DEP/PCI

DEP/PCI Security Policy

FIPS 140-2 Non-proprietary Security Policy

S.A. Atos Worldline N.V. – Chaussée de Haecht 1442 Haachtsesteenweg
B-1130 Bruxelles-Brussel - Belgium
RPM-RPR Bruxelles-Brussel - TVA-BTW BE 0418.547.872

COPYRIGHT

LEGAL DISCLAIMER

JURISDICTION AND APPLICABLE LAW

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1. INTRODUCTION

1.1. ABOUT THE DOCUMENT

This document is the security policy for the Banksys[1] "Data Encryption Peripheral" (henceforth called "DEP/PCI") by Atos Worldline S.A./N.V., discussing its features and its use from the technical perspective of the FIPS 140-2 validation program for cryptographic modules.

The DEP/PCI v4 is one of a range of Hardware Security Modules (HSM) designed by Atos Worldline S.A./N.V.. As nowadays encryption has become a fundamental component of many business-critical processes, the DEP/PCI fulfils the essential requirement of protecting all cryptographic keys used in an application. With its tamper-evident and tamper-responsive hardware, the DEP/PCI physically protects the confidentiality and integrity of all the data it holds.

Detailed information on the DEP/PCI and other Banksys products by Atos Worldline S.A./N.V. is available at Banksys web site: http://www.banksys.com.
For answers to technical or sales-related questions, refer to the contacts listed on the Banksys internet site.

1.2. ABOUT THE DEP/PCI

1.2.1. SCOPE OF VALIDATION

The DEP/PCI with only the boot firmware, FPGA firmware and alarm firmware running (i.e. with no DEP Application Software loaded) constitutes the scope of this FIPS140-2 validation. The purpose of this configuration is to provide a secure platform for loading DEP Application Software securely. DEP/PCI hardware together with the alarm firmware provides a physically secure platform. The boot firmware provides boot loader functionality to securely load application software. The FPGA firmware contains implementations of AES and SHS, which are used by the boot firmware (and may be also used by a DEP Application Software, if loaded).

The purpose of the DEP/PCI, after loading the DEP Application Software, is described in the paragraphs below. The resulting configuration consisting of application software on the DEP/PCI is no longer the certified module. It may also fulfil the requirements of FIPS 140-2, but this has to be validated and certified separately.

[1] Banksys is an Atos Worldline S.A./N.V. brand.

1.2.2. FIELDS OF APPLICATION

The DEP/PCI with application software loaded is a Hardware Security Module (HSM) that is suited for various fields of application:

- banking
- electronic funds transfer
- electronic purse
- PKI
- public services
- pay-TV
- e-commerce
- ...

It is a generic platform providing a wide range of cryptographic services, either built-in or provided by a loaded application software:

- encryption/decryption
- MAC computation
- hashing
- digital signature computation
- key generation
- random bits generation
- …

The cryptographic services of the DEP/PCI can use keys that are:

- internally generated
- offered as the service is requested
- pre-loaded

These services are part of the DEP Application Software, and are out of the scope of the current FIPS140-2 validation.

The DEP/PCI is primarily intended for use at the host side. It can be plugged into a workstation that is connected to a mainframe or to a server located in a computer room, or it can be plugged directly into a server located in a computer room.

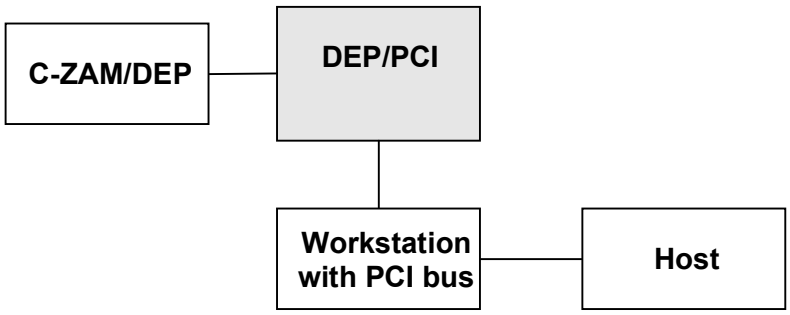

Figure 1: DEP/PCI hardware configuration

The scope of this validation is the configuration of DEP/PCI without DEP application software loaded, i.e. boot firmware, FPGA firmware and alarm firmware running on the hardware only. This configuration is equipped to securely load an application and/or keys into it. Only authorised personnel, such as Customer Administrators (i.e. crypto officers) and Operators belonging to the Software-loading group (i.e. users), can load keys and load application software, respectively.

The DEP/PCI detects tamper attacks, such as physical intrusion, temperature and chemical attacks, and responds appropriately to protect all sensitive data and log the events.

1.2.3. CRYPTOGRAPHIC MODULE SPECIFICATIONS

1.2.3.1.Physical Embodiment

The DEP/PCI is a multi-chip embedded cryptographic module. It contains a set of standard, production-quality IC chips that are interconnected. These ICs are encapsulated in an epoxy potting and enveloped in a cold-rolled steel enclosure to protect them from environmental or other physical damage.

1.2.3.2.Physical Boundaries

The DEP/PCI is a PCI card that can be plugged into any workstation that supports PCI cards.
The cryptographic boundary is made up by a black-lacquered cold-rolled steel enclosure, which is rivet-mounted on the PCI card. The cryptographic boundary is indicated by red dashed lines in Figure 2 and in Figure 3. All components inside the steel enclosure / cryptographic boundary are physically located on a printed circuit board, the so-called alarm card. The alarm card is completely surrounded by the enclosure and is furthermore encapsulated by an epoxy potting inside the enclosure. The alarm card is connected to the PCI card via two flexes (light-grey ribbon cables, see Figure 3). All components on the PCI card located outside the enclosure (interface components, power supply and batteries) are not security relevant and excluded from the requirements of FIPS PUB 140-2.

