Atos Worldline
An Atos Origin Company

Haachtsesteenweg 1442
1130 Brussels
Belgium

DEP Documentation

DEP ATOS Worldline Security Officer Guide

Version Management Report

Version	Name(s)	Date	Comments
01.00	TheSteamFactory	23/05/2000	First Draft
01.01	TheSteamFactory	05/06/2000	Second Draft
01.02	TheSteamFactory	04/10/2000	Third Draft
01.03	TheSteamFactory	20/11/2000	Final Draft
02.00	F. Demaertelaere	01/03/2001	Final version
03.00	F. Demaertelaere	20/02/2003	Documentation Platform Independent
03.01	F. Demaertelaere	31/07/2003	Update to new DEP PC AUX Program
03.02	P.Stienon, P.Verbelen	21/04/2006	New disclaimer, review
03.03	P.Stienon	29/08/2006	Merge of document “Delivery Procedures 1.0(6)”
03.04	P.Stienon	27/03/2008	Take into account of the Fips140-2 validation, disclaimer, ATOS ⇔Atos Worldline
03.05	N. Aboudagga, P. Stienon	01/04/2008	Update for FIPS certification
03.06	P.VERBELEN	26/05/2008	Few typo corrections
03.07	P.Stienon	20/06/2008	Idem, versions, number of DCCs
03.08	P.Stienon	01/09/2008	Correction for alarm software
04.00	Anna Papayan	16/02/2011	Information about DCS, KAWLs and hardware delivery report.

CONFIDENTIALITY

The information in this document is confidential and shall not be disclosed to any third party in whole or in part without the prior written consent of Atos Worldline S.A./N.V.

COPYRIGHT

LEGAL DISCLAIMER

While Atos Worldline S.A./N.V. has made every attempt to ensure that the information contained in this document is correct, Atos Worldline S.A./N.V. does not provide any legal or commercial warranty on the document that is described in this specification. The technology is thus provided "as is" without warranties of any kind, expressed or implied, included those of merchantability and fitness for a particular purpose. Atos Worldline S.A./N.V. does not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product or process disclosed.
To the fullest extent permitted under applicable law, neither Atos Worldline S.A./N.V. nor its affiliates, directors, employees and agents shall be liable to any party for any damages that might result from the use of the technology as described in this document (including without limitation direct, indirect, incidental, special, consequential and punitive damages, lost profits).

JURISDICTION AND APPLICABLE LAW

These terms shall be governed by and construed in accordance with the laws of Belgium. You irrevocably consent to the jurisdiction of the courts located in Brussels for any action arising from or related to the use of this document.

1. TABLE OF CONTENTS

1. TABLE OF CONTENTS 4

2. SCOPE OF THE DOCUMENT 6

2.1. REFERENCES 6

3. ATOS WORLDLINE ENVIRONMENT 7

4. AUTHORITY LEVELS AND MODES OF OPERATION 8

4.1. SET-UPS 8
4.2. KAWL KEY SET-UP 8
4.3. KBKS KEYS SET-UP 8
4.4. DCCS AND MODES OF OPERATION 9

5. CREATING BANKSYS DEFINITION LIST 11

5.1. CREATE THE BKS SECRET SHARING DEFINITION LIST 11
5.2. CREATE BKS CAPABILITY DEFINITION LIST 11
5.3. CREATE BKS KEY DEFINITION LIST 11
5.4. SAVE THE DEFINITION LISTS ON THE PC 12

6. CREATING A NEW CUSTOMER 13

6.1. CREATING CUSTOMER IDENTIFICATION 13
6.2. CREATING BANKSYS AUTHORITY KEYS 13
6.3. CREATING PRE-EXPIRED USERNAMES AND PASSWORDS 14
6.4. CREATING KAWL KEY 14

7. CREATING DCCS 14

7.1. CREATION PROCESS 15
7.1.1. Personalization of the Storage DCCs 15
7.1.1.1. Customer and Cust_ID 15
7.1.1.2. Mode 16
7.1.1.3. Card type and number 16
7.1.1.4. Card Parameters and Version Number 16
7.1.1.5. Write the Storage DCC 16
7.1.2. Personalization of the List DCCs 16
7.1.2.1. List Init 17
7.1.2.2. Number sets of cards 17
7.1.2.3. Write the List DCCs 17
7.1.3. Personalization of the DCSs 17
7.1.3.1. Card type and number 17
7.1.3.2. Write the Dual Control Storage 17
7.2. DATABASE STORAGE 17

