CRYPTOMATHIC
www.cryptomathic.com

CSG Case Study – Barclays

CRYPTOGRAPHY AS A SERVICE

In partnership with Barclays, Cryptomathic has developed Crypto Service Gateway (CSG), a solution to revolutionise the management of cryptography for businesses. Today Barclays has many projects using CSG which are achieving significant and steadily increasing cost savings.

As cryptographic costs are increasing within IT budgets, cost savings are but one of the many reasons Barclays chose to deploy CSG. The philosophy adopted, was based on the need to provide a cryptographic business service, agile to changing business needs. CSG's philosophy is truly unique as it provides user-friendly, transparent vendor agnostic cryptography as a service.

CSG as the technical centre of a cryptographic service allows a business agenda to be set. Typical drivers include 1) Improve responsiveness to market for business projects 2) Prevent cryptography being a project bottleneck 3) Standardise and simplify control and compliance 4) Minimise operational and future life-cycle costs.

CSG allows Barclays to be proactive in its cryptographic management; it is the first cryptographic solution to do this. CSG has been and continues to be a catalyst for change in Barclays' management of cryptography.

BARCLAYS

Barclays is an international financial services provider engaged in personal banking, credit cards, corporate and investment banking, and wealth management with an extensive presence in Europe, the Americas, Africa and Asia. With over 300 years of history and expertise in banking, Barclays operates in over 50 countries and employs approximately 135,000 people.

Barclays has a history of innovation including:

- 1966, Barclays launched the UK's first credit card
- 1967, Barclays installed the world's first ATM
- 2012, Barclays launched "Barclays Pingit", Europe's first P2P payments tool

In recent years, cryptography has been identified as an area that required further innovation to meet the strategic needs of the business. With security at the forefront of banking, most applications were requiring cryptographic resources, and the spiralling costs and complexity of deployments forced Barclays to be innovative once again.

CRYPTO HEADACHE

Over the last couple of decades at Barclays, use of mainframe-based cryptography has declined in favour of network-based hardware security modules (HSMs). This shift in technology triggered several problems.

The most pressing concern was an explosion in the number of HSMs being purchased by the company. Networked HSMs were often siloed into particular projects and it was difficult or impossible to share these resources with other projects. A typical project would require at least four HSMs to provide the necessary production resilience and testing capabilities, and before long Barclays had hundreds of devices across its data centres.

This approach also meant that important cryptographic decisions, such as algorithm choices or key sizes, were being enforced on a per-project basis. This severely reduced flexibly and would make it very expensive to deprecate a cryptographic algorithm (e.g. MD5 or SHA-1). Auditing such a disparate system was also expensive, with inspections required across a large number of separate systems, each with their own compensating controls and processes to verify.

A final consequence of the large number of HSMs was that Barclays' architects and developers had to be familiar with the idiosyncrasies of different brands of HSM, which results in additional training costs and protracted development times.

Barclays realised something had to change to make their use of cryptography affordable and scalable in the long-term.

REACHING A SOLUTION

Barclays looked to their vendors for an answer to the challenges they faced. While many shared elements of the vision Barclays held, the outlook was poor – there would be no solution for many years to come.

Karen Jordan,
Head of Barclays
Cryptography Service
Management

"CSG has enabled us to accelerate the delivery of crypto applications while generating financial and effort savings."

Meanwhile, Cryptomathic was debating the very same topic. As a provider of HSM vendor-neutral commercial cryptographic solutions since 1986, and a trusted supplier to Barclays, Cryptomathic was well aware of the problems associated with large scale deployments. Cryptomathic was already a leading vendor of lifecycle crypto key management solutions for the banking industry and had developed a prototype crypto service solution for a large ATM manufacturer. In 2008, Barclays and Cryptomathic joined forces to tackle the problem of "crypto as a service".

Following a series of workshops, both companies agreed a new solution was required in order to solve Barclays' current cryptographic problems and deal with the challenges of the future. A number of objectives were identified for this new system:

- Support HSMs from a variety of vendors
- Be centrally managed and easy to scale
- Help lower the development cost of cryptographic applications and allow them to be delivered into production faster
- Allow projects to share load across HSMs meaning fewer HSMs in total
- Make it easier and cheaper to perform audits

Based on these objectives, Cryptomathic developed the Crypto Service Gateway (CSG), a product that met Barclays' cryptographic needs for the foreseeable future.

