



CRYPTOMATHIC

Crypto Service Gateway



Product Sheet
CSG

Central control of all
cryptographic policies
and hardware

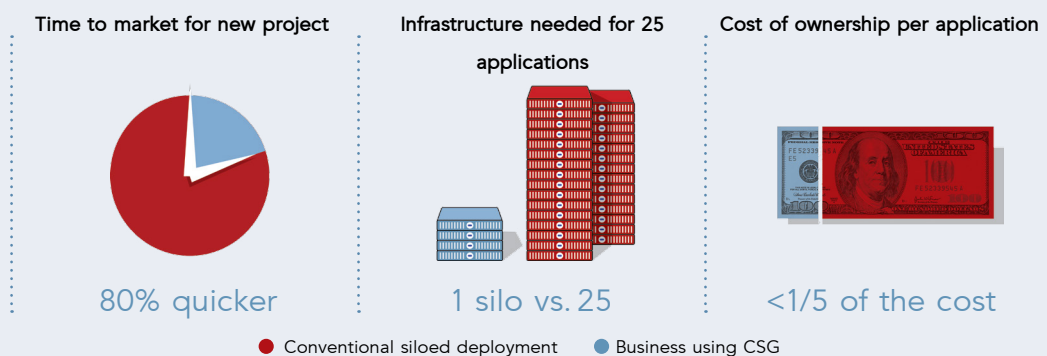


Achieve business agile & efficient crypto services, with central control of security policy and crypto hardware

Managing cryptography and Hardware Security Modules (HSMs) are the foundations of securing the digital assets of a business. When architecting and delivering security applications, businesses often end up inefficiently duplicating crypto infrastructure. Supporting an increasing number of siloed projects results in a loss of oversight and an increased risk of data exposure. The associated costs across multiple business units can also become unsustainable.

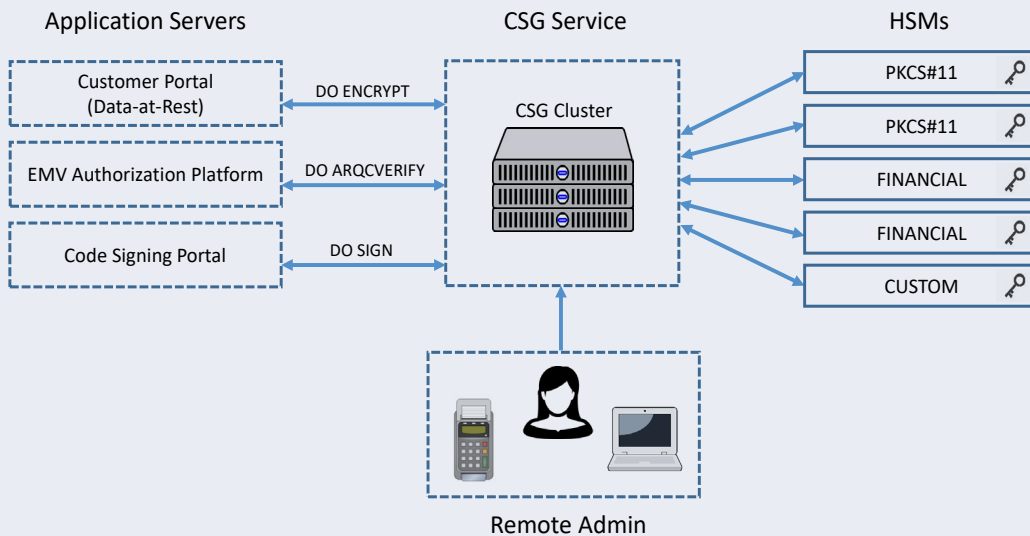
CSG (Crypto Service Gateway) is a central cryptographic infrastructure that simplifies application integration while ensuring the highest availability and utilization of HSMs. CSG shares HSM resources between applications, allowing central policy enforcement and management of HSMs. With CSG, a business can assert total control over its crypto estate, delivering increased efficiency, cost savings and confident compliance.