8. APPLICATION SOFTWARE INTEGRITY AND CONFIDENTIALITY . 19

8.1. PROTECTION OF CONFIDENTIALITY FOR FIPS-CERTIFIED DEPS 19
8.1. PROTECTION OF CONFIDENTIALITY FOR NON-FIPS DEPS 19

9. DELIVERY 21

9.1. DELIVERY HARDWARE 21

9.1.1. DEP Platform *21*
9.1.2. C-ZAM/DEP Xentissimo *22*
9.1.3. Cust_ID *22*
9.1.4. Pre-expired usernames & passwords *22*
9.1.5. KAWL key components *22*
9.1.6. DCC *22*
9.1.6.1. Smart cards 22
9.1.6.2. Use DCC Personalisation System 22
9.1.6.3. Labelling 23
9.1.7. Delivery Documentation *24*
9.1.7.1. Hardware Delivery Report 24
9.2. DELIVERY SOFTWARE 25
9.2.1. DEP Software Handover Form *26*
9.2.2. Delivery Confirmation Document *27*
9.3. DELIVERY DOCUMENTATION 27

10. MANAGEMENT ISSUES 28

11. ANNEXES 29

11.1. DELIVERY CONFIRMATION DOCUMENT 29
11.2. DEP SOFTWARE HANDOVER FORM 30
11.3. DEP HARDWARE DELIVERY REPORT 31

2. SCOPE OF THE DOCUMENT

This document provides an overview of all operations that have to be performed by the DEP Atos Worldline Security Officer (DEP AWL security officer) or by the Third Party's Security Officer to set-up and maintain a DEP Environment.

The document describes how to create a new customer to be managed, together with the management of the KAWL key, the BKS Authority Keys, DEP Control Cards (DCCs) and Application Software integrity/confidentiality. It deals also with the delivery procedures that have to be followed to maintain security when distributing the DEP products..

This guide is especially intended for the DEP AWL Security Officer or the Third Party's Security Officer but could offer additional information to other audience.

2.1. REFERENCES

This document contains references to other documents about the DEP. This paragraph gives a list of all the documents referred to:

- *DEP PC-AUX Program User Manual*
- *DEP C-ZAM/DEP User Manual*
- *DEP Customer's Security Officer's Guide*
- *DEP Security Mechanisms*
- *DEP/T6 Owner's Manual*
- *DCC Personalisation System User Manual*
- *DEP General Architecture*
- *DEP/PCI Security Policy*

There are no references made to the following documents, but they could be useful to understand this document.

- *DEP Introduction to DEP*
- *DEP Glossary*

3. ATOS WORLDLINE ENVIRONMENT

The DEP AWL Security Officer maintains the environment that is used for generating the deliveries. This environment is located at the Atos Worldline office. Only DEP AWL Security Officers are allowed to use this environment.

The environment consists of:

- A PC connected to DEP (not connected to any network), containing:
  - The DCC Personalisation System for the creation of DCCs and software signature,
  - The DEP Signing Tool to generate KAWLs,
  - Logbooks containing the created deliveries.
- A C-ZAM/PC, serving as a Smart Card Reader/Writer,
- A printer directly connected to the DEP/T6 via the COM port to print the KAWLs;

The PC, C-ZAM/PC and printer are located in a secure room at the Atos Worldline security department.

4. AUTHORITY LEVELS AND MODES OF OPERATION

4.1. SET-UPS

The DEP/PCI must be first configured from the Original Password State (initial state with the boot software) to the state DEP Application loaded. During this phase, the KAWL key will play an important role for software integrity checking.

As described in the document *DEP General Architecture*, in the state DEP Application loaded, there are different Authority Levels. All the devices of a functional operational DEP Environment should be set to the Customer Authority Level.

