# CRYPTOMATHIC

ELAN FINANCIAL SERVICES AND EMV SUCCESS
POWERED BY CRYPTOMATHIC

ELAN MIGRATES ITS CARD ISSUANCE TO EMV WHILE AUTOMATING ITS ACQUIRING AND PROCESSING SERVICES

Elan Financial Services®, a leasing service provider for VISA®, and MasterCard®, debit and credit card issuing and acquiring in the U.S, completed the transition to EMV®,, while also upgrading its systems to deliver faster and more versatile contact and contactless payment card services for its customers. Elan is now able to securely support the bespoke EMV payment card requirements for their numerous financial services customers. The solution automates EMV contact and contactless data preparation, crypto key management and transaction authorization for improved efficiency and end-customer flexibility.

The significant increase of complex cryptographic processes involved in EMV issuing and acquiring needed a whole new set of components to be integrated with existing Elan processing platform and back-office systems. To ensure a successful migration, Elan chose EMV and cryptographic expert, Cryptomathic, to deliver the complete solution for issuing EMV contact and contactless chip payment cards, as well as authorization of these transactions. As part of the EMV migration, the system provided by Cryptomathic also allows Elan clients to offer instant issuance of EMV contact and contactless cards to their own customers in local bank branches.
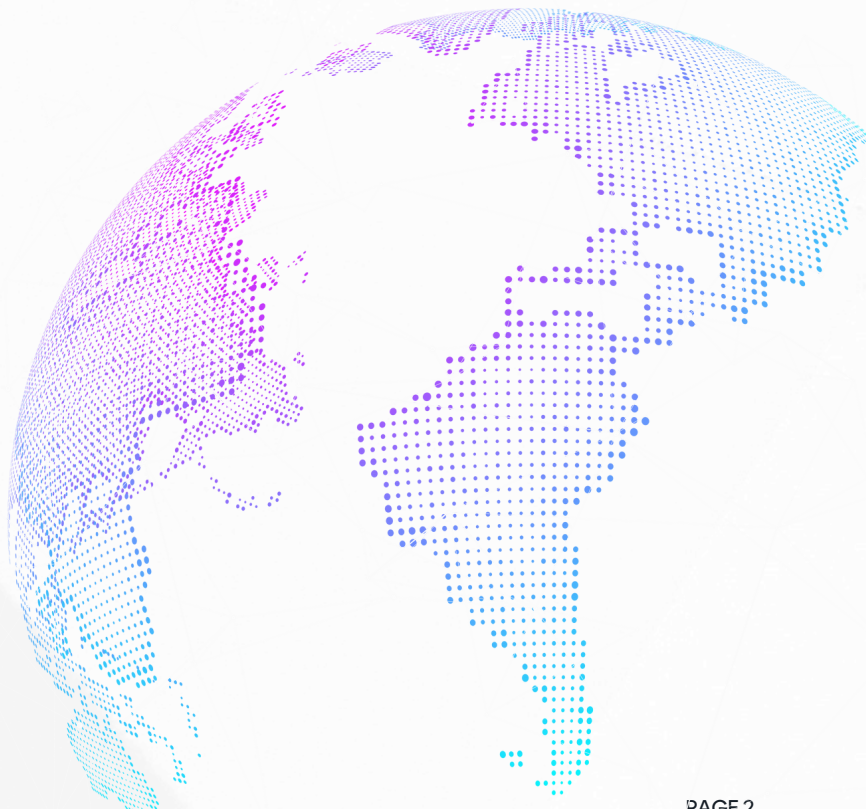
ELAN FINANCIAL SERVICES

Elan Financial Services is part of U.S. Bancorp and provides ATM and Debit processing services to clients nationwide. These services include an array of Electronic Fund Transfer (EFT) processing solutions such as ATM processing, bank and debit card POS processing, ATM network membership, ATM and POS gateway services, and turnkey ATM managed services. Elan also owns and operates the MoneyPass® Network.

