CRYPTOMATHIC
www.cryptomathic.com

CardInk Case Study - Crédit Agricole

EUROPEAN MULTI-APPLICATION EMV CARDS

Crédit Agricole has undertaken one of the world's biggest multi-application EMV issuing projects to date. Every fourth cardholding bank customer in France is receiving new chip-enabled credit and debit cards for domestic and international use from Crédit Agricole. The project has been one of the first to implement Common Personalization—a new standard introduced by Visa International and set forth by EMVCo.

CEDICAM AND EMV MIGRATION

CEDICAM (Centre d'Échanges de Données et d'Informations du Crédit Agricole Mutuel) is jointly owned by Crédit Agricole S.A. and the Crédit Agricole Regional Banks. The company is the Crédit Agricole Group's specialist in automated payment systems and management of financial flows.

CEDICAM has been commissioned to issue the new EMV credit and debit cards to the entire card base of Crédit Agricole, which holds more than 12 million cards. The new cards feature domestic and international applications as well as an e-purse.

The EMV migration began in the last quarter of 2004 with EMV 96 SDA (Static Data Authentication) cards and CEDICAM plans to issue EMV 2000 DDA (Dynamic Data Authentication) cards in the second quarter of 2006. Future plans include preparing the cards for the MasterCard CAP (Card Authentication Protocol) application for use of the cards with unconnected token-readers for high security internet banking before the end of 2005.

Crédit Agricole has previously been issuing chip payment cards to its clients and though these are generally accepted today for domestic transactions, they are not EMV compliant. The bank is now combining the existing cards with EMV chip applications in line with the 2005 European deadline set forward by MasterCard and VISA. EMV compliance ensures that card applications comply with the payment systems while guaranteeing security and interoperability.

CEDICAM has upgraded its card product platform to EMV, and Cryptomathic was selected to deliver a solution that meets the new requirements in the existing environment. Cryptomathic was able to meet the challenges posed by CEDICAM by offering maximum security and the latest technology, e.g. Common Personalization and DDA, while allowing CEDICAM to integrate the solution into the local French banking environment – customised for national needs and purposes.

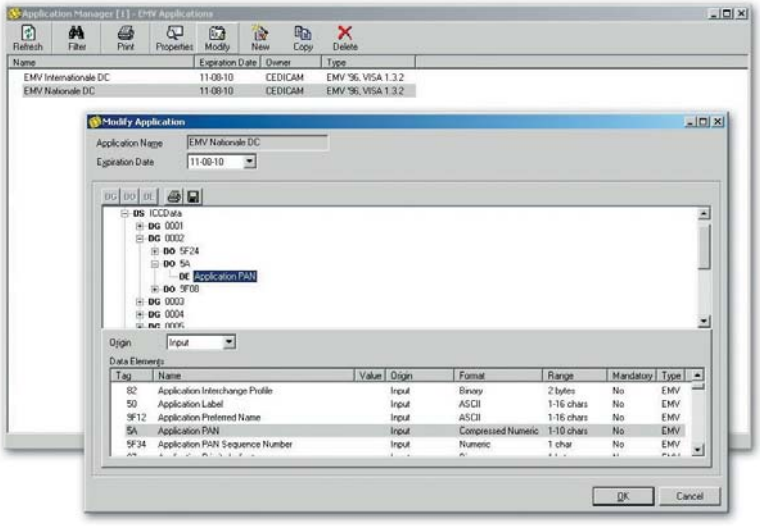
Fabrice Piau,
Security Officer, CEDICAM

Crédit Agricole has successfully achieved to manage the high level of security required for issuing EMV cards with the implementation of CardInk while maintaining the highest level of flexibility in the production line."

Single Card – Multiple Applications

CEDICAM issues multi-application smart cards which carry the French applications B0' and Moneo, as well as both a domestic and an International EMV debit and credit application - either VISA or MasterCard depending on the card brand. CEDICAM is an experienced pioneer in smart cards and is very successful in leveraging the benefits of multi-application smart cards, which create value to both card holders and card issuers over single-application cards.

