



Terminals & Card Applications

Haachtsesteenweg 1442
1130 Brussels
Belgium

DEP Documentation

DEP Glossary

1. TABLE OF CONTENTS

1. TABLE OF CONTENTS	3
2. SCOPE OF THE DOCUMENT	4
3. PRODUCT TERMINOLOGY	4
4. TERMS USED.....	6
5. KEYS.....	16
5.1. INITIAL AUTHORITY LEVEL	16
5.2. BANKSYS AUTHORITY LEVEL	17
5.3. CUSTOMER AUTHORITY LEVEL.....	17
5.4. NOTE.....	18
6. CAPABILITIES.....	18
7. ABBREVIATIONS	19

2. SCOPE OF THE DOCUMENT

This document explains the terms used in the DEP documentation. Normally, every term is well explained in the appropriate documents, but this document centralises all the definitions and the abbreviations.

The document starts with an overview of the DEP product terminology.

Together with the terminology and definitions, this document lists also some general keys and capabilities by their name (together with their tags).

3. PRODUCT TERMINOLOGY

- **DEP (Data Encryption Peripheral)**

The DEP is the name of the *banksys*' Host Security Module product line and is not considered as a product on itself. At this moment, the following DEP products are supported DEP/NT, DEP/Linux and DEP/PCI.



- **DEP Crypto Module**

The DEP Crypto Module is a name for *banksys*' own developed hardware responsible for cryptographic operations. Now, there is a DEP/ISA and a DEP/PCI considered as DEP Crypto Module.



- **DEP Platform**

A DEP Platform is any Personal Computer (PC) or server in which one or more DEP Crypto Modules have been installed. Communication and/or supervision of the DEP Crypto Modules is done with software running on the PC or server. A DEP Platform can be either the DEP/NT or the DEP/Linux.



- **DEP/ISA**

The DEP Crypto Module that is connected to the ISA slot of a DEP Platform (only supported in the DEP/NT). It is the first generation of the DEP Crypto Module.



- **DEP/PCI**

The DEP Crypto Module that is connected to the PCI slot of a DEP Platform. It is the most recent generation of the DEP Crypto Module (Common Criteria EAL3+ certificate begin 2003).



- **DEP/NT**

The DEP/NT is a DEP Platform based on a Windows NT 4.0 operating system with a Graphical User Interface. It supports both the DEP/ISA and the DEP/PCI.



- **DEP/Linux**

The DEP/Linux is a DEP Platform based on a Linux operating system (minimal Linux kernel 2.4). The DEP/PCI is interfaced through a command line. It supports only the DEP/PCI.



- **C-ZAM/DEP**

The C-ZAM/DEP is an independent chip card reader/encoder used to administer (loading keys and capabilities) a DEP Crypto Module.



- **DCC**

The DEP Control Card is a chip card used to store secrets (keys and capabilities) and non-secrets (Definition Lists).



4. TERMS USED

- **Alarm Software**

Executable software loaded during the production on the DEP Alarm of the DEP Crypto Module. It monitors continuously the tampering state of the DEP Crypto Module and takes the necessary actions in case of a tampering.

- **Application Capabilities**

Capabilities required by the Application Software or Boot Software to give the right to perform (cryptographic) operations or certain dedicated management functions (such as Application Software loading, Key backup/restore, ...). Application Capabilities can only be loaded when an Application Software is present in the DEP Crypto Module.

- **Application Keys**

Keys required by the Application Software in order to perform cryptographic operations. Application Keys can only be loaded when an Application Software is present in the DEP Crypto Module.

- **Application Secrets**

Application Secrets are secret values (Application Keys and Application Capabilities) that are used by the specific Application Software.

- **Application Software**

Executable software loaded inside the DEP Crypto Module that performs cryptographic functions for the host. Application Software can easily be downloaded in a secure way (using the functionality of the Boot Software).

- **Authentication Key (AK)**

A key required for authentication of a DCC. The Authentication Key is known at C-ZAM/DEP and DCC level. Every Authority Level and Mode of Operation has its own Authentication Key.