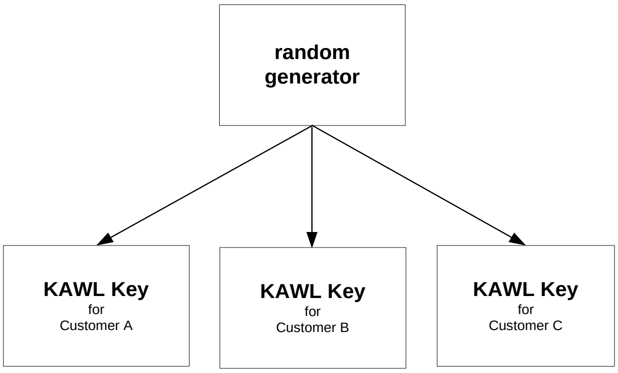
To increase the security and the manageability of the system, it is decided that every customer receives a unique KAWL key and a unique set of BKS Authority Keys.

Because these keys are different/unique per customer, they can be given to the specific Customer’s Security Officer without jeopardising the DEP Environment of other customers. The Customer’s Security Officer can reload the C-ZAM/DEP and the DEP Platform on his own without any intervention by DEP AWL Security Officer.

For more information about Authority Levels, refer to the document *DEP General Architecture*.

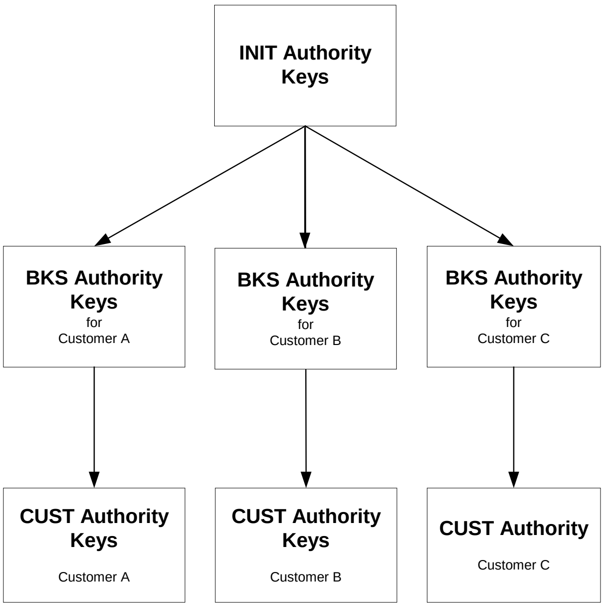
4.2. KAWL KEY SET-UP

This key will be used by the Customer administrators to initialise the DEP/PCI.



4.3. KBKS KEYS SET-UP

These keys are used at the application-loaded phase to personalize the DEP/PCI so that it can use the cryptographic functions.


INIT Authority Keys
BKS Authority Keys for Customer A
BKS Authority Keys for Customer B
BKS Authority Keys for Customer C
CUST Authority Keys Customer A
CUST Authority Keys Customer B
CUST Authority Customer C

These 2 set-ups are the basis for the DEP AWL Security Officer operations.