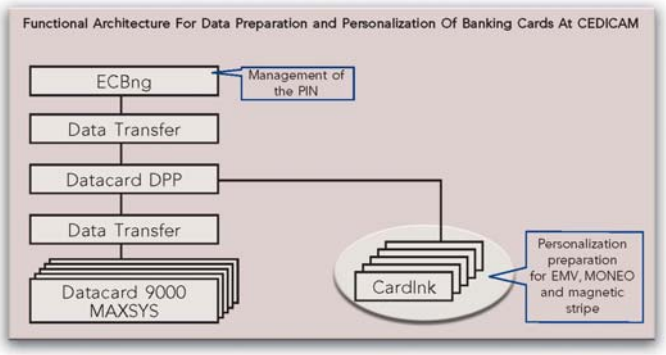
One of the features that provide smart card holders with real value is the possibility of having several applications residing on one payment card. It also adds customer value by offering card holders a wide range of functions. The issuing banks benefit from multi-application cards because they can target individual card holders, which is essential for building strong customer relationships and reducing marketing costs.



Solution Overview

The solution chosen by CEDICAM is Cryptomathic CardInk, a second-generation data preparation system. BULL is the prime contractor and integrator and provides the technical support.

The production involves a number of entities. CardInk performs the data preparation for EMV, Moneo and the magnetic stripe data. The Datacard DPP (Data Preparation Process) is used to manage the entire card production process, which is completely automated. CardInk is integrated into the DPP as a black box. The data produced by CardInk is written onto smart cards by a series of high volume DC 9000 and MAXSYS personalization systems.

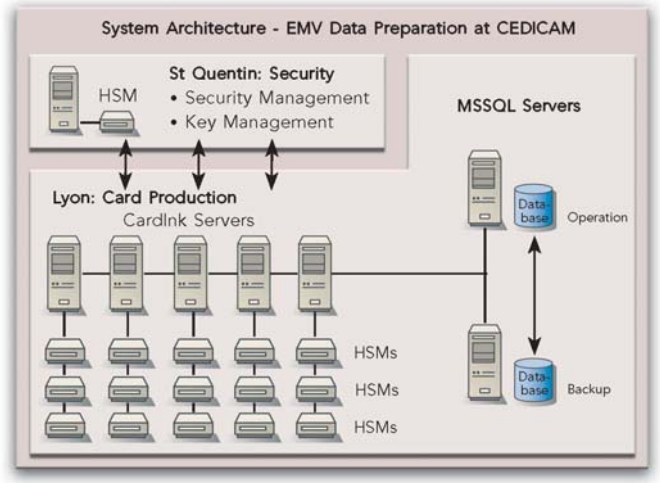


Solution Implementation

Cryptomathic meets the requirements of CEDICAM through a scalable and flexible data preparation solution while exceeding security standards imposed by the payment scheme providers and the national banking organisation.

CardInk is developed as a two-part client/server system. While the cryptographic keys and overall security are managed in CEDICAM's main location, the production site is located in another area of France. This physical separation between operations is possible through the configuration of separate CardInk installations which support one-time set-up and remote management.

The ultimate production requirement at CEDICAM is almost 100,000 multi-application smart cards per day. This high capacity is ensured by a solution consisting of several CardInk servers that operate in parallel. Each server is capable of preparing data for several thousands of multi-application smart cards each hour. The servers are synchronised and the production environment is very redundant. The approach is modularly scalable and allows for higher capacities in relation to future issuing requirements.



Secure Issuing and System Management

With the support for DDA, the cards issued by CEDICAM have maximum security. DDA denotes the type of authentication used during transactions and is the highest possible level of security within EMV. DDA requires that a "private" key used for securing card integrity and encrypting information, e.g. PIN-codes, resides on each card.

To accommodate this functionality, CEDICAM has chosen an architecture consisting of five CardInk servers with fifteen IBM4758 HSMs (Hardware Security Modules). HSMs are used to handle cryptographic data in a highly secure tamper-resistant environment so that the keys will never be disclosed in clear text.

The CardInk security architecture enables CEDICAM to manage cryptographic keys on a CardInk key management server and distribute them onto CardInk production servers by encrypting key files.