In addition, Elan provides support and program management including ATM, Debit and Credit card issuance and management, network communications monitoring, comprehensive fraud monitoring tools, web-based program administration, and a full rand of client support services. Elan products and services enable clients to provide their cardholders with access to their demand deposit and line of credit accounts at national and international locations. The approximately 2,000 clients of Elan include banks, credit unions, savings and loans associations, core processors, networks, independent service organizations (ISOs), and merchant processors.

THE CHALLENGE & REQUIREMENTS

To maintain its leadership role in the Payments industry, Elan migrated its systems to be able to process EMV contact and contactless transactions and enable clients to issue Visa and MasterCard EMV cards.

This project went beyond merely supporting EMV: Elan wanted to simplify the EMV migration process while providing more value-added and flexible services for its clients. Elan created several strategic and operational requirements for the new EMV system.

Strategic Requirements:

- Migrate the current Visa and MasterCard magnetic stripe card system to EMV contact and contactless technology for both online and offline transaction processing.
- Support central EMV contact and contactless issuance for multiple card bureaus, as well as instant issuance at local branches.
- Meet all EMV contact and contactless key and card management requirements.

Operational Requirements:

- Automatically select from a set of Visa and MasterCard card profiles for various BIN ranges.
- Prepare complete EMV contact and contactless data for card personalization - including all the cardholder data and keys/certificates required.
- Process and authorize EMV contact and contactless transactions.

As a high priority, it was necessary to deliver all of the above with the minimum disruptions to the current Elan systems.

> " With Cryptomathic's issuing and authentication solution, Elan is now providing an integrated solution that delivers the end-to-end EMV environment, from card issuance to payment authorization. This is a great benefit for Elan and our clients - improving efficiency and security while achieving compliance. "
>
> **Troy Cullen**
> **President & General Manager for ATM & Debit Services, Elan Financial Services**

THE SOLUTION

Elan required flexibility in offering numerous Visa and MasterCard EMV contact and contactless chip card profile options. A complex arrangement was needed to securely manage multiple EMV Issuer key sets through the life-cycle, with the ability to perform EMV authentication and cryptogram validation on credit and debit transactions.

Cryptomathic was able to integrate individual best-of-breed products together with customized application logic to create a system offering fast EMV migration with unified overview and control, thereby completely satisfying the strategic and operational requirements. This approach gave the benefits of robust and industry-proven components for the specific functions of card preparation and

key management, together with easy-to-integrate connections to existing systems and processes. The solution establishes a unified and coherent path from card issuing through to processing and authorization, while efficiently orchestrating the required key management for security, high availability and performance.

SOLUTION COMPONENTS

Elan implemented Cryptomathic's BMS, CardInk, CSG and CKMS to deliver the comprehensive solution for their EMV requirements. These individual components and their functions are explained in the following sections.

BIN Management Systems (BMS)

BMS is a web-based application for business-line staff that allows on-boarding of issuers and the selection of multiple Visa and MasterCard EMV contact and contactless card profiles. It automates the process and reduces the onboarding lead-time.

When required, the BMS also provides granular controls, enabling the business users to create specific Visa and MasterCard card profiles for each BIN range for their card products.

Once the data base is populated with the BIN, card profiles and Application Transaction Counter (ATC) parameters, then other system components can automatically obtain the profile details for each BIN requested.

CardInk - EMV Data Preparation System

Elan chose CardInk, an EMV data preparation system for single and multi-application EMV cards, to delivery the comprehensive, secure and versatile EMV data preparation from cardholder data. CardInk supports applications from all major payment brands, including MasterCard and Visa. As the Issuer's processor, Elan creates and stores Visa and MasterCard standard chip card profiles within Cryptomathic's data preparation system. Through CardInk, Elan now has the ability to perform EMV key generation, key import and export, and protection of Issuer Master Keys (IMKs) within the security of Hardware Security Modules (HSMs). With EMV key management, Elan can control the cryptographic security keys associated with cards and manage the institution's entire card life-cycle.