BENEFITS OF CSG AT BARCLAYS

CSG provides Barclays with a centralised crypto service capability. As of August 2014, Barclays have 56 applications (both new and legacy) running on a single CSG cluster, PIN translation in three European countries and four Internet and Interactive Voice Response (IVR) channels in the UK. An additional 81 applications are in testing phase and will be deployed into production in due course.

By using CSG, Barclays have significantly reduced their time-to-market on new projects requiring cryptography and have also reduced costs.

In one project alone, CSG allowed Barclays to deliver a critical application into production in just six weeks rather than the previously typical six months. On the same project Barclays avoided significant monetary costs on HSM hardware by utilising existing HSM capacity within the business. Neither saving would have been possible prior to the introduction of CSG.

BARCLAYS' CSG DEPLOYMENT

Barclays have deployed four instances of CSG into their UK data centres: one for production use, one for disaster recovery, one for test and one for development. Each non-development installation comprises:

- Four CSG servers and one CSG administrator client
- Four Thales nCipher HSMs (for general purpose cryptography)
- Remote monitoring

CSG has also been deployed in Singapore, and the United States. Key distribution for these sites is managed from the UK.

NUMBER CRUNCHING

The excellent monitoring and logging capabilities of CSG allow Barclays to examine their usage of the service over arbitrary periods of time.

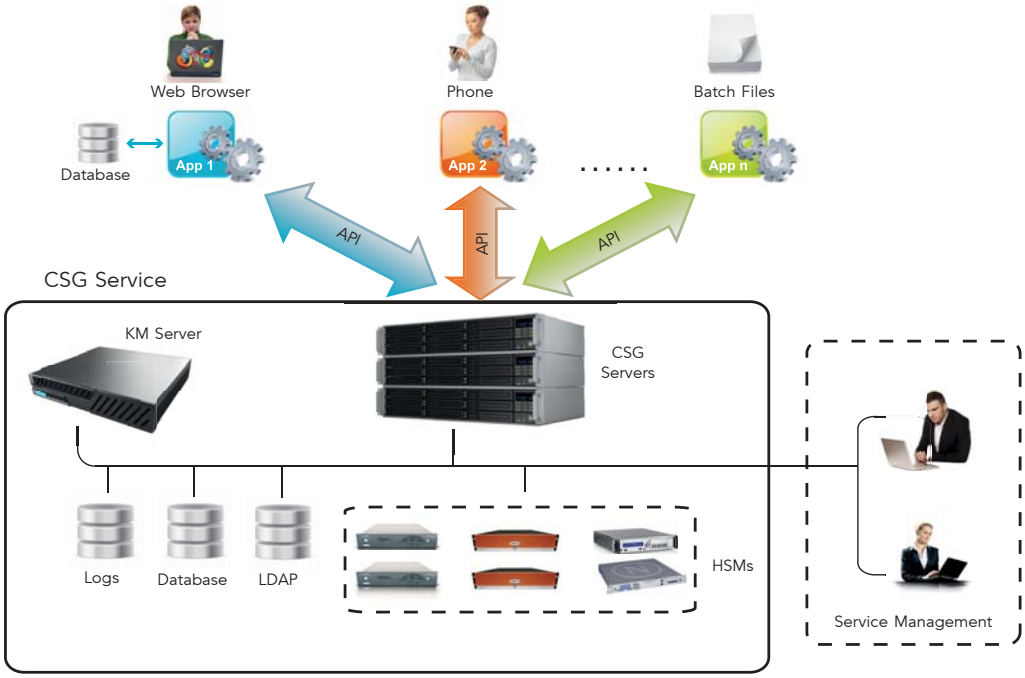
CSG provides a web services interface for monitoring the current status of the system, including transaction numbers and HSM health metrics. To give some idea of the volumes involved, Barclays are currently pushing approximately 6 million transactions a month through the CSG system. Latency measurements are very reassuring, with over 99% of transactions taking less than 50ms.

The table below shows the transaction loads over the previous month (at the time of writing):

Load Level	% Time at Load	Time at Load
None (0tps)	63.0	21.1 days
Very low (1-10tps)	36.5	12.2 days
Low (10-100tps)	0.2	1.7 hours
Modest (100-500tps)	0.3	2.2 hours
Moderate (500-2000tps)	0.0	5 minutes
High (2000-10000tps)	0.0	0 seconds