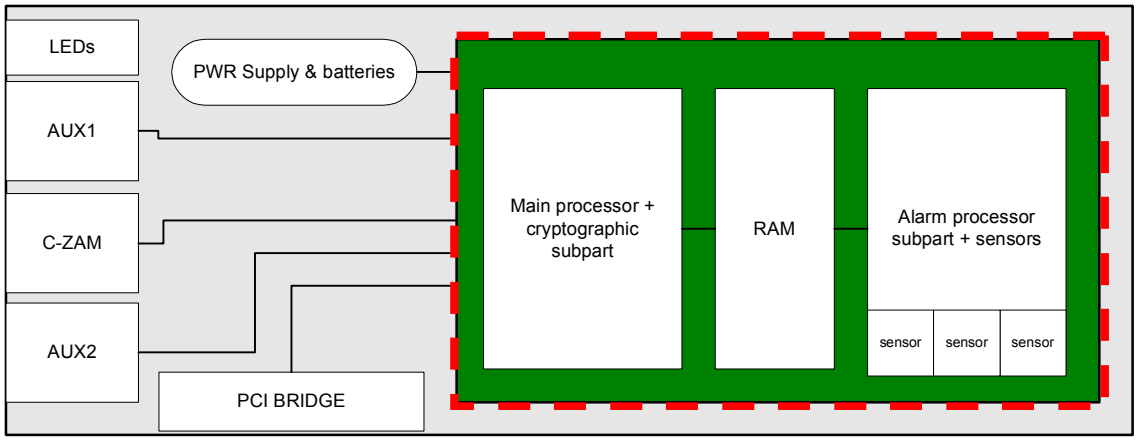

Figure 2: DEP/PCI hardware block diagram
(dashed red line indicates cryptographic boundary)

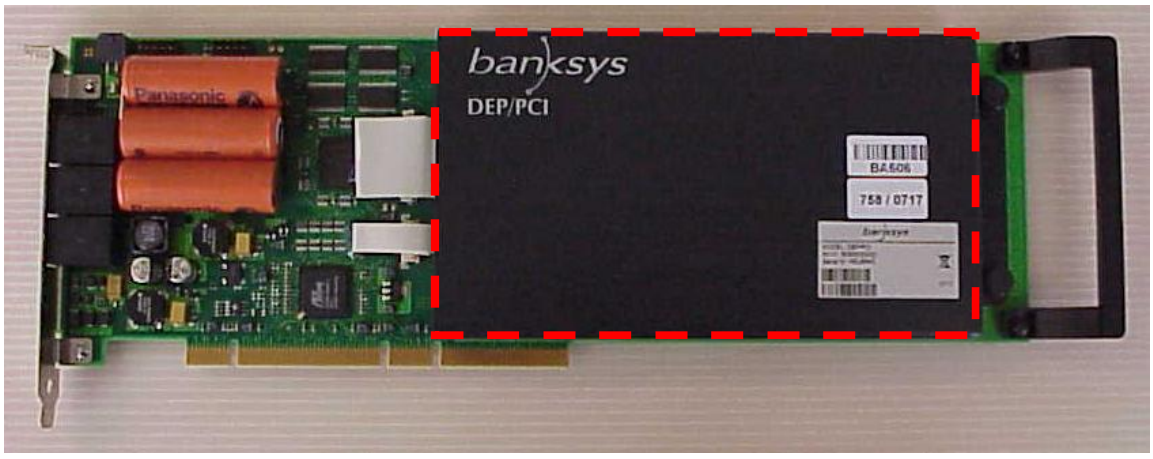

Figure 3: DEP/PCI hardware front view
(dashed red line indicates cryptographic boundary)

The rear of the DEP/PCI card is presented in Figure 4.

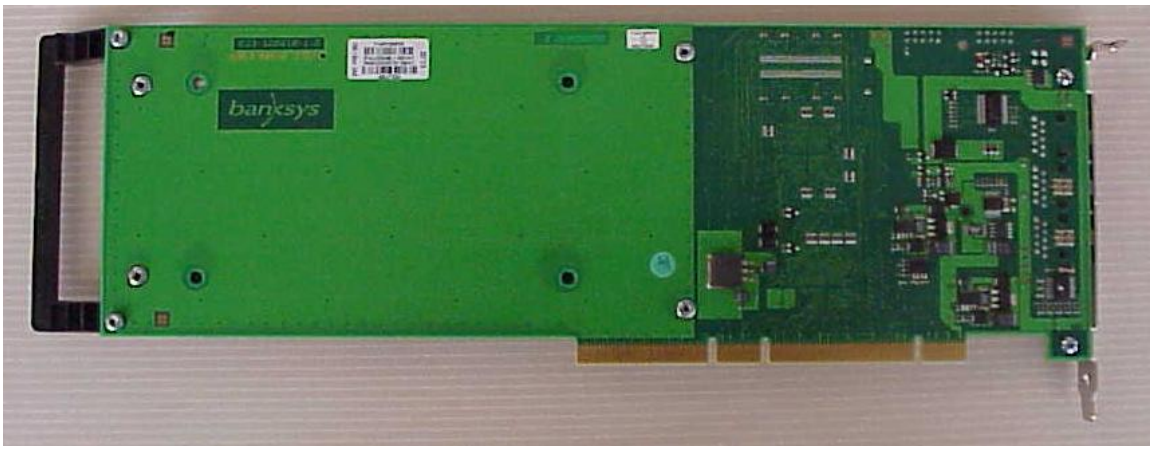

Figure 4: DEP/PCI hardware rear view

Therefore DEP/PCI is comprised of two main parts:

- The black-lacquered steel enclosure, i.e. the cryptographic boundary, containing the potted alarm card, which holds mainly:
  - the main processor and the cryptographic FPGA
  - the alarm processor
  - the RAM accessible by both processors
  - the alarm sensors
- The PCI card (all parts of it are excluded from the security requirements of FIPS 140-2) contains mainly:
  - the power supply and batteries,
  - the PCI bridge,
  - the serial line 'AUX1', which is not used,
  - the serial line 'C-ZAM': to connect a **C-ZAM/DEP,** an external chip card encoder/reader that is used for administration purposes
  - the serial line 'AUX2': to communicate with the alarm card of the DEP/PCI to, for example, log security incidents to a printer or another device
  - the LEDs, which present the status of the DEP/PCI, such as an indication whether the PCI card is busy, free or in error.

