CRYPTOMATHIC
www.cryptomathic.com

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 manage keys for its card payment acquirer network and its payment terminal management system.

Cryptomathic Crypto Key Management System (CKMS) and Cryptomathic Terminal Key Management System (TKMS) has allowed Swedbank to benefit from better streamlined key management processes, with more automation of procedures and reduced administrative overhead. This modernization provides Swedbank with a high level of assurance that its financial cryptographic key management systems are being managed in a secure and measurably effective manner.

Swedbank is a modern bank firmly rooted in Swedish savings bank history. Swedbank is the largest retail bank in Sweden, it is the leading card payment acquirer of Visa and MasterCard in the Nordics and Baltics, and the fifth largest card payment acquirer in Europe. Swedbank issues payment cards to over 9 million customers and acquires card payment transactions on behalf of 540,000 merchants, part of which requires ATM and POS terminal key management for around 300 systems in total.

BACKGROUND

The integrity and availability of card payment systems are underpinned by cryptographic services, which rely on the security surrounding their cryptographic keys. The number of keys in use within large scale card payment systems is in the millions, and this presents a significant management challenge for the banks that operate them. Moreover, the banks must ensure that systems are managed in accordance with strict regulatory control. Internal and external audit processes provide the bank and the regulators assurance that the card payment systems are being operated effectively. Noncompliance can lead to extensive fines and, in the worst cases, security breaches, reputational damage or the eventual loss of certification and valuable customers.

Swedbank has a wealth of experience in operating secure key management facilities. As well as managing thousands of keys for one of the largest payment acquiring networks in Europe, Swedbank is responsible for provisioning keys to EFTPOS payment terminals adhering to international and national Swedish standards. The original key management system had been in place for many years, and the technology was in a legacy state and approaching end of life. The user experience was cumbersome, with little scope for improvement, which lead to an increased risk of operator error and a consequent increased risk to operations. The system was at the limit of its ability to scale and meet the demands of a growing business, and it was becoming increasingly difficult to maintain the security of the system in line with an evolving regulatory landscape. The system was ultimately prohibitively expensive to operate on many levels, so Swedbank sought a new long term solution.

NEW SOLUTION DRIVERS

There were several drivers for a new solution that needed to address deficiencies in Swedbank's existing key management system:

- Offer tamper evident audit logs using tamper resistant HSMs and role based access control
- Enable the bank to easily demonstrate compliance to applicable regulatory payment scheme standards and internal audit requirements
- Provide support for the various key formats that enable the interoperability of banking key management systems
- Provide management of key meta data, e.g. originator usage period
- Improve user experience through a flexible key management workflow without compromising on security
- Support scaling the number of keys to meet projected growth of the bank's business
- Agility to enable operators to react quickly to changes in crypto policy and immediately respond to security incidents
- Provide 24/7 access to security incident investigation or internal audit
- Produce comprehensive management reports

Stefan Andersson,
Business Security
Manager, Swedbank

> *"Cryptomathic's solution has enabled Swedbank to meet its compliance requirements and significantly reduce the cost of key management to security operations."*

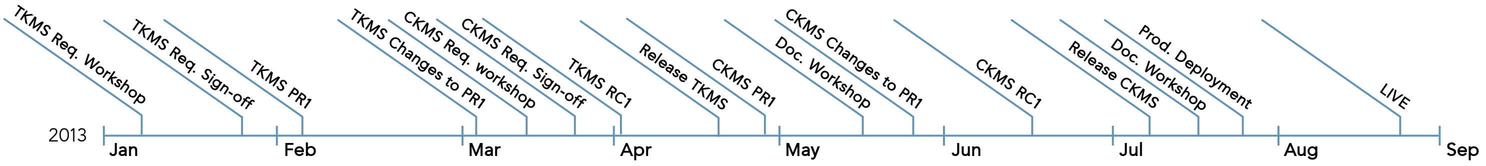
In addition to these drivers, because the legacy system was quickly approaching end of life, Swedbank needed to identify a vendor who could reliably deliver a replacement solution to a demanding set of requirements within a short space of time.

FINDING A NEW SOLUTION

As well as needing a key management system that could manage keys for card payment acquiring systems, Swedbank needed a system to derive keys for EFTPOS card payment terminals according to Swedish standards. Some proprietary key formats related thereto were also required.

Swedbank looked to existing vendors and the wider market for potential solution partners. Several companies claiming to offer life cycle key management solutions for the banking sector were identified. Due to the functionality of its CKMS solution, its reputation in delivering complex security solutions, its unrivalled expertise in banking key management and open attitude to customer needs, Cryptomathic was chosen as the supplier for both systems. In selecting CKMS, Swedbank were investing in a key management solution specifically designed for the banking market. This investment would allow Swedbank to benefit from a comprehensive set of features that Cryptomathic has developed over many years by working closely with a broad customer base of high profile banks, card payment schemes and processors.