On the key management server, keys are loaded into HSMs via secure PIN-pads that are interfaced directly with the HSM. This adds security and eliminates risks as CEDICAM only uses trusted clients.

The standard security of CardInk is also compliant with CEDICAM's internal procedures, where security management and daily production are physically separated. Audit logs are MAC'ed and encrypted, and the secure client server communication uses AES for encryption.

Finally, CardInk supports exchange of cryptographic keys with the French bank organisation Groupement des Cartes Bancaires. This exchange is mediated through the BULL system CGDC-BNTng.

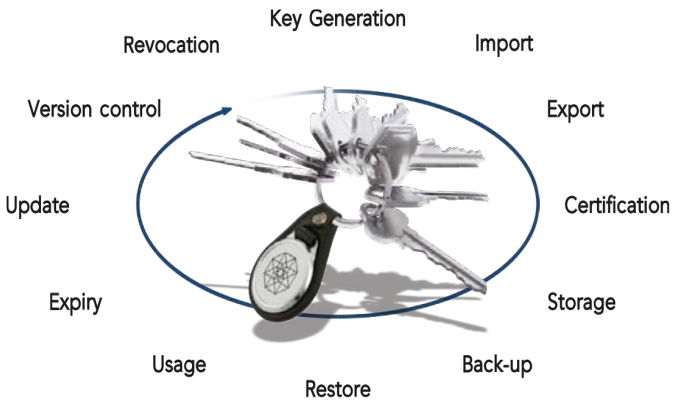
CRYPTOMATHIC PRODUCTS IN THE EMV PRODUCT SUITE

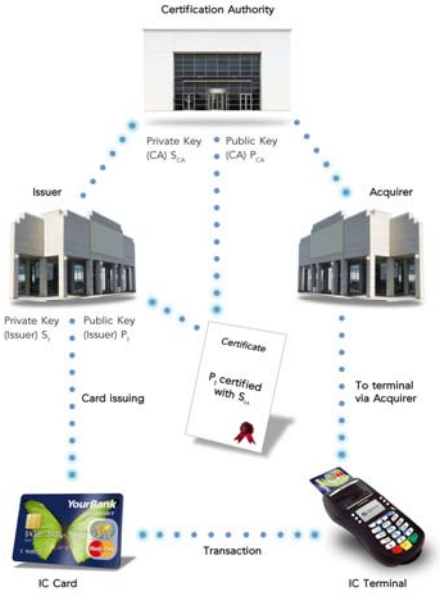
CRYPTOMATHIC CARDINK

Cryptomathic CardInk is a data preparation system (data formatting and key management), which offers exactly that while maintaining flexibility to meet any card issuing environment (e.g. mag stripe, chip, single- and multi-applications, instant issuing). CardInk is implemented by bureaus, data processors and card issuers alike and is the only major system that is both HSM vendor and card platform independent. This ensures that customers are not tied in to one particular technology and hence ensures a high return on investment. Cryptomathic CardInk supports a wide number of applications including MasterCard, Visa, AmEx and integrates with systems such as those from ACI Worldwide, Böwe Cardtec, Mühlbauer and Datacard. Cryptomathic CardInk is very scalable and not only perfect for high volume central issuance but it is also suitable for instant issuance.

CRYPTOMATHIC KMS

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 EMV CA

The Cryptomathic EMV CA is an essential service component for EMV card authentication. The main purpose of the EMV CA is to allow a central authority to issue and manage the certificates of Card Issuers within a given region. EMV card authentication is based on PKI (Public Key Infrastructure) but unlike traditional PKI, which is based on a standard called X.509, EMV is a standard of its own. Even though EMV is a proprietary standard it is widely used across the globe, with billions of EMV smart cards issued since its initial roll-out. Cryptomathic EMV CA is designed in a flexible client -server structure enabling the payment scheme provider to tailor the system to the specific needs of its organisation. The Cryptomathic EMV CA professionally manages all the Issuer and Certification Authority's tasks and offers all the features expected from professional trust management software including, multiple CAs, secure user administration, and performance all sensitive cryptographic operations within HSMs.

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, Cryptomahtic 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 prodes 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