Those two parts are connected through two flexes: the smaller one for power and the bigger one for communication. These flexes establish the connection between the serial lines and the PCI bridge on one hand and the alarm card on the other.

The host, to be able to use cryptographic services provided by the DEP/PCI, has to connect to the workstation in which the DEP/PCI is inserted.

The **C-ZAM/DEP** is used as a keyboard for entering keying material. Since the **C-ZAM/DEP** itself is not part of the DEP/PCI, it is beyond the scope of the FIPS140-2 validation. The **C-ZAM/DEP** is directly connected to the DEP/PCI through the serial line "C-ZAM".

Figure 5: The C-ZAM/DEP device

1.2.3.3.DEP/PCI Components

The following table lists the DEP/PCI v4 components as validated here:

DEP/PCI v4 components	
Hardware	♦ PCI card (version 033-120010-1.0) (all components on the PCI card are excluded from security requirements of FIPS 140-2) ♦ Alarm card (version 033-120020-2.0) ♦ Flex (version 033-120030-3.0)
Firmware	♦ Boot firmware (version 4.0.l) ♦ Alarm firmware (version 5.0.m) ♦ FPGA firmware (version 66 14 42)

Table 1: DEP/PCI components

The boot firmware is intended to load DEP Application Software; the latter is not subject to this FIPS140-2 validation.

1.2.3.4.Physical configuration

The DEP/PCI card is placed in one of the PCI slots of the closed shielded DEP Platform. Up to four DEP/PCI cards can coexist in a DEP Platform.

1.2.3.5.Security rules

Among the security rules that the DEP/PCI enforces, two categories are to be distinguished:

- imposed by FIPS 140-2
- imposed by Atos Worldline S.A./N.V.

According to the FIPS 140-2 Related Security Rules, DEP/PCI shall:

1. support the following logically distinct interfaces sharing one physical port:
   - Data input interface
   - Data output interface
   - Control input interface
   - Status output interface
   - Power interface
2. inhibit all output via the data output interface during self-tests and whenever an error state was entered.

3. logically disconnect the output data path from the processes while performing computations on sensitive data, such as encryption, zeroization...
4. not permit that Critical Security Parameters (CSPs) enter the DEP/PCI in a plain text format, except if split knowledge is used.
5. not permit the output of critical security parameters in plain text format.
6. enforce identity-based authentication.
7. support the following authorised roles: Administrator, Operator and User.
8. not retain authentication of an Operator when it is powered up after being powered off.
9. not support a bypass mode or a maintenance role.
10. be protected using a hard opaque potting material as coating.
11. be protected by a tamper proof enclosure.
12. implement environmental failure protection for temperature and voltage.
13. implement all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
14. protect CSPs from unauthorised disclosure, modification and substitution.
15. provide means to ensure that a key entered into or stored within is associated with the correct entities to which the key is assigned.
16. deny unauthorised access to plain text secrets contained within the DEP/PCI.
17. provide the capability to zeroize all CSPs contained within the DEP/PCI.
18. force its boot firmware to support only approved security functions.
19. conform to the EMI/EMC requirements specified in FCC Part 15, Subpart B, and Class B.
20. perform the self-tests during power-on and on demand.
21. issue an error message via the status interface whenever an error state is entered due to a failed self-test.
22. not perform any cryptographic functions while in an error state.
23. not support multiple concurrent Operators.
24. force its boot firmware to provide only a FIPS mode of operation.
25. contain production-quality ICs that meet commercial-grade specifications for power, temperature, reliability, and shock/vibration with standard passivation; these ICs are enclosed in an epoxy potting and in a cold-rolled steel enclosure.
26. be implemented as a production-grade multi-chip embodiment.

The Atos Worldline S.A./N.V. security rules impose that:

1. Atos Worldline S.A./N.V.-relevant data items (AWRDIs) are not security-relevant and shall never be zeroized by the DEP/PCI. This relates to items such as time-outs, methods for pooling…
2. Administrators and Operators from Atos Worldline S.A./N.V. and from the Customer must follow the procedures outlined in the security officer guidance pertaining to both initialisation and personalisation phases. This applies when the DEP/PCI is in its manufacturing state and after zeroization.
3. The Administrators must change the pre-expired passwords to personal ones prior to usage phase.

1.2.4. CRYPTOGRAPHIC PORTS AND INTERFACES

1.2.4.1.Physical ports

Physical port(s)	FIPS Interface(s)
PCI	♦ Status Output ♦ Control Input ♦ Data Output/Input ♦ Power This interface provides all power that will be used in normal condition: i.e. all cryptographic operations of the DEP/PCI.
Backup-battery interface	♦ Power interface It is used to give backup power to the DEP/PCI, which enables the DEP/PCI to maintain and protect its critical security parameters (CSPs) when no power is available anymore. The battery is continuously monitored by the alarm processor, which alerts the Administrator in case of trouble (voltage low condition).
Serial C-ZAM/DEP	♦ Status Output ♦ Control Input ♦ Data Output/Input It is used to communicate with the **C-ZAM/DEP** device.
Serial Aux-2	♦ Status Output ♦ Control Input for alarm processor It is used to communicate with the alarm processor.
Serial Aux-1	Not used.

Table 2: Physical ports

1.2.4.2.Logical interfaces

The logical interfaces of the DEP/PCI are shown in Figure 6.