Elan has expanded its Card Management services to include Chip Card Data Preparation and Key Management to ensure chip data elements and keys are configured correctly, meeting Visa and MasterCard profile certification standards. The data preparation or "pre-card personalization" solution offers flexibility in choosing from multiple Visa and MasterCard EMV profiles, including online Signature preferring, PIN preferring, and both contact and contactless.

Elan supports the educational training necessary to assure a smooth implementation. Furthermore, Elan will guide clients in chip card profile selection, BIN set-up and facilitate processes in which the card

data and keys are sent to clients' card bureau provider for personalization and testing.

Elan's card management system feeds data to CardInk, which outputs EMV data in standard formates, i.e. TLV and Common Personalization. CardInk output flies are supported by a variety of personalization systems, including Mühlbauer, Atlantic Zeiser, Datacard, CIM and Matica - and supports both central and instant issuance.

Crypto Service Gateway (CSG)

Elan chose Cryptomathic to build out its processing platform in support of chip card transactions with EMV Data Element Field 55, sent by the merchant and ATM acquirer for authorization. CSG expands the capabilities of Elan to include the interrogation of online cryptograms, and offline data authentication, to advise the card is authorized as genuine, defined by issuer-determined risk parameters.

CSG is a platform for the delivery of business agile & efficient crypto services. It provides central control of security policy and crypto hardware (HSMs), along with simple APIs for the consumption of both general purpose and financial crypto.

The CSG and its EMV extension (the Authorization System) deployed at Elan, facilitate the centralized management of HSMs, integration with third-party components (host platform) and comprehensive compliance demonstration through policy enforcement and detailed logging.
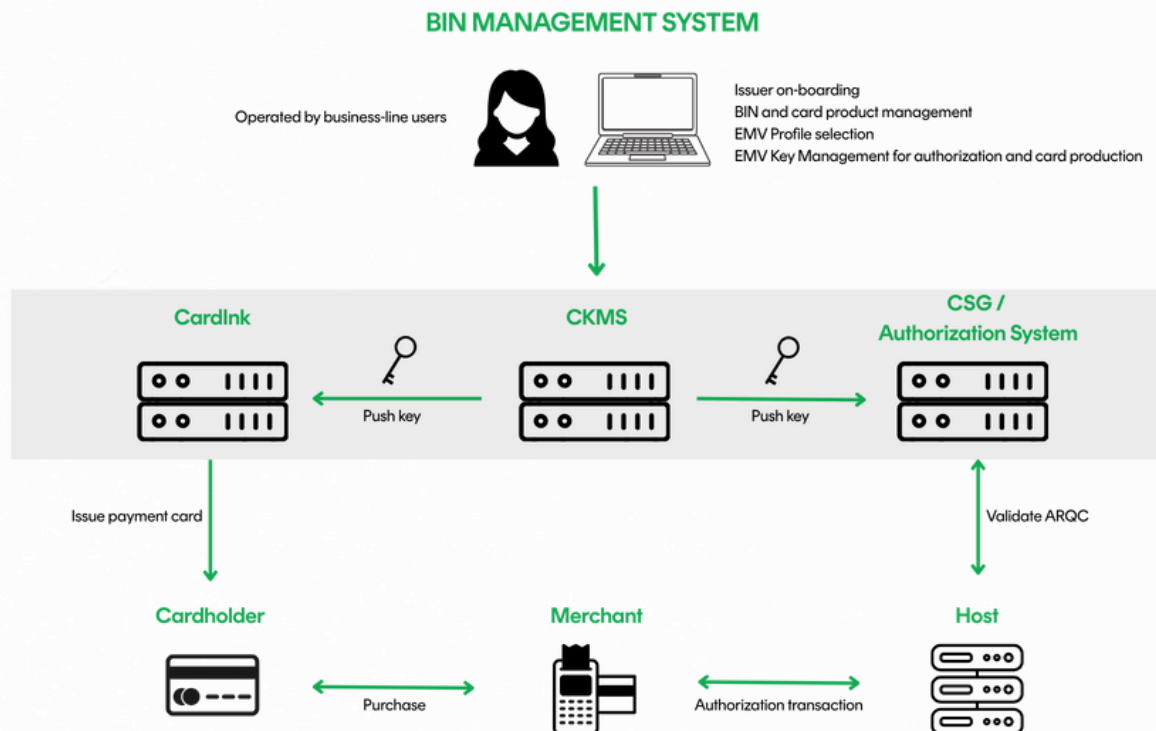
Deploying a secure CSG platform enables processors to easily develop additional CSG extensions which consume hardware-backed crypto without the time or costs associated with deploying new crypto without the time or costs associated with deploying new crypto hardware for every project.