- **Authority Capability**

An Authority Capability is a dedicated capability that limits access to cryptographic operations/functions with Authority Keys. See paragraph 6 on page 18 for a list of the Authority Capabilities.

- **Authority Keys**

The set of keys used to execute functions coupled to a certain Authority Level. E.g. the Authority Keys are used to protect the communication between the C-ZAM/DEP, DCC and DEP Crypto Module. See paragraph 5 on page 16 for a list of the Authority Keys.

- **Authority Level**

The Authority Levels provide a level of functionality/protection for the DEP Crypto Module. Every Authority Level has different Authority Secrets. Different Authority Levels have different functions available. The possible Authority Levels are No Authority Level, Initial (INIT) Authority Level, Banksys (BKS) Authority Level and Customer (CUST) Authority Level. Application Software can only be loaded when the DEP is at CUST Authority Level.

- **Authority Secrets**

Authority Secrets are secret values (Authority Keys and Authority Capabilities) that are used to build up the different Authority Levels.

- **Banksys' Security Officer**

The Banksys' Security Officer is the person responsible for the key management operations at *banksys*. The Banksys' Security Officer manages the BKS Authority Keys. The personalisation of the DEP Control Cards is done under control of the Banksys' Security Officer.

- **Boot Software**

Executable software loaded during the production inside the DEP Crypto Module that starts-up the DEP Crypto Module and is responsible for loading Application Software.

- **Capability**

Capabilities are required in the C-ZAM/DEP and DEP Crypto Module to be allowed to perform certain secure operations. A Capability could be defined as 'the right to perform'. It is implemented as a cryptographic result that is verified before a function is available.

- **Capability Definition List**

The Definition List containing the descriptions and properties (name, tag and the reference to the Secret Sharing Scheme defined in the SSH Definition List) of capabilities used in the DEP Environment.

- **Chip Card**

A programmable credit card-sized secure data storage device. The DEP Control Cards are personalised chip cards.

- **Chip Card Reader (CCR)**

A device required to read/write the information from/to a chip card. The C-ZAM/DEP has a built-in Chip Card Reader.

- **Customer Identification (CUST ID)**

The Customer Identification is a unique identification number of the customer. The Banksys' Security Officer guarantees that the Customer Identification is unique.

- **Customer's Security Officer**

The Customer's Security Officer is the person responsible for the key management operations of the customer. This person is responsible for the key management, both at Authority Level (BKS Authority Keys, CUST Authority Keys and CUST Authority Capabilities) and at Application Software level (Application Keys and Application Capabilities). It is the Customer's Security Officer that operates the C-ZAM/DEP.

- **C-ZAM/DEP**

The C-ZAM/DEP is the main key management device in a DEP Environment. This device can be connected directly to the DEP Crypto Module and guarantees a secure key input and treatment. The device possesses a display, chip card reader and keyboard for this purpose. Communication with the different peripherals (DEP Crypto Module and DCC) are protected with the Authority Keys.

- **DCC Personalisation System**

The system that is responsible for the initialisation of virgin chip cards so that they become a DEP Control Card (DCC). This initialisation procedure is also called '*personalisation*'. The personalisation of the DCCs is done under supervision of the Banksys' Security Officer.

- **Dedicated File (DF)**

The sub directory on a chip card is a Dedicated File that again can contain Elementary Files or sub directories in the form of Sub Dedicated Files.

- **Definition List**

A Definition List contains the definitions and properties of keys (Key Definition List), capabilities (Capability Definition List) or Secret Sharing Schemes (SSH Definition List) to be used in the DEP Environment. It can be written on a DCC List.

- **DEP/Linux Software Directory**

This is the directory where the DEP/Linux Software Environment will be installed on the Linux platform.

- **DEP/Linux Software Environment**

The entire package of software (tools, DEPD Daemon, driver, ...) that allows communication with and management of the DEP Crypto Module(s).

- **DEP Alarm**

The DEP Alarm refers to the alarm processor of the DEP Crypto Module. This hardware is responsible for monitoring the DEP Crypto Module and taking the necessary actions when intrusion or tampering is detected (Tamper Responsiveness).

