

CENTRALISED KEY MANAGEMENT

Today MasterCard Europe benefits from a fully automated and centralised key management system developed by Cryptomathic. Every member bank has a number of hardware security modules that are now fully managed and handled centrally from Brussels.

KEY MANAGEMENT CENTRE TO MASTERCARD EUROPE



MasterCard Europe

MasterCard Europe is a European banking organisation which owns and manages many of the most commonly used payment systems, including Maestro, EC (EuroCheque), Cirrus, CLIP and Eurocard. MasterCard Europe is a subsidiary of Mastercard Corp.

Managing the Keys

MasterCard Europe used to put much effort into maintaining the keys in their network. They had staff employed that would travel between their hundreds of member banks and update the keys in their network by entering them manually into each box in the distributed network. Today they manage this process centrally from their secured operations venue with multiple and secure user authentication, each with their unique administrative role and credentials. From here the operators can update and configure the cryptographic keys on each individual Network Security Platform (NSP) as well as enter new, shared network keys into all boxes with just a click on a button.

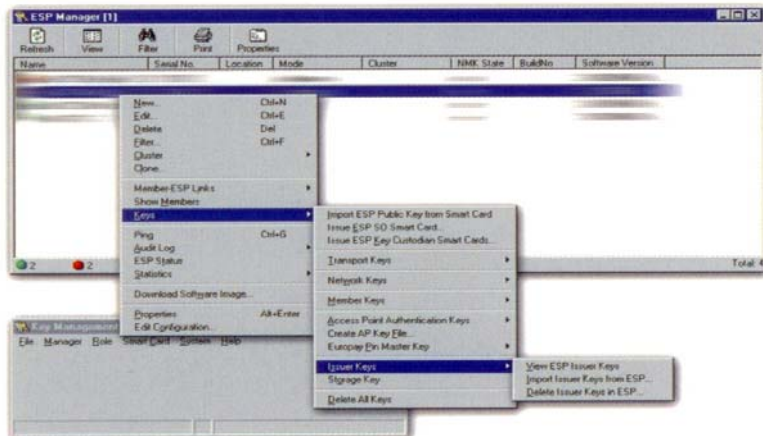
Updating the Keys

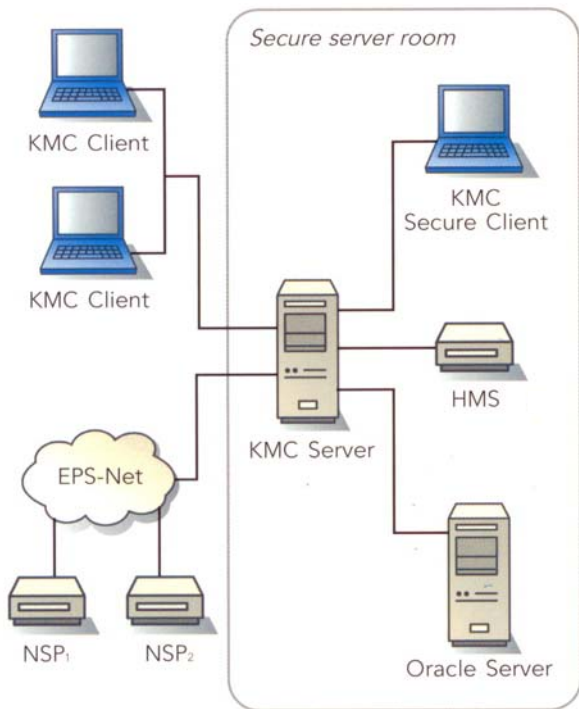
When using cryptographic keys for high volumes of sensitive data, it is important to change the encryption keys at regular intervals. These network keys are used by all NSPs to communicate within their own virtual network. When the keys are updated, it is of utmost importance that they are updated on as many NSPs as possible and in as short time as possible. At the same time, it is important that all events are logged securely and that the Key Management Centre (KMC) allows the administrators to communicate with each NSP individually to ensure that all communication to and from the NSPs and the KMC is non-repudable.

Jean Paul Boly
MasterCard Europe

With the Key Management Centre we are able to reduce costs while increasing both network security and performance. We chose to outsource the design and development of the KMC to Cryptomathic due to their extensive knowledge and strong market position within e-Security – especially cryptography. It was important to us that all relevant de facto and industry standards were followed to ensure interoperability throughout the network and to guarantee our member banks a cost-efficient and highly secure infrastructure."

"The KMC is an extremely useful tool for updating and maintaining the security in our networks – this is a good example of the efficiency that allows us to stay in the lead."





Solution Overview

The KMC system is built around a three-tier architecture with an application server (KMC Server), which provides services for a number of client applications (KMC Client). An Oracle database server is used as repository for the system. The KMC Server has a network interface to the NSPs and uses a hardware security module to secure all keys.

The KMC system is primarily used for managing the system keys, e.g.:

- generating and updating keys for the NSPs
- importing and distributing keys from the member banks
- performing key back up and recovery

Secondly, the operators use the system to monitor the availability and performance of the NSPs. This is done by:

- checking the NSP status
- validating and importing NSP statistics
- backing up audit log information from the NSPs for archival purposes

Strong User Authentication

Secure operations have been a design goal from the beginning of the project. The KMC Server is located on a physically secured operations site to which only a limited number of system operators have access. Smart cards are used in order to provide strong user authentication. All sensitive operations must be performed within the secured area and with the presence of multiple operators. All non-sensitive operations can be carried out by auditors and operators who are not allowed on the secured operations site.

