use the security services need not be concerned with issues such as encryption algorithm, key length, mode of operation, padding scheme, etc.



Cryptomathic CSG is standards based, and business platform independent; its interfaces to authentication, key management, monitoring and logging systems allow easy integration of third-party components with the system.

CSG aids compliance for internal and external audits, e.g. PCI DSS and payment card scheme regulations and is extremely scalable and reliable.

Cost Savings and ROI

CSG is unique in that it provides a high return on investment through cost savings. Direct savings are achieved due to a reduced need for testing crypto code during development, and a reduction in the amount of HSMs required (including HSM support and storage costs). Indirect savings are predominantly achieved through resource minimisation as updates and upgrades are done centrally and automatically, with no need for expensive application regression testing. These measures come together to yield an increase in technical efficiency.

TECHNICAL SPECIFICATIONS

Application Architecture
- J2EE service
- Multiple HSMs
- Simple integration
- Secure administration
- High availability

Security Architecture
- Scalable cluster
- Granular control by policy
- Managed encryption keys
- Two factor authentication for administration
- Digitally signed audit log
- Dual control for critical actions
- Asynchronous policy management workflow

Authentication Schemes
- Username / Password
- LDAP based authentication
- RADIUS-based authentication

Operating Environment
- J2EE on Red Hat Enterprise Linux
- J2EE on Microsoft

Database
- Not required

Hardware Security Modules
- AEP Networks
- ATOS
- Futurex
- HPE Atalla
- IBM
- PKCS#11
- SafeNet
- Software Crypto
- Thales / nShield
- Utimaco

USER INTERFACE EXPERIENCE

The dashboard allows you to monitor the health of the system, including figures for average min/max transaction rates, transaction latency and internal server queue size. These figures can be split down according to HSMs and applications.

POLICY

The easy-to-use policy language allows you to control what users can do, what cryptographic algorithms they use, and to prove compliance to auditors. Security managers review and approve policies and digitally sign them via the UI. The operations team then uploads the policy and can schedule its activation in advance.

```
[USER Maria]
Permission = DO ENCRYPT

[PARAMS MyParams]
Cipher = AES
Mode = CBC
Managed = true
```

ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. Since 1986, Cryptomathic has provided customers with systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing and advanced key management utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

Learn more at cryptomathic.com