

Cryptomathic Secure Key Entry

Secure Key Management for IBM 4758

Cryptomathic Secure Key Entry extends the standard CCA (Common Cryptographic Architecture) functionality and takes the IBM 4758 module to a higher level of security. In order to avoid data being passed through PC memory, a Gemplus GCR card reader is connected directly to the serial port on the IBM 4758 module. The GCR card reader from Gemplus includes a smart card reader, keyboard and display.

With Cryptomathic Secure Key Entry it is possible to initialise the module master key and export and import operational keys between IBM boxes in a highly secure way using either the smart card reader or the keyboard and display. The master key, which protects all other keys in the module, is essential for secure usage of the IBM module and can be managed using the Cryptomathic Secure Key Entry. Normally, when setting up the module, parts of the master key will reside temporarily in the memory of the workstation in order to enable recovery, but by connecting the card reader to the hardware module, this potential vulnerability is eliminated.



IBM 4758

The IBM 4758 version 2 module is a hardware security module that can provide cryptographic functionality and key management to your application with a high level of security. A standard IBM 4758 module adds the following security to your application:

- User authentication: The user must log on to gain access to protected keys
- Role-based access: A user is assigned a role with access to a certain set of cryptographic functions
- Key protection using a 3DES master key



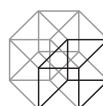
Enhancing Security

Cryptomathic Secure Key Entry solution solves two main issues for the IBM 4758 module:

- The initialisation and recovery of the master key using the GCR card reader gives you an easy and secure way to handle the master key. The master key is handled differently compared to operational keys, as the master key can only be exported at the same time as the key is generated. This means that after the master key has been generated and exported, the key cannot be exported again. This ensures that the master key cannot be compromised by the Cryptomathic Secure Key Entry.
- Export and import of operational keys enables you to exchange keys between different systems and also between IBM 4758 modules with different master keys.

Using smart cards, the master key as well as DES, 3DES and RSA operational keys can be managed. Each key is managed using a general key management scheme. This means that the key is exported in up to 255 parts. Only by providing a pre-specified number of these parts, depending on the key management scheme used, can the key be imported.

When the key is exported to the display and imported from the keyboard, the master key as well as DES and 3DES operational keys are supported. Each key can be exported in up to 255 parts and can only be imported if all parts are provided.



Technical Specifications

Operating Environment

- Microsoft Windows NT
- Microsoft Windows 2000

At request porting to other operating environments supported by the IBM 4758 CCA is possible.

Cryptomathic Secure Key Entry Components

- IBM 4758 firmware¹
 - Signed UDX firmware for an IBM 4758 module (version 002/023)
 - Reference guide
 - Installation guide

- GCR Card Reader from Gemplus
 - Reader
 - Power supply
 - Installation guide
 - Serial cable
- 10 GPK smart cards

¹The IBM 4758 module is not included in the package.

Cryptomathic Secure Key Entry can be customised to meet customer-specific requirements and can be purchased either separately or with Cryptomathic CardInk or Cryptomathic's range of trust products.

Cryptomathic CardInk

Cryptomathic CardInk is a data 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.

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

Cryptomathic CardInk is capable of generating and importing bank master keys from separate key generation systems. The Cryptomathic Secure Key Entry facilitates secure import and export of these keys. Also, the transport keys used for encrypting the cardholder data can be securely exported using the Cryptomathic Secure Key Entry.

Cryptomathic's Trust Products

Cryptomathic's family of trust products includes all the applications needed to set up and maintain a trust community, also known as a Public Key Infrastructure (PKI). Cryptomathic's trust products range from the central Certification Authority (CA), with supporting applications for registration of users and distribution of certificates, to components for time stamping and remote signature generation, which may be added as required.

With Cryptomathic's trust products you can include the benefits of digital signatures and reliable authentication in a business application for internal or external use, offer trust services as a service provider, or even set up a public Certification or Time Stamping Authority. The simple, yet flexible, license forms and pricing models make Cryptomathic's trust products an attractive choice for solutions of any scope or size.

Interoperable – The trust products comply with business standards and are tested for interoperability. This ensures that the applications fit into existing infrastructures.

Scalable and stable – Designed with scalability and stability in mind, the trust products fit both current and future requirements.

Proven – Large enterprises and banks as well as financial and government institutions rely on Cryptomathic's trust products to protect their business.

Flexible – The trust products are designed for easy integration with existing business systems. In addition, our e-Security tools allow you to enable new and legacy applications to handle digital signatures.

Secure – Built by world-class security experts, Cryptomathic's trust products offer premium security.

Hardware Crypto Enabled – For physical security and even better performance all the trust products support hardware security modules.

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 data preparation for 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 fill in the interest card on our web site: www.cryptomathic.com