The first version of the KMC system was introduced in the spring of 2000. Since then the system has been continuously extended and enhanced. The KMC system allows a high degree of flexibility while preserving the highest level of security for operating the Network Security Platforms.

Name	Member ID	Location	Key Service	MS	CC	EP
900000001	900000001		Transport Key RSA			
900000013	900000013		Transport Key RSA			
900000015	900000015		Transport Key RSA	1		
900000016	900000016		Transport Key RSA	1		
900000017	900000017		Transport Key RSA			
900000019	900000019		Transport Key RSA			1
900000020	900000020		Transport Key RSA			1
900000021	900000021		Transport Key RSA			
900000022	900000022		Transport Key RSA	3	5	7
900000023	900000023		Transport Key RSA		20	28
900000024	900000024		Transport Key RSA	3	5	7
900000002	900000002		Transport Key RSA			
900000001	900000001		Transport Key RSA			
900000004	900000004		Transport Key RSA			
900000003	900000003		Transport Key RSA			

Key ID	PIAN Low	PIAN High	Expiry Date	Key Name	Service	Live/Test	Imported
00014	00000000000000000001	00000000000000000004	1211	Key type: K3I	Electronic Purse Integrity	Test	On-Behal
00015	00000000000000000001	00000000000000000004	1211	Key type: AC	EMV Authentication	Test	On-Behal
00011	00000000000000000001	00000000000000000004	1211	Key type: KDP	Electronic Purse Purchase	Test	On-Behal
00012	00000000000000000001	00000000000000000004	1211	Key type: K3L	Electronic Purse Validation	Test	On-Behal
00013	00000000000000000001	00000000000000000004	1211	Key type: KDL	Electronic Purse Load Aut.	Test	On-Behal
00009	00000000000000000001	00000000000000000004	1211	Key type: DN	EMV Dynamic Validation	Test	On-Behal
00008	00000000000000000001	00000000000000000004	1211	Key type: SMC	EMV Confidentiality	Test	On-Behal
00010	00000000000000000001	00000000000000000004	1211	Key type: PAK	PIN Validation, Mag. Stripe	Test	On-Behal
00005	00000000000000000001	00000000000000000004	1211	Key type: CVR1	CVC 1 Validation	Test	On-Behal
00006	00000000000000000001	00000000000000000004	1211	Key type: CSC	Electronic Purse Confidenc.	Test	On-Behal
00007	00000000000000000001	00000000000000000004	1211	Key type: SMI	EMV Integrity Generation	Test	On-Behal
00001	00000000000000000001	00000000000000000004	1211	Key type: K3V	Electronic Purse Currency	Test	On-Behal
00002	00000000000000000001	00000000000000000004	1211	Key type: CVR2	CVC 2 Validation	Test	On-Behal
00003	00000000000000000001	00000000000000000004	1711	Key type: KTV	Electronic Purse Parameters	Test	On-Behal

General Attributes:
 PIAN Low: 00000000000000000001 Expiry Date (MMYY): 1211 Key Set Reference: 2345
 PIAN High: 00000000000000000004 Mark Newly Imported Keys as Test Keys

Decision Matrix:
 If Invalid: [Approved] Decision Algorithm: [1 - Algorithm 1]
 If Non-Verifiable: [Approved] Session Key: [1 - Algorithm 2]

Height Of The Tree: [N/A] Branch Of The Tree: [0/0]

CRYPTOMATHIC PRODUCTS IN THE KEY MANAGEMENT SUITE

KEY MANAGEMENT SYSTEM

The Cryptomathic Key Management System (KMS) provides clients with a centralised solution to flexibly manage a very large number of keys throughout their entire life cycle - without drowning in work. Cryptomathic KMS has been designed to reduce the enormous increases in work-load and costs associated with traditional key management through its flexible and automated protocols that allow, for example, keys to be securely pushed to any key distribution target as and when required and for key custodians to use asynchronous log-on to projects to add components securely, reducing the need for key ceremonies. Cryptomathic KMS easily manages both symmetric keys and asymmetric key pairs using Cryptomathic KMS Key Projects—representation of the current state of a set of keys together with their history and general lifecycle management.



CRYPTOMATHIC SIGNER

Cryptomathic Signer is an innovation in digitally signing and certifying electronic documents, from emails through to pdf and any other document type. The basis of the solution differs from other PKI implementations in that the user does not have to carry their private key around with them or store it on their computer. Instead, they simply have to authenticate themselves to the service and sign the relevant electronic document within the server itself. This means that they are not only signing exactly what they see but they also maintain the security of the private signing key.

CRYPTOMATHIC AUTHENTICATOR

The Authenticator is an independent authentication server. Firstly, it is independent of token suppliers so customers are not tied to any particular authentication vendors or technologies when choosing the Authenticator. Secondly, the same level of independence applies to HSMs, allowing the Authenticator to support the customer's preferred HSM brands and models.

Through a wide and growing range of user and transaction authentication methods, the Authenticator is able to adapt to future requirements and safeguard the value of the initial investment. It is also possible to provide your customer base with tokens that meet their individual needs without the need for additional infrastructure costs. For example: high risk customers could be provided with tokens based on more complex authentication techniques or even multiple authentication techniques, while low risk customers could be issued with tokens using less complex authentication therefore maximising protection while also minimising costs. Cryptomathic Authenticator allows the business to tailor the authentication needs across the business and to migrate between authentication mechanisms as the prevalent fraud migrates.



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 over 20 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