- **DEP Control Card (DCC)**

A Chip Card personalised for use in a DEP Environment. It can be either a *DCC List* or a *DCC Storage*.

- **DEP Control Card Identification (DCC ID)**

The DCC ID is a unique identification number of the DCC. The Banksys' Security Officer guarantees that the DCC identification number is unique per personalised DCC.

- **DEP Control Card List (DCC List)**

A personalised Chip Card used for storing Definition Lists.

- **DEP Control Card Storage (DCC Storage)**

A personalised Chip Card used for storing Application Secrets and/or Authority Secrets. Application Secrets and Authority Secrets can be stored using a defined Secret Sharing Scheme.

- **DEPD Daemon (DEPD)**

The DEPD Daemon is a process running on the DEP/Linux. It is responsible for the communication with the DEP Crypto Module.

- **DEPD Daemon Configuration File**

The DEPD Daemon Configuration File has a certain number of parameters that fine-tune the behaviour of the DEPD Daemon.

- **DEP Environment**

The DEP Environment is the collection of different components that are necessary to manage, operate and use the DEP. It is a combination of a DEP Platform, a DEP Crypto Module, the C-ZAM/DEP and DCCs.

- **DEP Handler Supervision**

This GUI program available on the DEP/NT handles all management functions of the available DEP Crypto Module(s). It allows parameterising and managing the available DEP Crypto Module(s). In addition, it offers also some supervision information.

- **DEP Main**

The DEP Main refers to the main processor of the DEP Crypto Module. The main processor runs the Application Software and is responsible for the management of the Application Keys and Application Capabilities.

- **DEP Master Key (DMK)**

The DEP Master Key of the DEP Crypto Module is used to encrypt/decrypt all Application Keys for backup purpose. The DEP Master Keys should only be known at DEP Crypto Module level.

- **DEP Parameter (DEP_PARAMETER)**

The DEP Parameter mechanism allows storing information in a DEP Crypto Module and provides means to protect and limit the use of this information to specific interfaces. The information can also be read again from the host. The purpose of the DEP Parameter mechanism is to provide means to the Security Officer to influence the behavior of specific interfaces: a part of the information used by the interface is not sent to the DEP, but is already present in the DEP Crypto Module.

- **DEP PC-AUX Program**

Auxiliary program used to create and edit Definition Lists and exchange them with a C-ZAM/DEP.

- **DEP System 2 (DS2)**

DEP System 2 refers to the operating system of the previous generation of the *banksys*' Host Security Modules.

- **DEP System 3 (DS3)**

DEP System 3 refers to the operating system of the current generation of the *banksys*' Host Security Modules.

- **DEP System 4 (DS4)**

DEP System 4 is an extension made on the DS3. It allows a faster processing of the incoming messages possible.

- **DS2 (Key) Backup**

A DS2 Backup is a secure backup of all the Application Keys of previous generation of the *banksys*' Host Security Modules based on the DEP System 2.

- **DS3 (Key) Backup**

A DS3 Backup is a secure backup of all the Application Keys inside the DEP Crypto Module of the current generation of the *banksys*' Host Security Modules based on the DEP System 3.

- **Elementary File (EF)**

An Elementary File is a file on a chip card. Data is stored in Elementary Files, which can exist at any of the three directory levels. A distinction between several types of Elementary Files is made. The difference between those different file types lies in their access rights (Public File, Secret File or Working File).

- **Graphical User Interface (GUI)**

The Graphical User Interface includes all the applications on the DEP Platform that interact in a graphical way with the user.

- **Hash Code**

A Hash Code over a message is a message digest or fingerprint of the message. The Hash Code changes when even one bit in the message is modified. Besides it is practically impossible to find the message that results in the same message digest as another message.

- **Host Interface Supervision**

The Host Interface Supervision is part of the DEP/NT and allows parameterising the communication protocol between the DEP/NT and the host. In addition, it offers also some supervision information.

