



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.

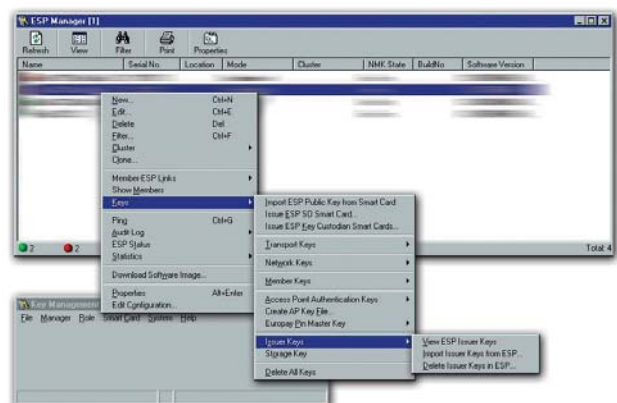
Updating the Keys

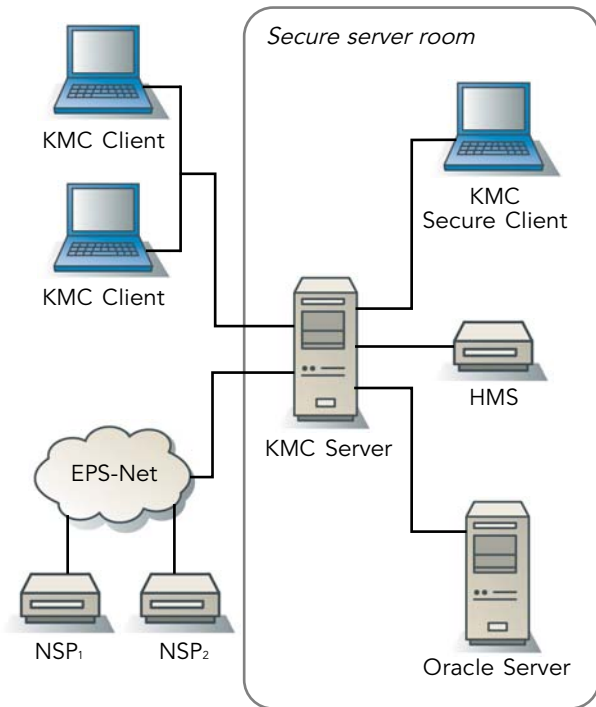
When using cryptographic keys for high volumes of sensitive data, it is important to change the encryption keys at regular intervals. These network keys are used by all NSPs to communicate within their own virtual network. When the keys are updated, it is of utmost importance that they are updated on 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.

Name	Member ID	Location	Key Service	MS	CL	EP
900000012	900000012		Transport Key RSA			
900000013	900000013		Transport Key RSA			
900000015	900000015		Transport Key RSA			
900000016	900000016		Transport Key RSA			
900000017	900000017		Transport Key RSA			
900000019	900000019		Transport Key RSA			
900000020	900000020		Transport Key RSA			
900000021	900000021		Transport Key RSA			
900000022	900000022		Transport Key RSA	3	5	7
900000023	900000023		Transport Key RSA	3	5	7
900000024	900000024		Transport Key RSA	3	5	7
900000032	900000032		Transport Key RSA			
900000031	900000031		Transport Key RSA			
900000034	900000034		Transport Key RSA			
900000035	900000035		Transport Key RSA			

Key ID	PAN Low	PAN High	Expiry Date	Key Name	Service	Use/Test	Imported
00014	0000000000000001	0000000000000004	12/1	Key type KSL	Electronic Purse Integrity	Test	On-Behalf
00015	0000000000000001	0000000000000004	12/1	Key type AC	EMV Authentication	Test	On-Behalf
00011	0000000000000001	0000000000000004	12/1	Key type SSP	Electronic Purse Purchase	Test	On-Behalf
00012	0000000000000001	0000000000000004	12/1	Key type KSL	Electronic Purse Validation	Test	On-Behalf
00013	0000000000000001	0000000000000004	12/1	Key type KSL	Electronic Purse Load Aut.	Test	On-Behalf
00018	0000000000000001	0000000000000004	12/1	Key type EM	EMV Dynamic Validation	Test	On-Behalf
00019	0000000000000001	0000000000000004	12/1	Key type SMC	EMV Confidentiality	Test	On-Behalf
00010	0000000000000001	0000000000000004	12/1	Key type PSL	PSM Validation, Mag Stripe	Test	On-Behalf
00005	0000000000000001	0000000000000004	12/1	Key type CVK1	CVK 1 Validation	Test	On-Behalf
00006	0000000000000001	0000000000000004	12/1	Key type KSC	Electronic Purse Confidential	Test	On-Behalf
00007	0000000000000001	0000000000000004	12/1	Key type SML	EMV Integrity Generation	Test	On-Behalf
00011	0000000000000001	0000000000000004	12/1	Key type KSL	Electronic Purse Delivery	Test	On-Behalf
00012	0000000000000001	0000000000000004	12/1	Key type CVK2	CVK 2 Validation	Test	On-Behalf
00013	0000000000000001	0000000000000004	12/1	Key type KSC	Electronic Purse Purchase	Test	On-Behalf

General Attributes:
 PAN Low: 0000000000000001
 PAN High: 0000000000000004
 Expiry Date (MM/YY): 12/1
 Key Set Reference: 2045
 Mark Newly Imported Keys as Test Keys.

Decision Matrix:
 If Invalid: [Dropdown]
 If Non-Verifiable: [Dropdown]

Derivation Algorithm:
 ICC Master Key: [Dropdown]
 Session Key: [Dropdown]

Height Of The Tree: [Input: 10]
 Branch Of The Tree: [Input: 10]

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 keys 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.

Nordic

Cryptomathic A/S (HQ)
Jægergårdsgade 118
DK-8000 Aarhus C
Denmark
Tel. +45 8676 2288
Fax +45 8620 2975

Cryptomathic A/S
Christians Brygge 28
DK-1559 Copenhagen V
Denmark
Tel. +45 8676 2288
Fax +45 3333 9756

Benelux

Cryptomathic NV
Interleuvenlaan 62 / box 19
B-3001 Leuven
Belgium
Tel. +32 (0) 16 394 822
Fax +32 (0) 16 394 821

Germany

Cryptomathic GmbH
Bretonischer Ring 7
D-85630 Grasbrunn
Germany
Tel. +49 (89) 451 8740
Fax +49 (89) 451 8741

UK/Ireland

Cryptomathic Ltd
329 Cambridge Science Park
Milton Road
Cambridge CB4 0WG
United Kingdom
Tel. +44 (0) 1223 225350
Fax +44 (0) 1223 225351



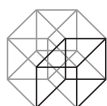
About Cryptomathic

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 almost 20 years of experience, we have assisted our customers by providing systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing, and advanced key management through best-of-breed security software and services.

Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with its established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

www.cryptomathic.com

**CRYPTOMATHIC**

www.cryptomathic.com