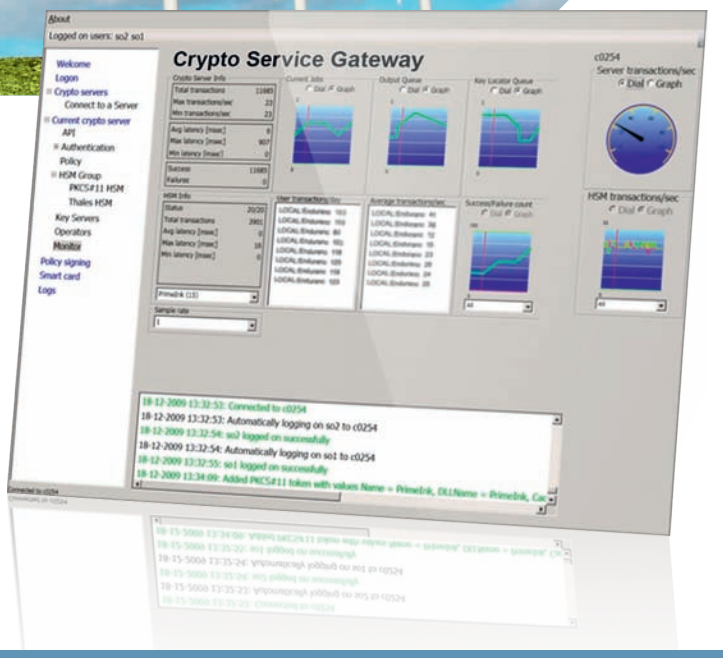
CRYPTOMAThIC
www.cryptomathic.com

Case Study
A British High Street Bank – Crypto Service Gateway



SECURITY AS A SERVICE

A major British High Street Bank has adopted the Crypto Service Gateway (CSG) solution to support a new approach to provision of security and cryptography across the breadth of its applications and products. The Cryptomathic CSG allows the bank to centralise hardware cryptography, management of keys, and to have fine-grained policy enforcement and auditing over access to key material where only fragmented support existed before. The core aim has been to increase technical efficiency across all departments concerned with cryptographic processes, and the bank chose Cryptomathic's solution and contributed towards its second generation incarnation as the world's first complete software solution for deploying a cost and time saving, scalable and reliable security service.

THE BANK'S REQUIREMENT FOR THE CRYPTO SERVICE GATEWAY

The bank customer is one of the world's largest financial service providers with an extensive international presence across most continents. Its products and services are diverse, and correspondingly its security requirements. Within the UK several hundred HSMs are required to support service provision to the bank's more than 15 million customers. Given the quantity and variety of HSMs used, it can become difficult to recognise their working condition, productivity, performance, health, and usage – the problem of management and monitoring. Project architects who design systems that utilise HSMs in the bank find that recreating the same crypto infrastructure in each project, and directly integrating against HSM APIs becomes costly to maintain, but also takes a long time to develop. As in any other high street bank, their development staff do not have all the necessary experience of working with different HSMs, even when supported by their well-trained security professionals. Hence, avoiding design mistakes and implementation delays, will save valuable project time and resources.

Encryption of the data is the easy part, but ensuring that the data can be migrated from encryption under an older key to a new one, or upgraded to a stronger encryption algorithm can be very challenging – especially without causing significant downtime to the system whilst the data is translated. Sometimes simply keeping track of which data records are encrypted with which keys can be challenging.