This industry-focused evolution has resulted in CKMS growing into a mature, all-encompassing key management solution based on a distributed architecture – the only truly centralized product on the market today. Where previously operators had to be in the same place at the same time to perform key management tasks, CKMS provides easy to use lifecycle key management with a unique asynchronous workflow that allows operators to perform tasks in a much more flexible way, at different times, from different places. Secure authentication of operators and a completely customizable role based access control system add further flexibility, enabling Swedbank to mold CKMS to the specific requirements of their business. A history of every action performed on a given key – when and by whom – coupled with the use of banking grade HSM technology and secure tamper evident logging has enabled Swedbank to easily demonstrate compliance to its regulators.



CRYPTOMATHIC CKMS

The standard CKMS solution is central to the overall architecture. CKMS manages keys for Swedbank's own card issuing and authorization systems as well as thousands of keys for more than fifty partners in their card payment acquirer network. CKMS also manages the base derivation keys for TKMS.

Swedbank distributes keys to a large number of external organizations in a wide range of formats. While CKMS already had support for a large number of these formats off-the-shelf, some minor enhancements were made and added to the standard product for the benefit of Cryptomathic's entire CKMS customer base.

CRYPTOMATHIC TKMS

TKMS is responsible for deriving keys for EFTPOS payment terminals. TKMS was delivered as a completely new solution, based on the proven CKMS security architecture. The base derivation keys are managed within CKMS and distributed to TKMS. Managing these keys in CKMS provides for centralized control of meta data and lifecycle key management. TKMS uses the base derivation keys to derive sets of keys that are output in encrypted parameter files according to Swedish card payment standards. The parameter files are then picked up by another system and loaded onto the payment terminals to complete the provisioning process before they are distributed to merchants.

TKMS complements CKMS and together they provide the best and truly centralized key management system for the Swedish banking market.