4.4. DCCS AND MODES OF OPERATION

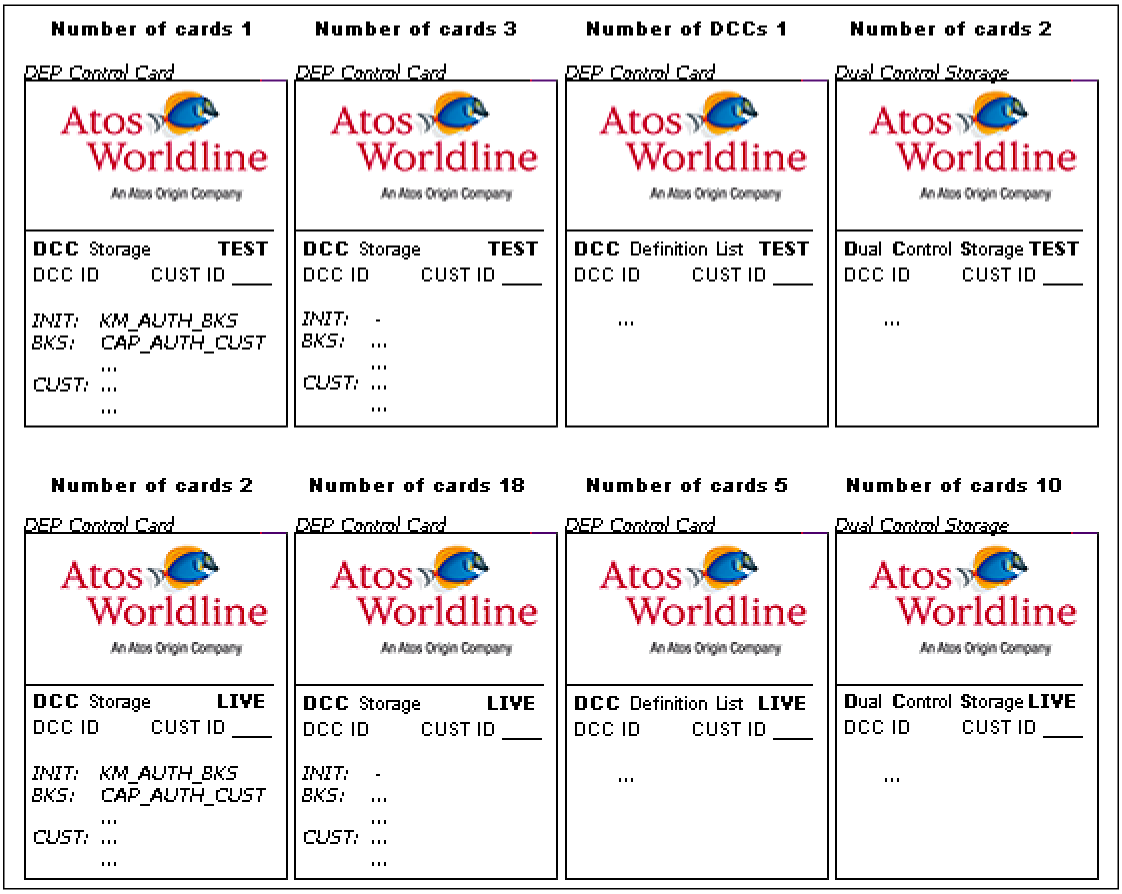
A standard distribution of DCCs is defined. This package contains DCCs for the Test Mode of Operation and the Live Mode of Operation. The Customer Identification 0001 is used for the entire set of Test DCCs and the real Cust ID is used for the Live DCCs.

All the delivered DCCs are at BKS Authority Level.

The following DCCs are handed over to the Customer’s Security Officer when the standard package is delivered:

- 2 DCC Storage with TEST mode of operation (CUST ID 0001) containing the KM_AUTH_BKS and the CAP_AUTH_CUST
- 2 virgin DCC Storage with TEST mode of operation (CUST ID 0001)
- 1 DCC List with TEST mode of operation (CUST ID 0001) containing the Atos Worldline Definition List (see paragraph 5 on page 11)
- 2 virgin Dual Control Storage with TEST mode of operation (CUST ID 0001)

- 2x2 DCC Storage with LIVE mode of operation containing the KM_AUTH_BKS and the CAP_AUTH_CUST
- 16 virgin DCC Storage with LIVE mode of operation
- 5 DCC List with LIVE mode of operation containing the Atos Worldline Definition List (see paragraph 5 on page 11)
- 10 virgin Dual Control Storage with LIVE mode of operation



The DCCs are PIN protected to avoid un-allowed access to the information on the DCCs. The DCCs given to the customer are protected by the PIN “1234”, it is the responsibility of the Customer Security Officer to change this PIN.

The DCCs with the KM_AUTH_BKS and CAP_AUTH_CUST contain sufficient information for the Customer’s Security Officer to generate the CUST Authority Keys. Note that the DEP AWL Security Officer will not define the CUST Authority Keys. The Customer’s Security Officer will define his own CUST Authority Keys. In this way he can be certain he is the only one *knowing* the secret values.

More information on the creation of the CUST Authority Keys can be found in the document *DEP Customer’s Security Officer’s Guide*.

The DCS are used for FIPS certified DEP/PCI and used to store the credentials of customer administrators’ and software-loading operators, KAWL components, and key parts for key reconstruction in DEP.

Additional DCCs can be obtained on request. E.g. it could also be possible that the customer needs additional DCCs for storing keys and capabilities; although the Customer’s Security Officer has received two identical DCC sets containing the necessary information to create the CUST Authority Keys, it could always be possible that the customer needs additional DCCs containing the BKS Authority Keys and the CUST Authority Capability (e.g. in case of defect)…

5. CREATING BANKSYS DEFINITION LIST

The banksys Definition Lists are the Definitions Lists at BKS Authority Level. They need to be generated before DCCs can be created.

The creation of the Atos Worldline Definition Lists is done using the *DEP PC-AUX Program*. For a detailed description of how to use this program, refer to the *DEP PC-AUX Program User Manual*.