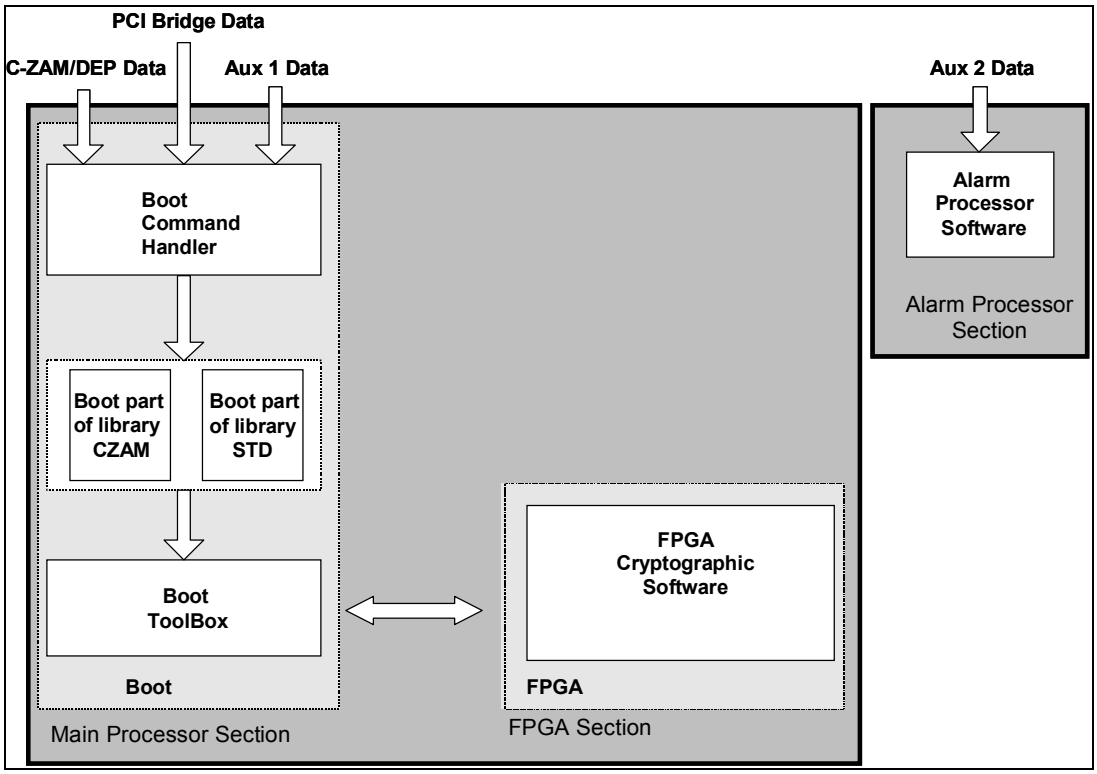

Figure 6: DEP/PCI-Software Environment

The DEP/PCI contains three major firmware parts:

1. The Boot Firmware (in EEPROM)
   This part executes when no Application Software has been loaded. As soon as Application Software is loaded, this part is "switched off" and execution is transferred to the Application Software.
2. The FPGA Firmware (in FLASH)
   This part provides the basic cryptographic functions of the DEP/PCI.
3. The Alarm Firmware (in EEPROM)
   This part executes concurrently with the other two, and continuously monitors the various sensors of the DEP/PCI for alarms. If an alarm is triggered, it initiates zeroization, thus resetting the DEP/PCI completely. (If an Application Software would be loaded, the alarm firmware would also remove the Application Software and return the control to the Boot Firmware.)

The interfaces that exist in the DEP/PCI are the following:

1. PCI bridge interface
   This interface is for communication, through the Boot Command Handler, with the part of the STD library that is in the Boot firmware.
2. C-ZAM/DEP interface
   This is used for communication, through the Command Handler, with the part of the C-ZAM library that is in the Boot firmware.

3. AUX 1 interface
   This interface is not used.
   The DEP/PCI does not send data to AUX1, and the DEP/PCI ignores all incoming data from AUX1.
4. AUX 2 interface
   This interface is used for:
   - The authentication of the DEP/PCI Alarm-Processor-Section hardware
   - The reading of the alarm status and the alarm logging
   - The administration of the alarm part

Note:
All these interfaces are physically connected to the DEP/PCI alarm card by means of the two flexes.

1.2.5. OPERATIONAL ENVIRONMENT

The FIPS140-2 Operational Environment requirements are not applicable, since the DEP/PCI has a limited non-modifiable environment. It does not support the loading or execution of non-trusted code and the integrity and authenticity of software/firmware upgrades, furnished by Atos Worldline S.A./N.V., are verified and evaluated via a CMAC.

1.2.6. SECURITY LEVEL

The DEP/PCI meets the overall requirements applicable to Level 3 security of FIPS140-2. The following table gives the compliance level of each section.

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Machine Model	3
Physical Security	3
Operational Environment[2]	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

Table 3: Security level

[2] The operational environment is not applicable, because DEP/PCI has a limited non-modifiable environment.

2. IDENTIFICATION AND AUTHENTICATION POLICY

2.1. ROLES ASSUMPTION

Three roles are supported by the DEP/PCI:

1. *Customer Administrator role (Crypto officer role)*
   It is assumed that there are at least two Administrators. They are allowed to perform exclusive operations: change their pre-expired passwords, enter the customer-individual KAWL[3] base secret (using split knowledge, i.e. two components), create a specialised group of Operators (Software-loading group), monitor the password and username creation of the different Operators, and save/restore the configuration of this group.
2. *Software-loading Operator role (User role)*
   The Operator for the Software-loading role is member of the Software-loading group. The minimum number of Operators in the group is two. The members of the group are dedicated to this role and cannot perform any other cryptographic task with regard to the DEP/PCI.
3. *Non-authenticated role*
   The non-authenticated role allows a non-crypto Operator to perform specific security operations with the DEP/PCI such as checking status and sending an ECHO. Furthermore, non-authenticated role can perform zeroization (e.g. by quickly moving the DEP/PCI or the device it is built-in, as the accelerometer sensor of DEP/PCI will detect this as a tamper attempt and trigger zeroization).

There is no maintenance role for DEP/PCI.

2.2. IDENTIFICATION

2.2.1. Customer Administrator

During the personalisation phase, each customer Administrator first enters in clear text his pre-expired password and username (provided securely by Atos Worldline S.A./N.V.). The DEP/PCI hashes the password and compares it with the SHA-256 hash value that was stored in the boot at the manufacturing phase. If it matches, the customer Administrator is authenticated and he can enter his new password. The DEP/PCI stores only the SHA-256 hash of the new password. Thus, the new password becomes the identity-based authentication credential for the customer Administrator.