- **Host Security Module (HSM)**

The purpose of a Host Security Module (HSM) is to store secret keys in it and to use these keys in a strictly defined way. Moreover, a HSM supports the secure creation of the secret keys that need to be stored in it and offers the functionality to load in a secure way these keys in the protected environment of the device. To meet these requirements it is necessary that a HSM is protected against tampering, meaning that someone having physical access to the device should not be able to obtain the secrets that are stored in it. Because the keys may only be used in a strictly defined way, also the loading of software that has access to the keys should to be protected adequately.

- **Issuer Key (IK)**

A key required for accessing a files on a DCC. The Issuer Key is known at C-ZAM/DEP and DCC level. Every level of operation has its own Issuer Key.

- **KeyMAC**

A cryptographic Hash Code that is calculated over all the keys available in the DEP Crypto Module. The KeyMAC is recalculated regularly to verify the integrity of the keys.

- **Key Backup**

A Key Backup (DS2 Key Backup or DS3 Key Backup) is a secure backup of all the Application Keys available in the DEP Crypto Module. The backup is protected with the DEP Master Key.

- **Key Backup Conversion Procedure**

The Key Backup Conversion Procedure is the procedure for converting a Key Backup from the DS2 generation (DS2 Key Backup) into a Key Backup for the DS3 generation Host Security Modules (DS3 Key Backup).

- **Key Definition List**

The Definition List containing the descriptions and properties (name, tag , length, type, generation method and the reference to the Secret Sharing Scheme defined in the SSH Definition List) of keys used in the DEP Environment.

- **Manipulation Detection Code (MDC)**

A Manipulation Detection Code is a synonym of a Hash Code.

- **Master File (MF)**

A Master File is the major overall file of the DCC. It can contain Elementary Files and Dedicated Files.

- **Message Authentication Code (MAC)**

A Message Authentication Code is a Manipulation Detection Code that guarantees the integrity/authenticity of the message and that identifies the sender of the message. A Message Authentication Code is normally calculated with a cryptographic algorithm using cryptographic keys.

- **Mode of Operation**

Indicates in which mode the DEP Environment has to operate: in live (LIV), for development purposes (DEV) or for testing purposes (TST).

- **ParameterMAC**

A cryptographic Hash Code that is calculated over all the parameters and its derived data available in the DEP Crypto Module. The ParameterMAC is recalculated regularly to verify the integrity of the parameters.

- **Personal Identification Number (PIN)**

Personal Identification Number that identifies and authenticates the cardholder and that is required to access certain secure functions on a DCC.

- **Public File (PF)**

A Public File is an Elementary File that can be read freely, but changing it is restricted.

- **Personal Identification Number Printing (PIN Printing)**

The PIN Printing operation is the sensitive operation of printing the clear secret PIN code of a chip card.

- **Secret File (SF)**

A Secret File is an Elementary File that can never be read via a chip card interface. It can only be used internally in and by the chip card. Changing a Secret File is restricted.

- **Secret Sharing Definition List**

The Definition List containing Secret Sharing Schemes used in the DEP environment.

- **Secret Sharing Scheme (SSH)**

The Secret Sharing Scheme defines the way in which a secret is divided in different parts to be distributed among different persons.

- **Secret Sharing Index**

The Secret Sharing Index is the identification code of a specific Secret Sharing Scheme in the Secret Sharing Definition List.

- **Secure Hash Algorithm (SHA)**

The Secure Hash Algorithm (SHA) is a secure algorithm delivering a Hash Code over a message.

- **Security Officer**

A Security Officer is responsible for the management of secret keys and capabilities.

- **Software Authentication Code (SW AC)**

A Software Authentication Code is a Message Authentication Code calculated over the Software Application to guarantee the integrity and origin of the software. The Banksys' Security Officer calculates the Software Authentication Code.

- **SoftwareMAC**

A cryptographic Hash Code that is calculated over the Application Software available in the DEP Crypto Module. The SoftwareMAC is recalculated at every startup.

- **Sub Dedicated File (SDF)**

A Sub Dedicated File is a directory in a Dedicated File. These SDFs cannot contain any more sub directories, but can only contain Elementary Files.