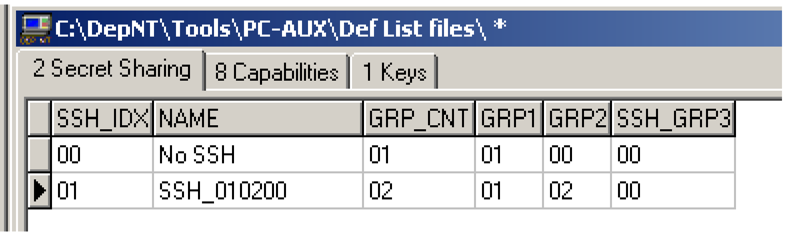
The following Definition Lists must be created:

- BKS Secret Sharing Definition List
- BKS Capability Definition List
- BKS Key Definition List

Of course, these Definition Lists should only be created when they do not exist yet.

5.1. CREATE THE BKS SECRET SHARING DEFINITION LIST

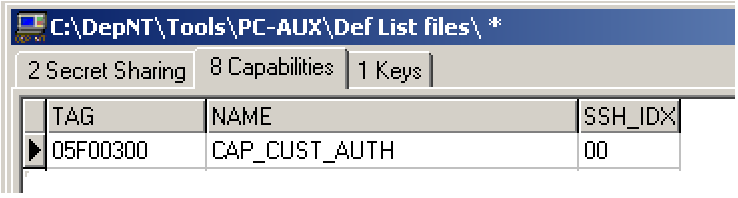
Enter the following secret sharing scheme in the Secret Sharing Definition List (refer to the *DEP PC-AUX Program User Manual*).



	SSH_IDX	NAME	GRP_CNT	GRP1	GRP2	SSH_GRP3
	00	No SSH	01	01	00	00
▶	01	SSH_010200	02	01	02	00

5.2. CREATE BKS CAPABILITY DEFINITION LIST

Enter the following capability definitions in the Capability Definition List (refer to the *DEP PC-AUX Program User Manual*).

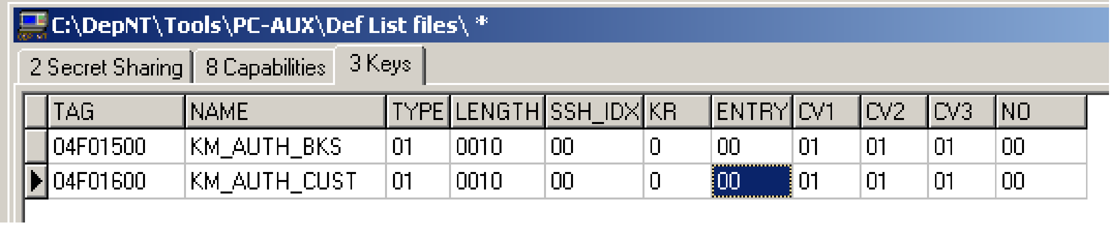


	TAG	NAME	SSH_IDX
▶	05F00300	CAP_CUST_AUTH	00

5.3. CREATE BKS KEY DEFINITION LIST

Enter the following key definitions in the Key Definition List (refer to the *DEP PC-AUX Program User Manual*).

NEW DEFINITION LIST FORMAT



TAG	NAME	TYPE	LENGTH	SSH_IDX	KR	ENTRY	CV1	CV2	CV3	NO
04F01500	KM_AUTH_BKS	01	0010	00	0	00	01	01	01	00
04F01600	KM_AUTH_CUST	01	0010	00	0	00	01	01	01	00

5.4. Save the Definition Lists on the PC

When the Definition Lists are created they must be saved (refer to the *DEP PC-AUX Program User Manual*).

Afterwards they are included (through a shortcut) in the DCC Personalisation System.

6. CREATING A NEW CUSTOMER

As described in the document *DEP Security Mechanisms*, there are two alternative methods to bring the DEP Environment in BKS Authority Level:

- BKS Authority Keys are generated inside the C-ZAM/DEP
- BKS Authority Keys are generated by the DCC Personalisation System

Creating a new customer is different between the two methods, especially for the creation of the DCCs and the management of the BKS Authority Keys.

Because in practice only the latter alternative is used, the paragraphs below do not explain the use of the C-ZAM/DEP when creating a new customer.