[3] KAWL keys are AES 256-bit keys that are used for protection of confidentiality and authenticity of DEP Application Software and Operator group configuration.

Two customer Administrators are required for the personalisation of the DEP/PCI. Each of them authenticates with his new password and enters his split knowledge component of the KAWL base secret. The two components are combined in the DEP/PCI, and from the resulting KAWL base secret then four different keys are derived for:

- Application software decryption
- Application software authentication code verification
- Operator group configuration backup encryption/decryption
- Operator group configuration backup authentication code generation/verification

Only the two customer Administrators (crypto officers) are allowed to enter the KAWL base secret. Its components are entered through the **C-ZAM/DEP** serial port.

The two customer Administrators together create the specialised group of Operators. At creation time, the Operators of this group enter their password and username under the supervision of the customer Administrators. The DEP/PCI hashes the passwords and stores only the SHA-256 hash in a separate memory space, specific to each group.

2.2.2. Software-loading Operator

During the personalisation phase, each member of the Software-loading group enters his password and username under the supervision of the two customer Administrators. Subsequently, the Software-loading Operator authenticates himself to the DEP/PCI using this password and username whenever he is to perform local Software-loading operations. Software-loading has to be processed by two Software-loading Operators.

2.2.3. Summary

Role	Type Of Authentication	Authentication Data
Customer Administrator role (crypto officer role)	Identity-based username and password	Password
Software-loading Operator role (User role)	Identity-based username and password	Password
Non-authenticated role	No authentication	No data

Table 4: Roles and required identification/authentication

2.3. AUTHENTICATION

Before carrying out a cryptographic function on the DEP/PCI, the Administrators and the Software-loading Operators must authenticate themselves by use of a username and a password. Feedback is limited to the result of the authentication (failure or success).

Authentication mechanism	Strength of mechanisms
Username and password	Crypto Officers (Customer Administrators and Operators) accessing the DEP/PCI using the C-ZAM/DEP must authenticate themselves, using a username and a password that is between 10 and 20 characters. The characters used in the password must be from the character set of [a..z, A..Z, 0..9 and special characters as éçà…]. As this yields a minimum of $10^{26+26+10} = 10^{62}$ possible combinations, the possibility of correctly guessing a password is $1/10^{62}$, which is less than 1/1,000,000. Due to a correctional delay of 60 milliseconds for every non-successful authentication (so that there is a maximal limit of 1000 non-successful authentications per minute), the probability of successfully authenticating to the module within one minute is less than $1/10^{59}$, which is less than 1/100,000.

Table 5: Strength of authentication mechanisms

3. ACCESS CONTROL POLICY

3.1. ROLES AND SERVICES

3.1.1. Roles

In the DEP/PCI, there are 3 different roles, which are defined in paragraph **2.1 ROLES** :

1. Customer Administrator role (Crypto officer role)
2. Software-loading Operator role (User role)
3. Non-authenticated role

3.1.2. Services

3.1.2.1.Authentication services

The authentication services consist in:

- Authenticating through a username and password, to be in an authenticated state in the DEP/PCI; this has to be done by the Customer Administrators and the Software-loading Operators.
- Ending the authentication (logging off), this can be done by the Customer Administrators and the Software-loading Operator.
- Replacing the pre-expired username and password; this has to be done by the Customer Administrators.
- Changing password, this can be done by the Customer Administrators and the Software-loading Operators.

3.1.2.2.Key-management services

These services consists of:

- Entering the KAWL base secret (from which KAWL keys for software decryption, verification of software CMAC, and encryption/decryption and CMAC generation/verification for Operator group configuration are derived); this can be done by the Customer Administrators.
- Deleting the KAWL keys, this can be done by the Customer Administrators.

3.1.2.3.Software-loading service

This service is used to load the DEP Application Software. Only the Operators of the Software-loading group can perform this service. It consists of:

Loading Software, if enabled. Software must be signed by Atos Worldline S.A./N.V., otherwise it is rejected by the DEP/PCI.

3.1.2.4.Reset service

Anyone having logical access to the PCI bridge interface can perform the following service:

- Reset: this service erases all data contained in the DEP/PCI, removes the authentication data: passwords, usernames, keys, Application Software and the Application Keys, and returns control to the Boot Firmware.

The following reset service can be carried out only by the Customer Administrators:

- Resetting the login and return to the pre-expired usernames and passwords.

3.1.2.5.Show-Status services

The following three services can be performed by anyone having logical access to the PCI bridge interface:

- Requesting a Status: these services request a DEP/PCI status: version of boot and alarm firmware, content of the software.
- Getting Diagnostics: this service diagnoses the DEP/PCI and gives information about the memory status.
- Retrieving serial numbers: this service returns the serial number of the DEP/PCI card.

The following service can be performed by anyone having logical access to the serial C-ZAM/DEP interface:

- Retrieving information on the groups of Operators: this service provides information on the existing groups and in a group, on the existing Operators.

3.1.2.6.Self-Test services

These can be performed by anyone having logical access to the PCI bridge interface.

- Performing a self-test: this service asks the DEP/PCI to realise a self-test.

- Sending an Echo: this service allows testing the communication between the DEP/PCI and the HOST, by sending and receiving data.
- Testing the FIFOs: this service executes a complete communication test on the DEP/PCI.

3.1.2.7.Configuration services

Only the customer Administrators can perform these services. They consist in:

- Configuring the groups of Operators.
- Creating members of the groups of Operators.
- Deleting members of the groups of Operators.
- Saving the Operator group configuration in encrypted form.
- Restoring the Operator group configuration from previously saved encrypted form.

