

Cryptomathic CardInk Personalization Preparation System

A Paradigm Shift

The migration from magnetic stripe cards to smart cards is a paradigm shift. Smart cards feature secure storage, data processing, and cryptographic operations providing security and added value to the users.

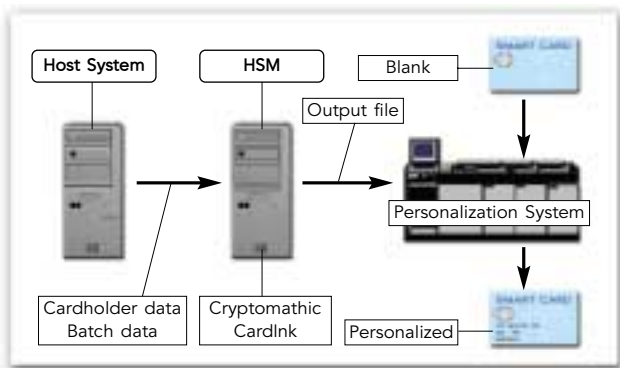
Cryptomathic CardInk is a personalization preparation system, which is used for issuing single- and multi-application smart cards. Based on an input file, which contains information on cardholders, Cryptomathic CardInk generates the application data to be stored on the card – including all cryptographic data.

Cryptomathic CardInk complies with the EMV and CEPS standards and covers the applications of MasterCard and VISA.

Architecture

Cryptomathic CardInk is the second-generation personalization preparation system from Cryptomathic and is developed in close cooperation with major international financial institutions.

Cryptomathic CardInk is a client/server system. Production can be controlled either through the client or by using an automated interface, which enables daily production to proceed without operator intervention. Secure clients for administration ensure users with different privileges the possibility of managing the system either locally or remotely via network.

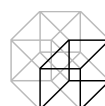


Cryptomathic CardInk provides:

Scalability – Cryptomathic delivers both low volume and full production systems with efficient synchronisation of multiple servers and multiple Hardware Security Modules. Entire configurations can be exchanged securely between separate installations providing the possibility of one-time set-up and qualification.

Flexibility – Cryptomathic CardInk manages the personalization preparation process. This includes set-up of an arbitrary number of issuers, extensive key management, and creation/import of required certificates. Individual smart card applications can be constructed and profiles for multi-application smart cards are set up.

Key Management – Cryptomathic CardInk is capable of generating and storing all cryptographic keys used in the personalization preparation. All keys are handled within physically secure Hardware Security Modules, and Cryptomathic CardInk has import/export facilities for the cryptographic keys. This applies to both symmetric and asymmetric keys including complete certificate management. Cryptomathic CardInk supports certificate requests for application provider certificate authorities (Europay/MasterCard and VISA CA).



Technical Specifications

Applications Supported

- Visa® Smart Debit and Credit (VIS 1.3.2 / VIS 1.4.0)
- MasterCard® M/Chip Select (version 2.1 / version 4.0)
- MasterCard® M/Chip Lite (version 2.1 / version 4.0)
- Europay® CLIP (CEPS version 2.3)

System Architecture

- Multiple servers
- Multiple clients for administration
- Multiple Hardware Security Modules
- System integration API
- Automated production

Security Architecture

- AES protection of network communication
- Access control via smart cards and privilege-based user roles
- Secure environment using Hardware Security Modules
- Cryptographic key generation/management
- Certificate generation/management
- Secure audit log of all events

Operating Environment

- Microsoft Windows NT™ Service
- Microsoft Windows NT4™ / Microsoft Windows 2000™

Database

- Oracle™ version 8
- Microsoft SQL Server™ version 7

Hardware Security Modules

- IBM 4758-02™ (complies with FIPS 140-1 level 4)
- IBM 4758-023™ (complies with FIPS 140-1 level 3)
- nCipher nShield™ (complies with FIPS 140-1 level 3)

Performance Monitoring

- Customisable integration into Microsoft Windows NT™ Performance Monitor

Application Design

Cryptomathic CardInk has an Application Editor that is used for creating applications. This includes configuration of content and output data structure as well as the option to specify the encryption of the output data in detail.

Layout and parameterisation of single- and multi-application structures are easily accomplished through the concept of card profiling. Here 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 stating them in the input file, so it is possible to fully control daily production via input file specifiers.

The functionality to manage customised data elements exists. This built-in feature provides unhindered possibilities of designing applications within the frameworks of the supported international standards.

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, consultancy, education, and complete security solutions.

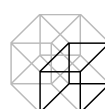
Our range of software products covers toolboxes for professional application development, trust products as well as personalization preparation of payment smart cards.

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 e-mail us at cardink@cryptomathic.com or visit our web site:

www.cryptomathic.com



CRYPTOMATHIC
e-Security for Better Business

A GUARDEONIC SOLUTIONS COMPANY