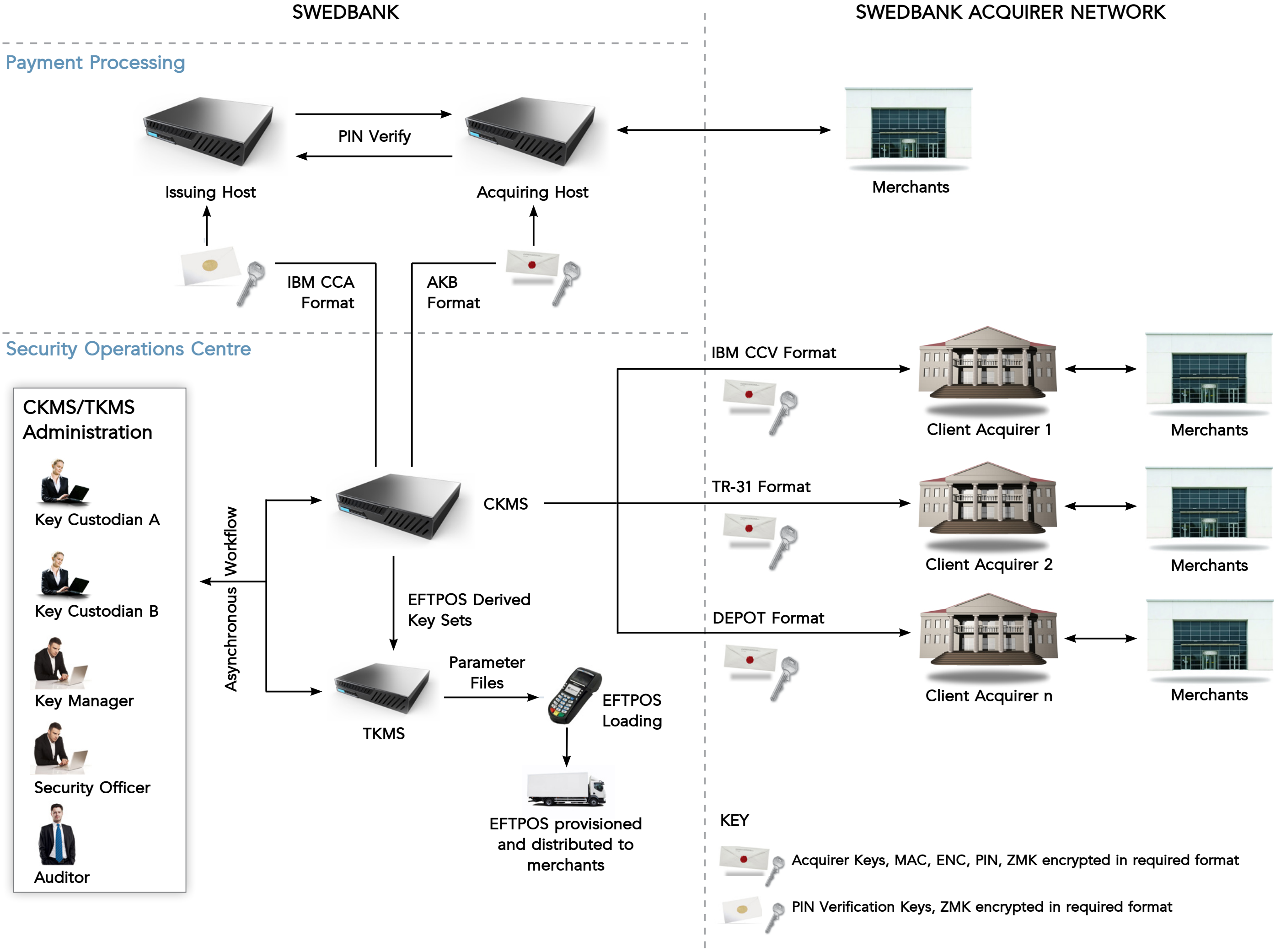
SOLUTION BENEFITS

Lifecycle Key Management

Within CKMS, for every action, there must be an approval. While availability of staff can often delay key management activities, Swedbank now benefits from the CKMS asynchronous key management workflow. This enables operators to split a key ceremony into separate parts, with each operator doing their task when they are available. This flexibility has enabled Swedbank to design key management procedures that are less disruptive to the business, while ensuring that no single operator can proceed though the key management lifecycle without the approval of a second operator. In turn, more of the operator's valuable time is free to be allocated to other tasks.

Compliance

A key management documentation framework allows Swedbank to quickly demonstrate its key management systems are being operated in an effective manner, according to design, and in-line with regulations.



The Swedbank project team and Cryptomathic drew upon many years of experience in cryptographic key management to design and develop the critical processes and procedures that make up such a framework. The documentation framework provides the ability to reliably check at any time that the system is operating as intended. Both CKMS and TKMS provide audit logs that record every operator action performed on the system. Global audit logs show a complete view of actions, while a history of lifecycle changes are kept with each individual key, providing a more direct route to investigation. All logs are integrity protected using keys stored in an HSM.

The overall solution enables Swedbank to not only meet its security and compliance obligations to the regulators, but it also provides the ability to quickly adapt to changes in policy and the regulatory landscape.

Integrity Through Interoperability

Swedbank is now able to support the full range of key files used by its card acquiring customers and its internal card payment host. This level of interoperability enables Swedbank to maintain closer control over the usage of keys, avoiding risky or error prone reformatting of key data during distribution and thereby preserving the integrity of keys. Maintaining the integrity of keys in this way significantly reduces the risk of compromise, which in turn significantly increases the overall security of the key management system.

Management Information

With such a large customer base across many countries, the ability to provide detailed management information was a core requirement. The comprehensive reporting systems built into CKMS and TKMS provide Swedbank with all the information it requires to support critical management processes.

Cryptomathic Secure Code Execution (SCE)

Cryptomathic's SCE HSM applications extend the CKMS and TKMS server process to run inside the HSM. SCE technology is critical to the overall security design of the solution, ensuring that all security sensitive operations are executed atomically within the confines of the HSM. Cryptomathic's unique position in the market as experts in writing software for multiple brands of HSMs ensures that the confidentiality and the integrity of keys and data is preserved. This unique market position provides Swedbank with the benefit of truly best-of-breed banking key management.

Scalable for the Future

Together, CKMS and TKMS currently manage millions of keys. As this figure grows, Swedbank can move forward safe in the knowledge the system can scale indefinitely.

THE PROJECT

Cryptomathic had to deliver a new version of CKMS and the completely new custom solution in TKMS against a very aggressive time frame. Both solutions were delivered on time and on budget within 9 months against a deadline which culminated in a critical VISA audit to meet compliance requirements.

A series of workshops were held throughout the project lifecycle. Initial workshops were spent defining detailed requirements, which resulted in minor enhancements to CKMS, and then the larger task of defining detailed requirements for TKMS. Workshops held later in the project were specifically focused on designing the new processes and a procedural documentation framework according to Swedbank's unique business environment.

Detailed requirement specifications were completed and signed off, allowing Cryptomathic R&D to quickly commence work. Development proceeded in sprints, and pre-releases were shipped to Swedbank at regular intervals. Swedbank rigorously tested each pre-release according to specification, taking the opportunity to fine-tune their requirements and feed them back in to the development process. Cryptomathic's experience in effectively delivering projects in this manner shone through against an ambitious project timeline, and undoubtedly proved to be the basis for a timely delivery.

Development environments were built at Swedbank IT to enable the Swedbank team to complete a comprehensive acceptance test of both CKMS and TKMS. Test and production environments were built, systems were initialized and key management ceremonies were held according to the strict procedural control devised during the workshop phase of the project.

As part of the delivery, Cryptomathic designed and delivered a tailored training and awareness course for Swedbank security operations staff. This process was the final stage of the project, ensuring that the new systems were correctly operated moving forward.

CONCLUSION

Cryptomathic and Swedbank worked together to deploy a truly centralized key management system for Swedbank's entire payment card processing systems. The expertise and experience of both companies was evident throughout as the project was delivered against an aggressive time scale on schedule and on budget. Both Cryptomathic and Swedbank are happy with the outcome of the project, and look forward to a continued successful partnership in the years to come, with further enhancements planned.

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.

Learn more at cryptomathic.com

v1.0