- **Tag**

A Tag is a four-byte identification number of information used in the DEP Environment. There are data tags, function tags, key tags, error tags, capability tags, parameter tags, ...

- **Tamper Evidence**

“The intent of the tamper evidence is to provide evidence that an attack has been attempted and may or may not have resulted in the unauthorised disclosure or modification of the sensitive data. The disclosure of an attempted attack could be in the form of physical evidence such as damage to the packaging.” (ISO CD 13491) “The physical damage must be such so that the device cannot be placed back in service without a high probability of the tampering being detected.” (ISO 9564-1:1991(E))

- **Tamper Resistance**

“The intents of tamper resistance is to block attacks against the information to be protected from unauthorised disclosure or modification by employing passive barriers.” (ISO CD 13491)

- **Tamper Responsiveness**

“The intent of tamper response is to employ active barriers against attacks at unauthorised disclosure or modification of the protected information.” (ISO CD 13491)

- **Third Party’s Security Officer**

The Third Party could develop its own Application Software and being responsible for the distribution of its Application Software, and thus the key management that is linked to it. In this case, the Third Party needs a Security Officer equivalent to the banksys’ Security Officer, called the Third Party’s Security Officer.

- **Transport Key (TK)**

A Transport Key is a key used to encrypt messages sent between the different devices in a DEP Environment. In other words, it is a key to transport (sensitive) information from one device to another in a secure way.

- **Working File (WF)**

A Working File is an Elementary File whose protection rights are customisable.

5. KEYS

5.1. INITIAL AUTHORITY LEVEL

These keys are hard-coded in the C-ZAM/DEP.

Name	Tag
<i>KM_AUTH_INIT_CAP_DEP_XXX</i>	04F00000
<i>KM_AUTH_INIT_TK_CZD_DEP_XXX</i>	04F00300
<i>KM_AUTH_INIT_TK_DEP_DCC_XXX</i>	04F00600
<i>KM_AUTH_INIT_CAP_CZD_XXX</i>	04F00900
<i>KM_AUTH_INIT_IK_DCC_XXX</i>	04F00C00
<i>KM_AUTH_INIT_AK_DCC_XXX</i>	04F00F00
<i>KM_AUTH_INIT_TK_CZD_DCC_XXX</i>	04F01200

XXX stands for LIV for live mode, TST for test mode and DEV for development mode.

5.2. BANKSYS AUTHORITY LEVEL

The Banksys Authority Master Keys (KM_AUTH_BKS - 04F01500) consist of different parts:

Name	Tag
<i>KM_AUTH_BKS_CAP_DEP_XXX</i>	04F00100
<i>KM_AUTH_BKS_TK_CZD_DEP_XXX</i>	04F00400
<i>KM_AUTH_BKS_TK_DEP_DCC_XXX</i>	04F00700
<i>KM_AUTH_BKS_CAP_CZD_XXX</i>	04F00A00
<i>KM_AUTH_BKS_IK_DCC_XXX</i>	04F00D00
<i>KM_AUTH_BKS_AK_DCC_XXX</i>	04F01000
<i>KM_AUTH_BKS_TK_CZD_DCC_XXX</i>	04F01300

XXX stands for LIV for live mode, TST for test mode and DEV for development mode.

5.3. CUSTOMER AUTHORITY LEVEL

The Customer Authority Master Keys (KM_AUTH_CUST - 04F01600) consists of different parts:

Name	Tag
<i>KM_AUTH_CUST_CAP_DEP_XXX</i>	04F00200
<i>KM_AUTH_CUST_TK_CZD_DEP_XXX</i>	04F00500
<i>KM_AUTH_CUST_TK_DEP_DCC_XXX</i>	04F00800
<i>KM_AUTH_CUST_CAP_CZD_XXX</i>	04F00B00
<i>KM_AUTH_CUST_IK_DCC_XXX</i>	04F00E00
<i>KM_AUTH_CUST_AK_DCC_XXX</i>	04F01100
<i>KM_AUTH_CUST_TK_CZD_DCC_XXX</i>	04F01400

XXX stands for LIV for live mode, TST for test mode and DEV for development mode.