6.1. CREATING CUSTOMER IDENTIFICATION

Each customer has to be assigned a unique Customer Identification number (CUST ID), identifying the customer in the DEP Environment. A CUST ID is defined as a 2 byte hexadecimal value.

To guarantee the uniqueness, it is necessary to keep a table with the names of the customers and their CUST ID. This table is managed in the DCC Personalisation System.

This task has to be performed only once for each new customer.

Remark that one CUST ID (*0001*) is dedicated to a *Test Customer*. This CUST ID is then used for setting up a test environment.

6.2. CREATING BANKSYS AUTHORITY KEYS

For every customer, a unique set of BKS Authority Keys has to be defined. The DCC Personalisation System generates automatically new and random BKS Authority Keys when creating a new Customer (Identification).

After the generation of the BKS Authority Keys, they will be saved in a password-encrypted database and will remain under control of the DEP AWL Security Officer that possesses the password.

This task has to be performed only once for every new customer.

For more information, refer to the *DCC Personalisation System User Manual.*

6.3. CREATING PRE-EXPIRED USERNAMES AND PASSWORDS

The Security Officers in the security department of Atos Worldline have generated the pre-expired passwords and usernames for the customer administrators to be used as the initial authentication credentials for the FIPS certified DEP Platforms. These credentials are identical for all the customers. However, the DEP cannot perform any security operation, unless the pre-expired credentials have been changed by the Customer Administrator (crypto officers) of the customer.

6.4. CREATING KAWL KEY

For every customer, a unique KAWL key has to be defined. The random KAWL key is generated in the DEP. The DEP Signing Tool is used for KAWL generation, which is running on PC directly connected to the DEP.

After the generation, the KAWL keys are kept in the DEP memory and printed in two key components using the printer directly connected to the DEP/T6. Each customer administrator receives one KAWL component.

This task has to be performed only once for every new customer.

7. CREATING DCCS

DCCs can only be created for customers previously created and still available in the DCC Personalisation System.

During the creation of the DCCs, different information should be delivered to the DCC Personalisation System:

- Indication whether a DCC List,a DCC Storage or a DCS is personalised
- The Mode of Operation is TST or LIV, depending on a test environment or live environment
- The destination customer is selected by its unique CUST ID as generated (see paragraph 6.1 on page 13)
- The total number of DCCs and DCSs, and (only for DCC Storage) how many DCCs need to be created with the BKS Authority Key and the CUST Authority Capability
- Optionally, a dedicated PIN code should be entered (PIN 1234 is used for all DCCs)
- The earlier created Atos Worldline Definition Lists (see paragraph 5 on page 11) implicitly used by the DCC Personalisation System

7.1. CREATION PROCESS

During the personalisation process of the DCC, the DCC Personalisation System writes all the necessary information to obtain the DCCs defined in paragraph 4.4 on page 9.

The personalisation of DCCs is under control of the DEP AWL Security Officer that manages the password delivering access to the DCC Personalisation System.

During personalisation, the DCCs are put at BKS Authority Level. This means that:

- The complete directory structure of the DCC is created (INIT – BKS – CUST),
- At INIT Authority Level, the keys IK and AK, and the PIN are stored.

Three different DEP control cards are personalized: a DCC Storage, a DCC List and a DCS:

- DCC List: the lists with keys, capabilities and secret sharing schemes are stored on INIT Authority Level,
- DCC Storage: the *KM_AUTH_BKS* at INIT Authority Level and the *CAP_AUTH_CUST* are generated and stored at BKS Authority Level.
- DCS: only the file structure is created. No data is available except the CUST ID and the Mode of Operation.

7.1.1. Personalization of the Storage DCCs

During the personalization of the DCCs Storage, the following parameters must be defined:

- Customer
- Cust_ID
- Mode
- Card type and number
- Card Parameters
- Version number

7.1.1.1.Customer and Cust_ID

The Customer and its CUST_ID selected by default is the first one in the database. Select the correct customer and Cust_ID needed. If the customer does not exist yet, create a new, unique, Cust_ID.

7.1.1.2.Mode

Select the correct mode needed. Following modes are available:

- LIV
- DEV
- TST

7.1.1.3. Card type and number

Select *Storage* and enter the number of cards that will be personalized with the *KM_AUTH_BKS* and *CAP_AUTH_CUST*. The total number of cards will increase at the same time.