- Reduces costs through shared infrastructure and increased HSM utilization
- Centralizes policy and control over all crypto operations; keeping crypto decisions in the hands of the security team
- Enables complete central management and monitoring over entire HSM real-estate
- Provides easy to read audit logs for proof of compliance
- Simple-to-use API delivers increased development velocity and reduced time to market



Typical Use Cases

- Banks and financial services which require various payment related operations, e.g. EMV authorization, PIN management, CVV validation and tokenization
- Technology manufacturers and software companies who need code-signing or format preserving encryption
- Government/Healthcare agencies that need to encrypt a large amount of personal data-at-rest and in-transit
- Organizations such as banks or cloud service providers that want to provide agile HSM crypto services for secure applications



Technical Architecture

CSG provides a highly-available and scalable infrastructure for using HSM crypto services. A CSG server cluster sits between HSMs and the applications, distributing load to the appropriate HSM(s) and enforcing crypto policy.

CSG is managed using a dashboard allowing secure configuration, policy management and monitoring of the cluster. Administrators interact with CSG using two-factor smartcard

authentication, and calls to the API from applications are fully authenticated (including LDAP and RADIUS support).

Application-specific crypto parameters are all managed centrally through an easy-to-read policy language. The policy simplifies internal and external compliance audits (e.g. PCI-DSS), and empowers your security team with crypto agility.

Technical Specifications

Operating System:

- Windows Server
- Red Hat Enterprise Linux
- CentOS

HSMs:

- HPE Atalla
- Safenet/Gemalto
- Thales
- Utimaco

APIs:

- Crypto Query Language (CQL) for streamlined simple development
- Libraries: Java, C++, C#/ .NET
- Web Service: RESTful

Key Types:

- AES, 3DES, RSA, ECC

Algorithms/Modes:

- Hashing: SHA256, SHA384, SHA512
- Symmetric: ECB, CBC, IBMIPS, GCM, HMAC
- Asymmetric: PKCS#1v1.5, OAEP, PSS, ECDSA

Financial functionality:

- PIN validation and translation
- CVV/CVC validation
- ARQC validation
- EMV issuer scripting



CSG: Building Crypto-as-a-Service

CSG not only improves management and monitoring of HSMs but more importantly, streamlines and strengthens the process of deploying cryptographic applications. Easy-to-use APIs make development quick, and centralized policy enforcement makes compliance audits simple. On top of this, CSG provides a high return on investment through direct and indirect cost savings.

Additionally, CSG's companion key management system, CKMS, controls all the keys for simple key management compliance audits, and can also be used for applications that aren't using the CSG service.

CSG Case Study - Barclays

Cryptography as a service

Crypto Service Gateway (CSG) revolutionizes the management of cryptography for businesses. With CSG, Barclays now has over 125 applications running on a single crypto platform, achieving significant and steadily increasing cost savings and usage growth. Providing a cryptographic business service, agile to changing business needs, CSG's philosophy is truly unique, as it offers user-friendly, transparent, vendor agnostic cryptography as a service.



CKMS Case Study - Swedbank

Centralized key management for a major acquirer

Being one of the largest acquirers in Europe and managing keys for hundreds of applications, Swedbank has modernized its cryptographic key management activities to securely control the keys for its card payment acquirer network and its payment terminals.

ABOUT CRYPTOMATHIC

Cryptomathic is a global provider of secure server solutions to businesses across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile. With over 30 years' experience, we provide systems for Authentication & Signing, EMV, Key Management and PKI & ID, through best-of-breed security solutions and services. We pride ourselves on strong technical expertise and unique

market knowledge, with 2/3 of employees working in R&D, including an international team of security experts and a number of world renowned cryptographers. At the leading edge of security provision within its key markets, Cryptomathic closely supports its global customer base with many multinationals as longstanding clients.