3.1.3. Roles and services

Role	Authorised Services	Input
Customer Administrator role (crypto officer role)	Replace the pre-expired username and password.	I_CZD_CHG_ADMIN_LOGIN
	Enter KAWL base secret, from which KAWL keys for encryption/decryption and CMACing of application software and Operator group configuration are derived	I_CZD_SEND_KEY_CMPNT_AUTH
	Reset the login and return to the pre-expired login.	I_CZD_RESET_LOGIN
	Delete the KAWL keys.	I_CZD_DELETE_KBR
	Configure the groups of crypto Operator.	I_CZD_CONFIG_GROUP
	Create members of the groups of crypto Operators.	I_CZD_CREATE_GRP_MEMBER
	Delete members of the groups of crypto Operators.	I_CZD_DELETE_GRP_MEMBER

Role	Authorised Services	Input
	Authenticate by username and password.	I_CZD_USER_AUTH
	End authentication.	I_CZD_LOGOFF
	Change password.	I_CZD_CHG_PWD
	Self-Test services.	I_STD_ECHO, I_STD_SELF_TEST, I_ALA_SELF_TEST, DEP_Test
	Show-status services.	I_STD_GET_DEP_DIAGNOSTICS, I_STD_GET_DEP_STATUS, I_STD_GET_SERIAL_NR, I_STD_GET_TAG_STATUS, I_ALA_GET_COUNTERS, I_ALA_GET_LOG_BLOCK, I_ALA_GET_LOG_STATUS, I_ALA_GET_STATUS, I_ALA_HDW_VERSION, I_ALA_SFW_VERSION, I_CZD_GET_INIT_STATUS, I_CZD_GRP_NAME_QUERY, I_CZD_USER_NAME_QUERY
	Save the Operator group configuration in encrypted form.	I_CZD_BACKUP_USER_CONFIG
	Restore the Operator group configuration from previously saved encrypted form.	I_CZD_RESTORE_USER_CONFIG
	Reset alarm processor.	DEP_Reset 4
	Reset 386 processor.	DEP_Reset 2
Software-loading Operator role (User role)	Authenticate by username and password.	I_CZD_USER_AUTH
	End authentication.	I_CZD_LOGOFF
	Upload software in the DEP/PCI, only in dual control.	I_STD_SW_LOAD

Role	Authorised Services	Input
	Self-Test services.	I_STD_ECHO, I_STD_SELF_TEST,I_ALA_SELF_TEST, DEP_Test
	Show-status services.	I_STD_GET_DEP_DIAGNOSTICS, I_STD_GET_DEP_STATUS, I_STD_GET_SERIAL_NR, I_STD_GET_TAG_STATUS, I_ALA_GET_COUNTERS, I_ALA_GET_LOG_BLOCK, I_ALA_GET_LOG_STATUS, I_ALA_GET_STATUS, I_ALA_HDW_VERSION, I_ALA_SFW_VERSION, I_CZD_GET_INIT_STATUS, I_CZD_GRP_NAME_QUERY, I_CZD_USER_NAME_QUERY
	Change password.	I_CZD_CHG_PWD
	Reset alarm processor.	DEP_Reset 4
	Reset 386 processor.	DEP_Reset 2
Non-authenticated role	Self-Test services.	I_STD_ECHO, I_STD_SELF_TEST, I_ALA_SELF_TEST, DEP_Test
	Show-status services.	I_STD_GET_DEP_DIAGNOSTICS, I_STD_GET_DEP_STATUS, I_STD_GET_SERIAL_NR, I_STD_GET_TAG_STATUS, I_ALA_GET_COUNTERS, I_ALA_GET_LOG_BLOCK, I_ALA_GET_LOG_STATUS, I_ALA_GET_STATUS, I_ALA_HDW_VERSION, I_ALA_SFW_VERSION, I_CZD_GET_INIT_STATUS, I_CZD_GRP_NAME_QUERY, I_CZD_USER_NAME_QUERY
	Reset alarm processor.	DEP_Reset 4
	Reset 386 processor.	DEP_Reset 2

Table 6: Services authorised for roles

More information about the services of DEP/PCI and how to invoke them can be found in the corresponding guidance documentation, see: "Introduction to DEP", version 03.03, "DEP Customer's Security Officer's Guide", version 04.03, "DEP Quick Load Guide", version 03.02, and in particular "Detailed Functional Specification, Software BOOT", version 04.00.08, all by Atos Worldline S.A./N.V.

3.2. CRITICAL SECURITY PARAMETERS (CSPs)

The CSPs are the critical security parameters defined in the DEP/PCI. The complete list is given in the Table 7.
No integrity test on the CSPs is present in the DEP/PCI.

CSP Name	CSP Use/Source
Pre-expired usernames and passwords for the Customer Administrators (crypto officers)	Provided by Atos Worldline S.A./N.V. for first-time authentication of the Administrators. Only SHA-256 hashes of the pre-expired passwords are stored in DEP/PCI.
Passwords of the Customer Administrators (crypto officers)	New passwords created by the Administrators. They replace the pre-expired passwords and must be used for every subsequent authentication of the Administrators. Only SHA-256 hashes of the passwords are stored in DEP/PCI.

CSP Name	CSP Use/Source
KAWL base secret (256 bit long) and KAWL keys derived thereof KAWL_CMAC_SW, KAWL_ENC_SW, KAWL_CMAC_GroupConfig, KAWL_ENC_GroupConfig (all AES-256 keys)	KAWL base secret is generated by Atos Worldline S.A./N.V. and is provided securely to the Customer Administrators in split knowledge (two components). Each split knowledge component of the KAWL base secret is 256 bit long. The Customer Administrators load the components of the KAWL base secret into the DEP/PCI via the C-ZAM/DEP. After entry of each component, DEP/PCI recombines these and derives the following keys from the resulting KAWL base secret: KAWL_CMAC_SW, to verify the Software Authentication Code (SWAC) of the DEP Application Software; KAWL_ENC_SW, to decrypt the loaded DEP Application Software; KAWL_CMAC_GroupConfig, to generate/verify the CMAC of the Operator group configuration while saving/restoring it, respectively; KAWL_ENC_GroupConfig, to encrypt/decrypt the Operator group configuration while saving/restoring it, respectively.
Usernames/passwords of the groups of Operators (users)	First each group member creates his password and username, under the control of the Administrators. The username and password are used to authenticate the Operators for the function allowed by its group only. Only SHA-256 hashes of the passwords are stored in DEP/PCI.