7.1.1.4. Card Parameters and Version Number

- Pin Code: The Pin code for all the DCCs is "1234"; the Pin code should be filled in manually.

- DCC ID: The DCC_ID is extracted from the database and automatically incremented with $1_{hex.}$

- Version Nb: The version number equals '0001'.

7.1.1.5.Write the Storage DCC

The application checks the data and after the confirmation of the DEP AWL Security Officer and the insertion of the First Storage DCC, the personalization will start. The DCC Personalisation System asks automatically for following DCCs to be inserted.

Each Liv DCC Storage and its PIN is delivered in a separate secure envelope. The secure envelopes provide tamper evidence. The customer Security Officer can contact the Atos Worldline sales representative to obtain the identification numbers of the secure envelopes.

7.1.2. Personalization of the List DCCs

During the personalization of the DCCs list, the following parameters must be defined:

- Customer
- Cust_ID
- Mode
- List Init
- Total number of cards
- Version number

The Customer, Cust_ID, Mode and version number are handled in the same way as the personalization of the Storage DCCs.

7.1.2.1.List Init

Personalizing a DCC List, the List Init must be selected because every customer has his own Definition Lists. List Init indicates that the default Definition Lists containing the capabilities and Authority keys will be written at INIT Authority Level on the DCC card.

7.1.2.2.Number sets of cards

For the DCC List, Nbr sets of cards are equal to 2. It indicates how many times the Security Officer wants to write the Definition Lists.

7.1.2.3.Write the List DCCs

The application checks the data and after the confirmation of the Security Officer and the insertion of the First List DCC, the personalization will start. The DCC Personalisation System asks automatically for following DCCs to be inserted.

For more information, refer to the *DCC Personalisation System User Manual*.

7.1.3. Personalization of the DCSs

During the personalization of the DCSs, the following parameters must be defined:

- Customer
- Cust_ID
- Mode
- Card type and number
- Version number

The Customer, Cust_ID, Mode and version number are handled in the same way as the personalization of the Storage DCCs.

7.1.3.1.Card type and number

Select *Dual Control Storage* and enter the number of cards.

7.1.3.2.Write the Dual Control Storage

The application checks the data and after the confirmation of the DEP AWL Security Officer and the insertion of DCS, the personalization will start. The DCC Personalisation System asks automatically for following DCSs to be inserted.

7.2. DATABASE STORAGE

For each created DCC following information is stored (encrypted) in a database:

- Cust_ID
- Date of creation

- Pin Code
- Mode
- Atos Worldline Authority Key

For each customer, the Application Software is kept in the database.

This database is kept on the stand alone PC and protected by a pass-phrase. The pass-phrase is required once during the following operations:

- To add, to delete or to edit a customer
- To change the pass-phrase, to compute a certificate (SAC)
- To decrypt a PIN
- To write a DCC.

A logging is kept of all the personalised DCCs containing the personalisation date and time, the DCC ID, the CUST ID and the PIN code. There is a different logging for DCC List, DCC Storage and DCS.

For more information, refer to the *DCC Personalisation System User Manual*.

8. APPLICATION SOFTWARE INTEGRITY AND CONFIDENTIALITY

For every customer and every Application Software version, a Software Authentication Code needs to be calculated to guarantee the integrity of the Application Software and to identify the supplier. A Software Authentication Code is a Message Authentication Code calculated over the DEP Application Software[1]. It is calculated by the DEP Atos Worldline' Security Officer.

8.1. PROTECTION OF CONFIDENTIALITY FOR FIPS-CERTIFIED DEPS

In addition, for FIPS certified DEP/PCI the KAWL secret is used for protection of confidentiality and authenticity of the DEP Application Software. The Application Software must be signed by the DEP AWL Security Officer, otherwise it will be rejected by the DEP.

The KAWL key is unique for every customer, and thus the verification of the Software Authentication Code and the decryption of the Application Software are done by the DEP/PCI itself using the KAWL key.

For this operation, the following information is needed:

- The Mode of Operation is TST or LIV, depending on a test environment or live environment
- The destination customer is selected together with its unique CUST ID as generated (see paragraph 6.1 on page 13)
- The clear-text Application Software

The output is the encrypted Application Software and a Software Authentication Code File containing the Software Authentication Codes for the selected Application Software and the selected customer(s).