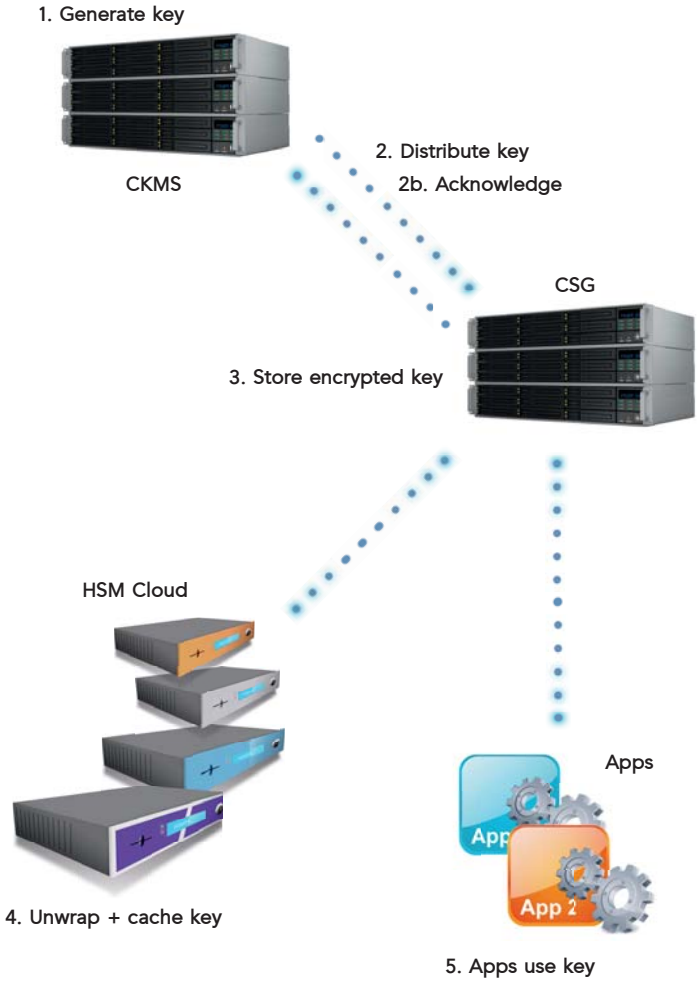
These numbers indicate just how much wasted capacity exists in a typical enterprise deployment. Barclays are servicing 39 live applications using only four HSMs and yet there is still a great deal of capacity available for more work. A typical enterprise business would have 234 HSMs to service the same demand.

Example of Service



CSG

Cryptomathic's CSG middleware provides a new interface between business applications and the underlying cryptographic resources, allowing multiple applications to share HSM resources without concern over the number available or the vendor(s) that supplied them. This reduces hardware vendor lock-in compared with traditional approaches and improves levels of resilience and performance management.



Centralised controls allow the business to restrict access to cryptographic functions and enforce policies on key length, rotation, mode of operation and so on. This is invaluable for demonstrating compliance with regulations and drives down the cost of audits.

CSG supports an easy-to-use API, called the Crypto Query Language (CQL), similar in syntax to SQL. CQL focuses on what needs to be done, not how. As a result, developers of all experience levels can skip the steep learning curve associated with most crypto APIs and deliver applications to production faster than ever before.

Strong authentication controls ensure only authorised users can adjust policy settings or deploy new applications or resources into the system. CSG can interface with a number of authentication services including LDAP, Active Directory and external two-factor authentication servers.

INTEGRATION WITH CKMS

"Do one thing and do it well." This is the mantra behind most UNIX applications and it applies to Cryptomathic products as well – CSG controls the use of cryptography in a business, but it doesn't handle the key management itself, it works in conjunction with a business' key management system.

Cryptomathic Key Management System (CKMS) is the leading key life-cycle management product and a perfect choice for managing the entire lifespan of the keys used by CSG. CKMS ensures the right keys are in the right place at the right time, while CSG ensures they can be efficiently used by only the correct authorised parties and only in the correct way.

CKMS 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. Use of key caching inside the HSM ensures that high-performance is maintained while retaining flexibility of distribution and update.

The security features of CKMS are designed to address the requirements of common key management regulations, meaning users will benefit from lower audit costs and an easier compliance process. CKMS is used in a variety of industries, but is particularly prominent in the financial services sector, where it is deployed by payment schemes, banks and third-party processors, across the world.

CONCLUSIONS

By working in close partnership, Barclays and Cryptomathic harnessed their combined experience in the field of enterprise cryptography to create the blueprint for crypto as a service. Cryptomathic took this blueprint and developed a solution that has revolutionised the way Barclays manages its cryptographic estate.

Cryptomathic has now expanded its CSG customer base to other institutions – both large and small - and is proud to be the world's first provider of technology for offering crypto as a service.

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