Table 7: List of CSPs

3.2.1. Access rights within services

Service	Cryptographic Keys And CSPs	Access Type(s) Read/Write/ Execute	Role(s)
Replace pre-expired password	Password	W	Customer Administrator
Change password	Password	W	Customer Administrator, Software-loading Operator

Service	Cryptographic Keys And CSPs	Access Type(s) Read/Write/ Execute	Role(s)
Enter the KAWL base secret	KAWL base secret (components), KAWL_CMAC_SW, KAWL_ENC_SW, KAWL_CMAC_GroupConfig, KAWL_ENC_GroupConfig,	W	Customer Administrator
Delete the KAWL keys	KAWL_CMAC_SW, KAWL_ENC_SW, KAWL_CMAC_GroupConfig, KAWL_ENC_GroupConfig,	W	Customer Administrator
Configure groups		W	Customer Administrator
Create groups	Passwords/usernames	W	Customer Administrator
Delete groups	Passwords/usernames	W	Customer Administrator
Save Operator group configuration	Passwords/usernames	R	Customer Administrator
	KAWL_CMAC_GroupConfig	E	
	KAWL_ENC_GroupConfig	E	
Restore Operator group configuration	Passwords/usernames	W	Customer Administrator
	KAWL_CMAC_GroupConfig	E	
	KAWL_ENC_GroupConfig	E	
Authenticate by name and password	Pre-expired password and password, Administrator password and username, group member password and username	E	Customer Administrator, Software-loading Operator
Load DEP Application Software	DEP Application Software	W	Software-loading Operator
	KAWL_CMAC_SW	E	
	KAWL_ENC_SW	E	
Reset (zeroization)	Destroy all CSPs	E	All roles
Remove DEP Software Application	Destroy all CSPs of the DEP Software Application	E	All roles

Table 8: Access rights within services

3.3. APPROVED MODE OF OPERATION

The object of the current validation is the DEP/PCI with the boot firmware, FPGA firmware and alarm firmware only. The DEP/PCI is intended to load DEP Application Software; it provides a limited set of cryptographic functions and it always operates in Approved mode of operation.

The DEP/PCI implements the following approved algorithms:

- AES-128, AES-192 and AES-256 encryption in ECB mode, encryption/decryption in CBC mode and CMAC verification (Cert. #883)
- SHA-1, SHA-256, SHA-384 and SHA-512 for hashing data (Cert. #875; only SHA-256 is used by boot firmware functionality, SHA-1, SHA-384 and SHA-512 may be used by a loaded application software)

As mentioned above, the DEP/PCI as certified (i.e. without DEP Application Software loaded) is always running in the Approved mode of operation. Operators may run the command I_STD_GET_DEP_STATUS (command tag 02000B00) from the management application to query whether the boot firmware is still active, i.e. no DEP Application Software was loaded. I_STD_GET_DEP_STATUS responds with a data structure called D_STD_DEP_STATUS (data tag 01001300), which contains the data field STD_CAPA_NBR_TOT. If this data field is equal to 0000, the boot firmware is still active and no application software has been loaded, i.e. the module is operating in the certified configuration and therefore also in the Approved mode of operation.
For details about how to invoke I_STD_GET_DEP_STATUS command and how to interpret its response please see "Detailed Functional Specification, Software BOOT", version 04.00.08, by Atos Worldline S.A./N.V., in particular chapters 5.2.3, I_STD_GET_DEP_STATUS, and 5.3.9, D_STD_DEP_STATUS.

3.4. SELF TESTS

The DEP/PCI shall perform the self-tests described in the three sections below.

3.4.1. Power-up self-tests

At each power-up, the DEP/PCI itself initiates the following tests:

- Cryptographic Algorithm test:
  - AES KATs (ECB encryption, CBC encryption decryption, 128, 192, 256 bit keys)
  - CMAC verification KAT
  - SHA-1, SHA-256, SHA-384, SHA-512 KATs
- Integrity check:
  - Boot firmware integrity test based on CRC-CCITT 16 bit check
  - Alarm firmware integrity test based on CRC-CCITT 16 bit check
  - Application software integrity test based on CRC-CCITT 16 bit check

- Critical function test:
    - Functional test of the FPGA
    - Sensors Tests
      Purpose is to check that all alarm sensors are working well.

The Administrators can also initiate these tests on demand for periodic testing of the cryptographic module, using the command I_STD_SELF_TEST.

3.4.2. Conditional self-tests

The following conditional self-tests will be performed:

- Software load test (SWAC),
- Key-integrity check (i.e. Check of type NORM), when a component of the KAWL base secret is manually entered.

3.4.3. Error state

If one of the self-tests fails, the DEP/PCI enters an error state and cryptographic operations are disabled. Only the functions to obtain a status or to redo self-tests are allowed.
If one of the self-tests fails continuously, there is no way to recover from this error state and the card must be returned to the manufacturer.

4. PHYSICAL SECURITY POLICY

The DEP/PCI is tamper-evident and tamper-responsive. Its metal cover is suitable to give evidence about any physical tampering or tamper attempt. DEP/PCI furthermore responds to an detected attack by destroying (zeroizing) the confidential data present in the DEP/PCI. This behaviour guarantees both confidentiality and integrity of the confidential data.

The data that must be deleted is all data that has been loaded or internally generated in the DEP/PCI since it was manufactured, or since a previous alarm caused the erasure of all data.

The crypto officers can also use the Reset Alarm Card command in order to erase all data and CSPs.

4.1. PHYSICAL SECURITY MECHANISMS

The DEP/PCI is a multi-chip embedded cryptographic module as defined by FIPS140-2 section 4.5. It is encapsulated in a three-layered, hard, opaque, tamper-evident enclosure. The innermost layer is a flex sheet covered on the inside with special tamper-detection wiring; the middle layer consists of an epoxy potting material and the outer layer consists of a cold-rolled steel enclosure.