5.4. NOTE

Note that keys have the same tag, whether they are meant for LIV, TST or DEV mode. The DEP security mechanisms ensure that a key value specified for a specific mode cannot be used by a device that is in another mode. This implies that keys of different modes cannot be mixed.

6. CAPABILITIES

- **CAP_AUTH_BKS** (Banksys Authority Master Capability - 05F00100)

Capability to create/save Banksys Authority Master Keys, create/save Customer Authority Master Capability, read/save/change definition of the C-ZAM/DEP keys and capabilities.

- **CAP_AUTH_CUST** (Customer Authentication Master Capability - 05F00300)

Capability to create/save Customer Authority Master Keys, create/save Customer Authority Capabilities for the DEP Crypto Module, create application keys on the C-ZAM/DEP, read/save/change the definition of Customer Application Keys/Capabilities.

- **CAP_BKS_SW_AC** (Software Authentication Capability - 05F00400)

The CAP_BKS_SW_AC is the capability to generate a Software Authentication Code with the C-ZAM/DEP.

- **CAP_STD_SW_LOAD** (Software Load Capability - 05000300)

The CAP_STD_SW_LOAD is the capability to load the Application Software.

- **CAP_STD_SAVE_KEYS** (Save Application Key Capability - 05000000)

The CAP_STD_SAVE_KEYS is the capability to create or restore a Key Backup to/from the host or DEP Handler Supervision.

- **CAP_STD_SET_PARAMETERS** (Set Parameters Capability - 050007xx)

The CAP_STD_SET_PARAMETERS is a capability to modify a parameter in the DEP Crypto Module.

- **CAP_STD_TRACE** (Set Parameters Capability - 05000500)

The CAP_STD_TRACE is a capability to activate the trace functionality of the DEP/NT.

7. ABBREVIATIONS

• AC	Authentication Code (sometimes called a 'Certificate')
• ADD	Algorithm Detailed Design
• AK	Authentication key (sometimes called a 'Acquire Key')
• AUTH	Authority Level
• BKS	Banksys (Authority Level)
• CAP	Capability
• CUST	Customer (Authority Level)
• CZD	C-ZAM/DEP
• DCC	DEP Control Card
• DEP	Data Encryption Peripheral
• DEPD	DEP Daemon (Linux only)
• DEA	Data Encryption Algorithm
• DES	Data Encryption Standard
• DEV	Development (Mode)
• DF	Dedicated File
• DFS	Detailed Functional Specifications
• DMK	DEP Master Key
• DNS	Dynamic Name Solving
• DP	DEP Protocol
• DS2	DEP System 2
• DS3	DEP System 3
• DS4	DEP System 4
• DUKPT	Derived Unique Key Per Transaction
• EDP	Enhanced DEP Protocol
• EFT	Electronic Fund Transfer
• EMV	Eurocard-Mastercard-Visa (standard)
• GUI	Graphical User Interface
• HSM	Host Security Module
• ICC	Integrated Chip Card
• ICV	Initial Check Value
• INIT	Initial (Authority Level)
• IK	Issuer key
• ISA	Industry Standard Architecture
• KD	Derived Key
• KM	Master Key
• LIV	Live (Mode)
• MDC	Manipulation Detection Code
• MF	Master File
• OS	Operating System
• PC	Personal Computer
• PCI	Peripheral Component Interconnect bus
• PF	Public File
• PIN	Personal Identification Number
• PKI	Public Key Infrastructure

- RAM Random Access Memory
- RSA Rivest - Shamir – Adleman
- RTC Real-Time Clock
- SDF Sub Dedicated File
- SF Secret File
- SHA Secure Hash Algorithm
- SO Security Officer
- SSC Self-Signed Certificate
- SSH Secret Sharing Scheme
- SW Software
- SW AC Software Authentication Code
- TK Transport Key
- TST Test (Mode)
- UKPT Unique Key Per Transaction
- WF Working File