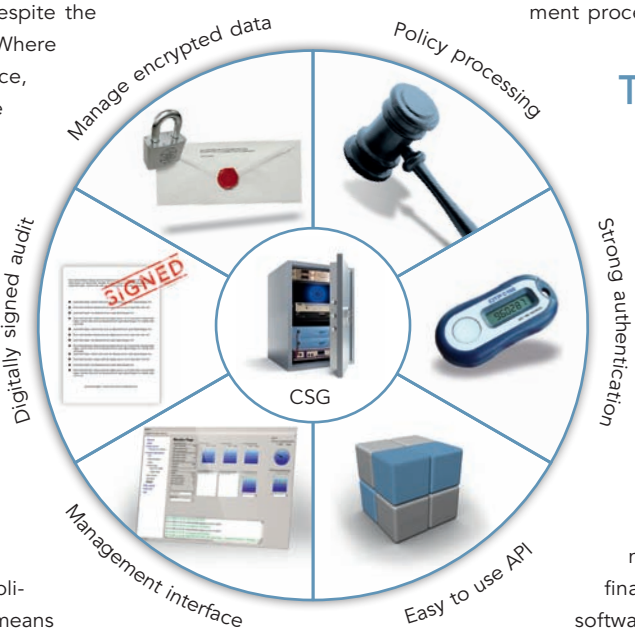
OPTIMAL UTILISATION OF HSMS

The bank makes extensive use of hardware cryptography – encryption using keys stored in Hardware Security Modules (HSMs), which are costly and specialised devices. But due to the paramount requirement for availability and resilience in the bank's systems, more and more devices become required to ensure a resilient system capable of supporting the peak load, despite the high performance of modern HSMs. Where one or two HSMs in theory might suffice, difficulties in configuration and secure sharing of the devices mean that a large product might need three times as many HSMs to support it, once the different development, testing, and disaster recovery instances are taken into account. Because of these problems accommodating multiple applications on the same HSM, and in getting the necessary reliability guarantees, HSMs are under-utilised. Some HSMs may have as little as 4% utilisation.

Even with efficiency and utilisation savings on HSMs, the sheer breadth of applications supported by a global player means that a wide variety of underlying HSMs will be required: Specialist applications such as payment authorisation require specialist HSMs. At an operations level the bank needs a unified view of its HSM estate, showing health and performance, in order to maintain the infrastructure at peak efficiency. The more detailed the data available, the easier it is to identify and remove bottlenecks. Such a monitoring and control system should permit mixing of different types of HSMs with different programming APIs and from different manufacturers, allow hot-swapping of devices and support scaling of the system to support even very high performance requirements.

It is not sufficient simply to operate a secure system; the bank has a requirement to prove that they are doing so. Like any bank they are subjected to regular audits from a variety of bodies including national and international card schemes. Demonstrating compliance with regulations can be very time consuming and burdensome in traditional projects. The particular security settings used may be buried deep in design and specification documents, which incur time and manpower to locate, and it may be even harder to demonstrate to an auditor that the system is actually operating as the design claims it should. The bank thus has a requirement at the cryptographic level to demonstrate both a coherent security policy, and the enforcement of that policy.

The bank uses a competitive outsourced development process to get the best price and quality for the software it needs. The development team that is selected to undertake a new project will contain specialists within the application domain of the project, but as cryptography becomes ever more present for data security in all applications, developers who are not security specialists are required to be ever more involved in protecting the data handled by their application. Rather than incurring the cost of hiring extra specialists, or risking delays to projects. The bank would far prefer to be able to make security and encryption safely accessible services to non-specialists. The bank desires a solution which keeps their software procurement process lean and fast.