The DEP/PCI cryptographic module fulfils the FIPS140-2 Security Level 3 physical requirements with its strong enclosure surrounding the alarm card, which is causing serious damage to the module when an attempt is made to remove or penetrate it (furthermore, inside the strong enclosure a hard opaque potting material is encapsulating the alarm card). There are some components on the DEP/PCI PCI card outside of the enclosure/potting (i.e. interface components, power supply and batteries), but these components are excluded from the requirements of FIPS140-2.

Beyond fulfilment of the physical security requirements of FIPS140-2 Security Level 3, DEP/PCI implements other physical security mechanisms, which are explained hereinafter in section 5 about mitigation of other attacks.

4.2. CUSTOMER ADMINISTRATORS REQUIRED ACTIONS

The customer Administrators are required to inspect the DEP/PCI after an alarm occurred, or when loading DEP Application software.

Physical security mechanisms	Recommended frequency of inspection/test	Inspection/test guidance details
Hard opaque tamper-evident metal cover	♦ Upon installation of the DEP/PCI within a host system ♦ If in a corresponding alarm state ♦ Periodically, as appropriate in the environment of use	Inspect the DEP/PCI metal cover for any sign of tamper attempts including scratches, gouges and suspicious marks on the metal housing.
Tamper-response and zeroization circuit	♦ Once every 2 years	Verify tamper-response behaviour with respect to movement, power level above or below normal, temperature above or below normal.
Alarm log files	♦ If in a corresponding alarm state ♦ Periodically, as appropriate in the environment of use	Review the alarm log files.

Table 9: Inspection/testing of Physical Security Mechanisms

5. SECURITY POLICY FOR MITIGATION OF OTHER ATTACKS

Beyond fulfilment of the security requirements of FIPS140-2 Security Level 3, DEP/PCI implements several security mechanisms to mitigate attacks not addressed by Security Level 3 requirements:

- **Temperature out-of-range detection**:
  An attacker might try to induce faults in the operation of the DEP/PCI by applying a temperature, which is out of range. Induced faults could apply cryptographic operations (for instance to mount a Differential Fault Analysis) as well as other security-relevant processing in the DEP/PCI.
  To mitigate this attack, a temperature sensor on the alarm card activates a tamper response (zeroization of CSPs) when the temperature goes out of the defined operational range of 0°C to 80°C.
- **Battery voltage out-of-range detection:**
  An attacker might try to manipulate the battery voltage input to the alarm card to take influence on the tamper detection and response mechanisms (powered by the battery voltage).
  To mitigate this attack, a voltage sensor on the alarm card, based on a comparator integrated circuit, activates a tamper response (zeroization of CSPs) if the battery voltage is below 2.9V or above 3.7V (nominal value is 3.3V). Tamper response will even be effective in case of a very fast drop of the battery voltage (e.g. power loss/cut), as dedicated capacitances on the alarm card guarantee that still zeroization can be performed.
- **Removal detection:**
  An attacker might try to remove DEP/PCI from its PCI slot to be able to have easier physical access.
  To mitigate this attack, removal of the DEP/PCI from its PCI slot is detected via this mechanism implemented on the alarm card. If removal is detected, a tamper response (zeroization of CSPs) is activated.
- **Physical penetration/drilling detection**:
  An attacker might try to overcome the enclosure of the alarm card by methods beyond the scope of FIPS140-2 Security Level 3.
  To mitigate such physical attacks, a flexible wiring consisting of very fine copper and silver lines encapsulates the alarm card and allows the detection of all kind of physical and chemical penetration (e.g. drilling, grinding, etching etc.). Dedicated circuitry on the alarm card detects if a line of the wiring is cut or if a shortcut between different lines of the wiring is made, and activates a tamper response (zeroization of CSPs) in this case.
- **Acceleration detection**:
  An attacker might try to move the PCI host device DEP/PCI is mounted in to get easier access to DEP/PCI or to remove the host device including DEP/PCI from its operational environment (e.g. to mount subsequent attacks in a laboratory environment).

To mitigate this attack, an accelerometer sensor on the alarm card activates a tamper response (zeroization of CSPs) when the DEP/PCI undergoes an acceleration of more than 0.015625g during more than one second along any of the three axes (this sensor furthermore mitigates all physical attacks on the steel enclosure of the alarm card, which cause signification vibration, e.g. bending, drilling, grinding).

DEP/PCI does not implement mechanisms for the mitigation of any side-channel attacks such as Power Analysis, Timing Analysis or TEMPEST attacks. However, DEP/PCI has a low level of electromagnetic signal emission compliant with the EMI/EMC requirements as specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

6. DEFINITIONS AND ACRONYMS

AES	Advanced Encryption Standard
AWRDI	Atos Worldline S.A./N.V. relevant data item
CBC	Cipher Block Chaining
CMAC	Cipher-based MAC
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DEP	Data Encryption Peripheral
EEPROM	Electrically Erasable Programmable Read-Only Memory
EFP/EFT	Environmental Failure Protection/Testing
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
HSM	Hardware Security Module
PKI	Public Key Infrastructure
KAT	Known Answer Test
LED	Light-Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NORM (check of type)	First 3 bytes of the encryption of a string of 16 bytes of zeroes with the key to be checked
RAM	Random-Access Memory
RSA	Rivest, Shamir and Adleman Public Key Algorithm
SWAC	Software Authentication Code

7. REFERENCES

- FIPS Pub 140-2: Security Requirements for Cryptographic Modules, May 25, 2001, plus change notices 1 to 4 (December 3, 2003), together with relevant
  - Annex A – Approved Security Functions,
  - Annex B – Approved Protection Profiles,
  - Annex C – Approved Random Number Generators,
  - Annex D – Approved Key Establishment Techniques,
- Derived Test Requirements for FIPS Pub 140-2, Security Requirements for Cryptographic Modules, March 24, 2004, Draft,
- Implementation Guidance for FIPS Pub 140-2 and the Cryptographic Module Validation Program,
- FIPS 197, Specification for the Advanced Encryption Standard (AES), November 26, 2001,
- FIPS 180-2 with change Notice 1 dated February 25, 2004, Secure Hash Standard (SHS),
- Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2004,
- NIST Special Publication 800-57, March 2007, Recommendation for Key Management – Part 1: General (Revised)