CRYPTOMATHIC
www.cryptomathic.com

Crypto Service Gateway - Business Benefits

Managing Application Level Cryptography and HSMs Across the Business

Implementing, operating and maintaining cryptography in an organisation can add significant overheads to the business' IT operations. There are direct costs associated with acquiring and maintaining hardware and software, but there is perhaps an even greater aspect of cost associated with the integration and ongoing management of hardware security modules (HSMs). Many organisations utilise HSMs for enhancing cryptographic security, safekeeping of keys and to ensure compliance.

Deploying cryptography, operating HSMs and managing keys is a very complex task, and tends to be decentralised and application- or project-driven, in other words, highly specialised and tailor-made for each instance. Very few developers have the required security background needed for writing crypto code and integrating HSMs. In turn that has an impact on cost through additional resources, extended project times, error correction, stability concerns and compliance requirements. Implementing cryptography within a single application or project is, in many cases, likely to add a 6-digit cost overhead and several months delay to the project.

Consider the advantages a business could achieve by incorporating cryptography as a service within its IT infrastructure - running as a centralised and integrated service ready for use any time of day. With an ever increasing number of applications requiring crypto, a practical and secure crypto service would remove a large part of the traditional hindrances of deploying and managing cryptography in large organisations.

The Cryptomathic Crypto Service Gateway (CSG) offers a wealth of benefits to organisations that rely heavily on crypto. These benefits are derived from the advanced features and functionality of CSG that enables the enhancement of business processes and operational efficiency. This paper explores the following non-exhaustive list of direct advantages that can be achieved by implementing the CSG.

Cryptography as a Service

The flexible and interoperable system architecture enables all applications in need of data security or cryptography to be seamlessly integrated into a new or existing HSM network. HSM security can now be applied to applications where it was previously viewed as being too costly to implement. HSMs can be securely shared across a variety of applications, combined with centralised and remote management; CSG now provides the world's first viable solution for crypto as a service.

Lower Project Costs

Traditionally, a new and fairly small project that requires just one HSM for processing will typically require a minimum of four HSMs – one for production and one for back-up, one for development and one for testing. CSG eliminates the need to acquire dedicated hardware for individual security projects. CSG can run HSM emulators for less sensitive operations, and shared HSMs can be re-used so capacity is only ever increased when the combined utilisation of crypto grows beyond a certain (maximum) threshold. Figure 1 illustrates the superfluous configuration and duplication of infrastructure of traditional HSM deployments.

Reduce Existing HSM Estate by 50% or More

Due to limited functionality and management capabilities of HSMs, the vast majority of devices are underutilised. CSG customers can successfully reduce the total amount of HSMs needed by more than half for production, back-up, disaster recovery, development and testing. Figure 2 illustrates HSM configuration with CSG.

Central Policy Enforcement

CSG applies a centralised and granular cryptographic policy that enables seamless updates for all necessary cryptographic functions without any changes in the application code. The policy includes which type of algorithms to be used, which keys can be used, and a number of other attributes and parameters that are allowed for any given application. The policy file is digitally signed and can be provided for audit purposes.

Obtain and Maintain Compliance

Compliance is often considered a necessary evil, which most organisations need to adhere to, whether the regulatory body is internal, payment scheme, or governmental. The centralised policy enforcement of the CSG collects all relevant information in a single place for easy audit and is in human-readable form, so that demonstrating compliance with internal and external policies is much easier.

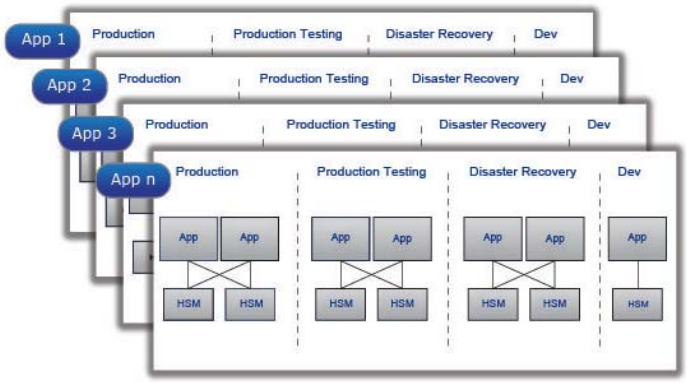

Fig 1: Traditional HSM Configuration

Fig 2: HSM Configuration with CSG

Together with policy enforcement and strong authentication, a company using CSG can effortlessly demonstrate compliance across all applications at the same time, and all from one point.

Resilience – Eliminate Disruption from Hardware Failure

Running the CSG means that HSM failure causes zero down-time with no disruption to production. Whether a disruption is uncontrolled, e.g. an HSM breaks, or controlled e.g. an HSM is taken off-line for a software upgrade, the applications maintain their resilience without any interruption whatsoever.

Easy Integration with CSG - Standardised APIs

It is very easy for developers who are not familiar with crypto to integrate applications with the CSG using one of the standard APIs or the manual CQL - Crypto Query Language.

Shortened Time to Market

Ease of integration and availability of crypto hardware and services significantly reduces the time to market for new applications, typically by two to three months.

No Regression Testing for Applications

Valuable development time and cost are further reduced for new projects as the CSG uses a standard and common set of cryptographic functions that need not be tested for each new application demanding crypto services via CSG.

Hardware and Software Encryption

Not all applications require hardware enhanced security so in many cases software encryption and authentication will suffice. CSG supports both hardware and software encryption ensuring the availability of the most optimal means of encryption.

Improve Workflows

Following simple and standard policies and methods of working will greatly improve the dynamics of the work flow using crypto as a service.

Avoid Human Error

In dealing with HSMs human error is very common. Errors include mistakes in installing and maintaining devices, typing key components, and integrating with HSMs in a secure manner – in order to eliminate threats and obtain compliance. CSG removes these difficulties by simplifying and automating manual procedures.

Centralised Management and Updates

HSMs often reside in different data centres, which can be split across great geographical distances, hence the efficiency in centralising managing and updating of HSMs saves time and effort.

Monitoring

CSG allows for administrators to monitor the performance and usage of individual HSMs and applications as well as the entire network, which makes all crypto operations completely transparent.

Maximise HSM Usage and End of Life Cycle

CSG treats HSMs as one cluster making it possible to utilise an individual HSM's maximum capacity (which it was originally built for anyway) of 80% - 100%. In addition HSMs often have short life cycles, e.g. five years, but there is no need to discard devices even without support until they actually break down, which could be years following the official end of life date.

Reduce Ongoing Support Costs

The initial cost of an HSM is doubled over five years because of annual maintenance and support. So if an organisation can reduce their HSM estate by e.g. 50% then the ongoing costs for HSMs will be reduced by that same percentage.

Commoditise HSMs – Increase Buying Power

HSMs are proprietary built devices that are not suitable for interoperability across brands. CSG gives customers the power to shop for the best HSMs, which typically combines speed and low cost. HSM vendor tie-in is thus eliminated.

Most major HSM brands are currently supported by CSG, including AEP Networks, Bull, Futurex, IBM, Safenet, Thales (including nCipher) & Utimaco.

Return on Investment Within Year One

Not having to acquire new HSMs coupled with shortened development time for new projects results in a very high return on investment, which in most cases can be achieved during the first year alone.

Contact Cryptomathic

To hear more about the individual points covered by this paper and how they may apply to your business, please contact your local Cryptomathic representative or email us on: **sales_enquiry@cryptomathic.com** or **technical_enquiry@cryptomathic.com**

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. With more than 25 years' experience, Cryptomathic provides 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