

## Cryptomathic CardInk Data Preparation System

### EMV Migration

The move from magnetic stripe to EMV is well underway with migration deadlines, i.e. liability shifts, set for most parts of the world. Card issuers are faced with large investments, increased competition and complicated technology. Therefore, they need solution partners with flexible offerings that support individual EMV migration strategies.

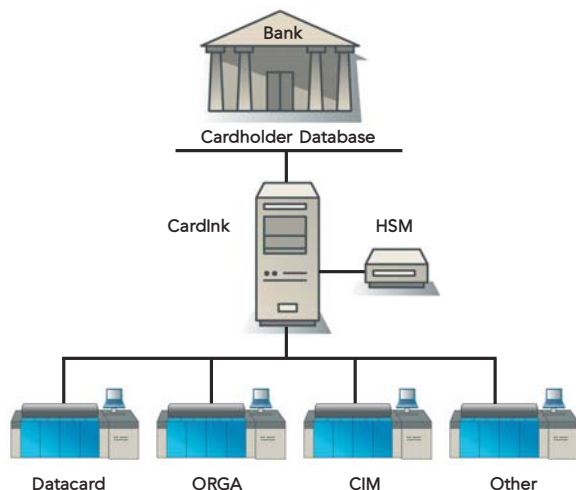
CardInk is a data preparation system for single- and multi-application EMV cards, designed to smooth the migration path and meet future business requirements. CardInk ensures secure data generation and key management based on banks' record files.

CardInk complies with the EMV standard and supports applications from major payment schemes, including MasterCard and Visa.

### System Architecture

CardInk is the second-generation EMV data preparation system from Cryptomathic. It has been developed in close cooperation with major international financial institutions and service suppliers to meet market demands.

CardInk can be used with the bank host system or in the card production bureau. The bank host, or a card management system, will feed data to CardInk, which will output EMV data in standard formats, i.e. P3 file and Common Personalization. CardInk output files are used on a variety of personalization systems, including Datacard, ORGA and CIM.

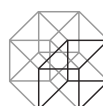


### Cryptomathic CardInk

**Card Issuer Flexibility** - CardInk is suitable for in-house card production. The system offers: security, stability, and low-maintenance and will suit almost any card strategy. CardInk interfaces with card management systems and is fully automated (using an API). This results in fast production, making data preparation an easy in-house task. CardInk works with a wide range of HSMs (Hardware Security Modules), integrating with card issuers' existing production environments.

**Card Bureau Flexibility** - CardInk is the most versatile data preparation solution available imposing no limitations on the numbers of cards issued or issuers supported, hence a high return of investment. The system is easy to set up, which means that bureaus can instantly issue cards across a number of different issuers and payment brands. CardInk integrates with all major personalization systems and supports a wide range of HSMs including the market's most cost-efficient.

**Key Management** - The core objective of CardInk is the management of cryptographic keys related to data preparation. All keys are handled in HSMs and CardInk provides secure import/export facilities. This applies to 3DES and RSA keys and includes end-to-end certificate management. CardInk supports certificate requests for application provider certificate authorities (MasterCard CA and VISA CA). The high level of security means that CardInk is the most secure data preparation system available. Security features include a secure audit log and secure remote client/server communication using AES encryption.



## Technical Specifications

### Applications Supported

- Visa VSDC SDA (VIS 1.3.2 / VIS 1.4.0)
- Visa VSDC DDA (VIS 1.3.2 / VIS 1.4.0)
- MasterCard M/Chip Lite (version 2.1 / version 4.0)
- MasterCard M/Chip Select (version 2.1 / version 4.0)
- MasterCard CLIP (CEPS version 2.3)
- BMS Moneo

### Platforms

- EMV 96 / EMV 2000
- GlobalPlatform
- MULTOS

### Formats Supported

- Common Personalization
- P3™ file<sup>1</sup>

<sup>1</sup>P3™ is a registered trademark of Thales e-Security Limited.

### System Architecture

- Multiple servers
- Multiple HSMs
- System integration API for automated production

### Security Architecture

- AES protected network communication
- Access control via smart cards
- Secure environment using HSMs
- HSM programming for key and certificate management
- Secure audit log of all events (in HSM)

### Operating Environment

- Microsoft Windows: NT4 / 2000 / XP
- Microsoft Windows Service

### Database

- Oracle version 8 and 9
- Microsoft SQL Server 7 and 2000

### Hardware Security Modules

- IBM 4758-02 (validated to FIPS 140-1 level 4)
- IBM 4758-023 (validated to FIPS 140-1 level 3)
- Eracom Protectserver Orange - CSA 8000 (validated to FIPS 140-1 level 3)
- nCipher nShield F3 (validated to FIPS 140-2 level 3)

### Other HSMs

- PKCS #11 interface
- HSM specific firmware

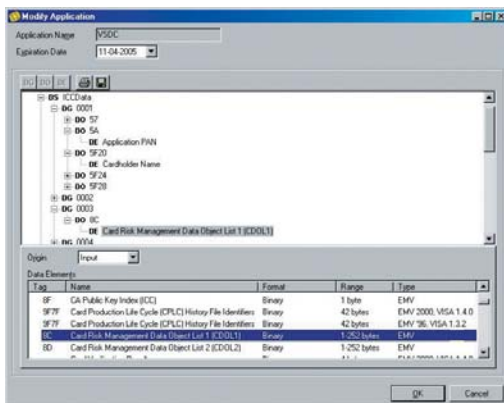
### Performance Monitoring

- Customisable integration into Microsoft Windows Performance Monitor

## Application Design

CardInk comes with a user-friendly graphical application editor, in which an operator can configure the TLV-structure of the data for individual applications. This feature makes it possible to design customised applications within the frameworks of the supported international standards.

Parameterisation of single- and multi-application smart cards is easily done through the concept of card profiling. It is possible to graphically design the data structure of a multi-application smart card by determining which applications and default operational parameters to use. Default production parameters can optionally be overridden by input file specifiers, allowing flexible control of daily production.



## About Cryptomathic

With more than 15 years of experience, Cryptomathic is one of the world's leading providers of e-Security. We can assist you in securing your business by providing best-of-breed e-Security software products and services as well as consultancy and education.

Our range of software products covers e-Security tools for professional application development, trust products as well as card personalization.

Cryptomathic's world-class experts offer e-Security consultancy at strategic level, for solution architecture, and integration.

We offer a complete modular education program, where you can learn what you need to know about e-Security – both on a general and product specific level.

We serve our customers through our head office in Denmark and our European subsidiaries. For more information, please visit our web site:

[www.cryptomathic.com](http://www.cryptomathic.com)



**CRYPTOMATHIC**  
e-Security for Better Business