THE CSG

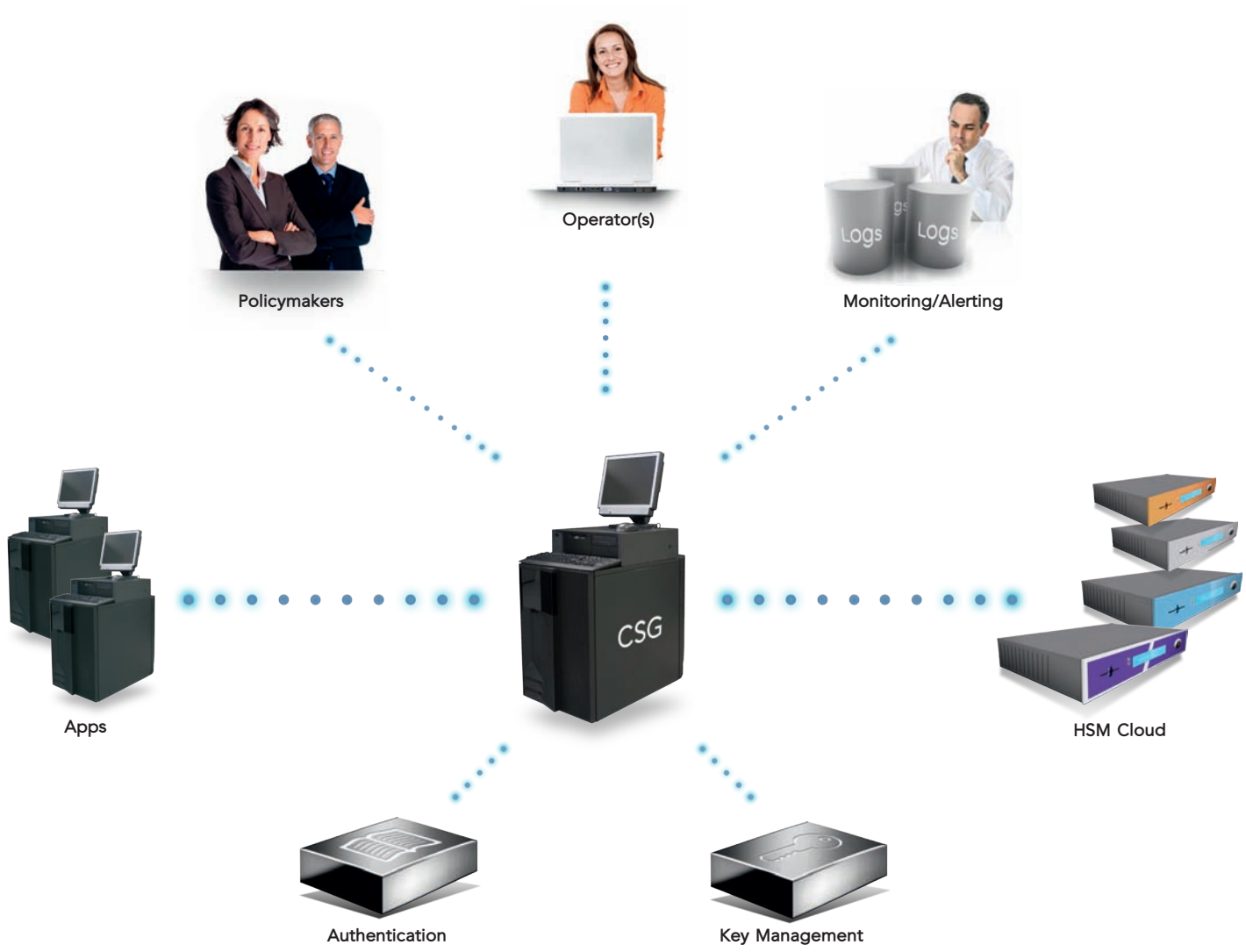
In the past, different vendor products have addressed the bank's requirements in part: maybe a manufacturer offering failover and recovery of HSMs, or an API supporting simplified crypto operations. But a plethora of ill-matched and proprietary components proves very difficult to combine into one efficient solution. For this reason the bank came to Cryptomathic, a security software provider uniquely placed to offer an integrated and total solution, which meets all the requirements of a large financial institution. Cryptomathic's CSG software consists of a cluster of Cryptographic

Servers sitting between the bank's applications and their HSMs. These servers act both to add value in offering new functionality, and to limit access to existing functionality – implementing a security policy.

The Crypto Service Gateway supports easy to use crypto APIs, making even complex crypto operations as easy to use for a typical developer as writing an SQL query. It supports a fine-grained but straight forward policy language, which allows administrators to control exactly what keys and commands different users of the system have access to. The policy language is simple enough to show to auditors and business architects who do not have programming experience. CSG also supports asynchronous review, approval and digital signature of the policy by senior security managers. Conventional operators can then apply the policy to the live system, without the ability to make unauthorised changes. CSG supports strong authentication for both its administrators (using smartcard and PIN) and for identifying the applications and end-users of the system; it can call out to an external two-factor authentication server, or integrate with a central LDAP or active directly.

CSG has extensive usage and audit logging, digitally signed for non-repudiation, which together with the policy language allows projects to demonstrate both theoretical and actual compliance with regulations.

CSG supports an innovative managed encryption format, which allows encrypted data to carry with it information about the keys used to encrypt, enabling easy migration between encryption keys, and upgrading to stronger algorithms. Applications using CSG's managed encryption will even be able to undertake a gradual migration of stored managed data between keys with zero downtime and no need for application awareness of the process.