Crypto Key Management System (CKMS)

CKMS is a centralized key management system that allows eland to manage the entire EMV key lifecycle. It includes generation distribution, usage, expiry, revocation and update of keys. In the context of this solution, it enables Elan to distribute keys automatically to Cardlnk and CSG. Web-services are also available to receive key requests from the BMS to automate the workflow of key generation. Manual key exchange with external third parties or issuers are also possible using either encrypted key files or components. Key management operations are performed synchronously or asynchronously via an intuitive GUI supported by secure PIN-pads and chip cards for strong authentication.

Issuer Processors, like Elan, are facing increased regulations and more complex system requirements for cryptographic keys largely imposed by credit and debit-card payment brands and Payment Card Industry (PCI) standards. They have to demonstrate compliance to the PCI-DSS requirements. CKMS also delivers tamper-evident audit logs to pass and simplify these PCI security audits.

BUSINESS PROCESSES

The solution delivered by Cryptomathic provides Elan with a flexible EMV infrastructure that supports end-to-end issuing and authorization processes.

The issue process includes:

1. The BMS is used to on-board new and existing issuers and to define new Visa and MasterCard Bank Identification Numbers (BINs) and the related EMV card profile(s)
2. Based on the BIN and card profile information, CKMS generates and distributes the keys required for card issuance and authorization
3. Cardlnk produces the data preparation file for personalization that is then sent to the card bureau.

The authorization process is as follows:

1. The authorization host receives the incoming transaction requests, which includes the Authorization Request Cryptogram (ARQC)
2. The host uses ISO8583 messaging to send the authorization request (ARQC) to the Crypto Service Gateway (CSG)
3. CSG validates the authorization request cryptogram received using its HSMs
4. CSG creates and send the Authorization Response Cryptogram to the host (ARPC). This response message may also include EMV scripting if it is required by the issuer.

Additionally, the solution provides the security team with more advanced and automated key management processes:

- Automated key generation based on BIN number and card profile
- Automated key distribution to card issuance and authorization systems
- Full control of key life-cycle
- Easier demonstration of compliance (PCI-DSS) using a centralized key management system with tamper-evident audit logs.

RESULTS

The migration project for Elan was all-encompassing, and complex with many different systems having to work together to accommodate the requirements set forth by Elan. Cryptomathic provided the solution for Elan that ensured a seamless migration of its card business to EMV, adding client value and addressing both the issuing side and the acquiring side for EMV contact and contactless cards and transactions.

One of the major challenges of the migration to EMV is the significant increase in the number of keys and crypto processing needed in order to secure the chip card and its transactions. This makes both the EMV card issuance and transaction acquiring much more complex than with magnetic stripe cards. The Cryptomathic solution enabled Elan to automate and centralize these key management processes while benefitting from quick and cost-effective demonstration of compliance to standards.

The use of well-designed Cryptomathic systems enabled the Elan project to be implemented earlier than anticipated with minimal disruption to magnetic stripe processing by Elan during the migration. The versatility of the systems allows Elan to easily match all client requirements and supports both instant and central EMV issuance from a single platform. This was a major requirement for Elan and a successful accomplishment for the Cryptomathic team.

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 30 years' experience, we provide systems for Authentication & Signing, EMV and Key Management, 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. 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.

www.cryptomathic.com   **enquiry@cryptomathic.com**