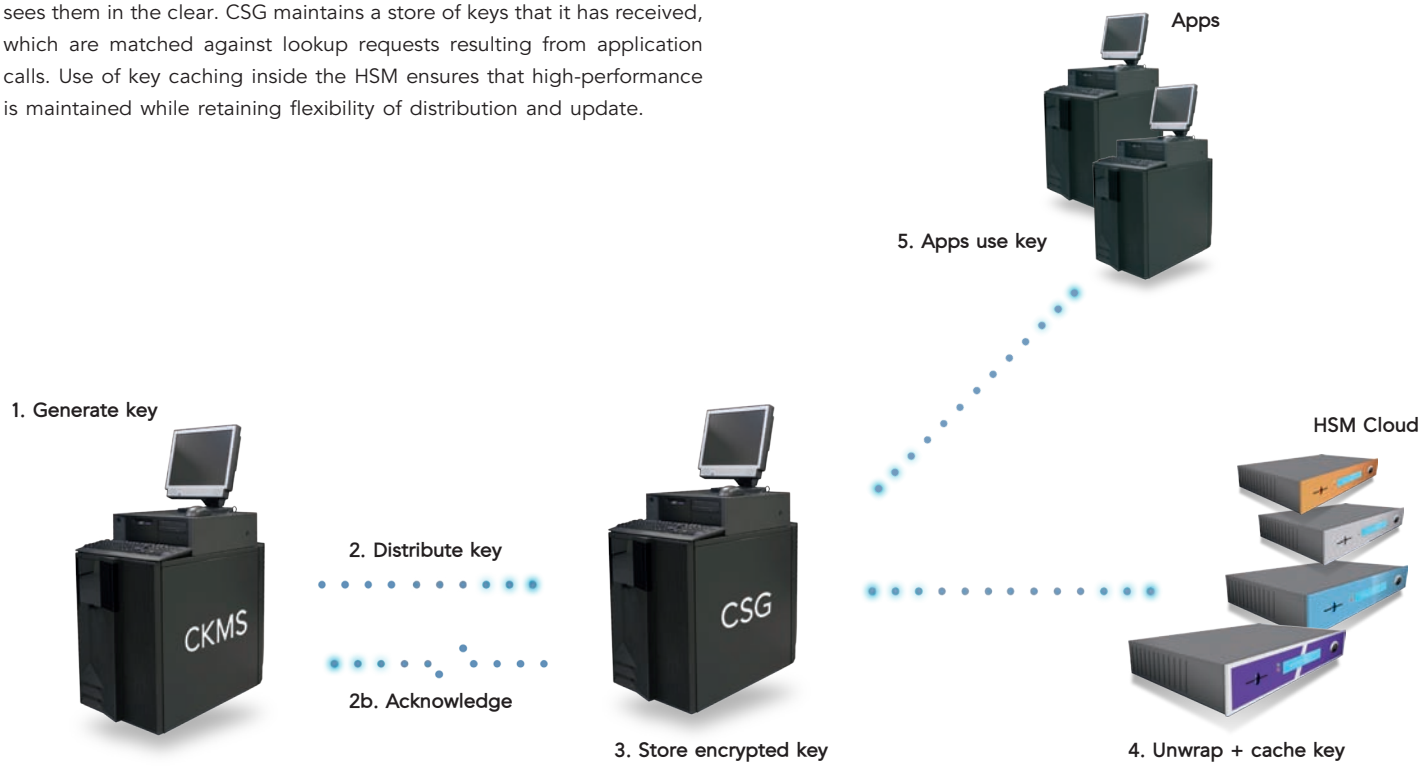
A NEW PARADIGM

The bank chose Cryptomathic CSG because its innovative, efficient character as a leading-edge solution matched the bank's own ambitious plans to conceive of a new and better way to deploy security internally in the 21st Century. It was designed and developed by programmers with decades of experience working with general purpose and specialised HSMs from a variety of international and local HSM vendors; CSG is truly the world's first viable solution for providing cryptography as a service.

KMS INTEGRATION

The CSG integrates seamlessly with Cryptomathic's Key Management System (KMS), dividing up the tasks of a cryptographic service between them. The two products work in partnership: the Key Management System ensures the right keys are in the right place at the right time, while the CSG ensures they can be efficiently used by only the correct authorised parties, and in only the correct way.

Keys are created (and automatically updated if required) by KMS, which uses a "key push" to distribute the key securely to each CSG server. KMS maintains a trust relationship between its own HSM and each HSM managed by the CSG server, so CSG only handles encrypted keys, and never sees them in the clear. CSG maintains a store of keys that it has received, which are matched against lookup requests resulting from application calls. Use of key caching inside the HSM ensures that high-performance is maintained while retaining flexibility of distribution and update.



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