8.1. PROTECTION OF CONFIDENTIALITY FOR NON-FIPS DEPS

The Application Software is encrypted by the DEP AWL Security Officer to guarantee the confidentiality.

[1] It is an AES256 CMAC evaluated on the DEP Application Software for FIPS-certified DEP Crypto Modules, and a SHA1 encrypted with the Banksys Authority Keys over the DEP Application Software for non-FIPS DEP Crypto Modules.

For non-FIPS DEP Crypto Modules only the DCC Personalisation System is able to generate encrypted Application Software and to calculate the Software Authentication Code.

For this operation, the following information is needed:

- The Mode of Operation is TST or LIV, depending on a test environment or live environment

- The destination customer is selected together with its unique CUST ID as generated (see paragraph 6.1 on page 13)

- The clear-text Application Software

The output is the encrypted Application Software and a Software Authentication Code File containing the Software Authentication Codes for the selected Application Software and the selected customer(s).

The BKS Authority Keys are used for both the decryption of the Application Software and the verification of the Software Authentication Code.

For more information, refer to the *DCC Personalisation System User Manual*.

9. DELIVERY

A DEP AWL Security Officer creates all deliveries. All deliveries are handed over to the Security Officer of the customer.

The Cust_ID (Customer Identification Number) is communicated to the Customer Security Officer by the DEP technician (DEP TECH) during the first delivery.

9.1. DELIVERY HARDWARE

A DEP technician always does the delivery. It consists of:

- Depending on the configuration:
  - A DEP Platform with at least one DEP Crypto Module, or
  - One or more DEP Crypto Modules,
- One or more C-ZAM/DEPs Xentissimo,
- A four digit Customer Identification number (Cust_ID),
- The following DCCs together with their PIN:
  - Test DCC Lists
  - Test DCC Storage
  - Liv DCC lists
  - Liv DCC Storage
  - Test DCSs
  - Liv DCSs
- 2 envelopes with the pre-expired usernames and passwords for the Customer Administrators,
- 2 envelopes with the KAWL key component with their corresponding key Check Values (key check of type NORM).

All the envelopes with the pre-expired credentials and KAWL key components are delivered to the right recipients.

It is the task of DEP marketing and sales (DEP MKT) to provide the DEP technician with the contact information head Security Officer of the customer.

The customer can ask for the name of the DEP technician to his Atos Worldline sales representative. Atos Worldline DEP technicians always carry their identity card. This allows the customer to verify the identity of the person presenting himself as being the DEP technician.

9.1.1. DEP Platform

A DEP Platform is a DEP/T6. For more information about DEP/T6 refer to the *DEP/T6 Owner's Manual* document. DEP Platforms are installed and configured by the DEP technician.

The DEP technician can collect DEP Platforms at the DEP manufacturer site.

9.1.2. C-ZAM/DEP Xentissimo

The C-ZAM/DEP is delivered to the customer at NONE authority level. This means that there are no keys or capabilities loaded in it (except for the hard-coded INIT authority level keys that are the same for each customer).

The DEP technician can order C-ZAM/DEPs at the Atos Worldline warehouse.

9.1.3. Cust_ID

The DEP AWL Security Officer guarantees that the customer identification number **Cust_ID** is unique. This is done using the DCC Personalisation System (see the *DCC Personalisation System User Manual*).

The DEP AWL Security Officer communicates the Cust_ID to the DEP technician.

9.1.4. Pre-expired usernames & passwords

Each customer administrator receives independently his own pre-expired credentials in a secure way and in nominative sealed secure envelope**.**

9.1.5. KAWL key components

Each component of the KAWL key is send to the adequate customer administrator via a secure way and a nominative sealed secure envelope**.** The special DMT tool is being used for printing the 2 KAWL components.

9.1.6. DCC

The DCCs are packaged in a secured envelope together with the corresponding PIN codes. The secured envelope contains the reference of the destination Customer's Security Officer.

This package is handed over to the Customer's Security Officer by a DEP technician.

9.1.6.1.Smart cards

When receiving a request of a customer, the DEP AWL Security Officer can order empty Smart Cards (type: Bull CP8 Integrated Chip Cards (ICC) with the TB Operating System) at the Atos Worldline warehouse. These are standard Smart Cards, delivered by the Smart Card manufacturer, which did not go through any procedure yet.

9.1.6.2.Use DCC Personalisation System

To convert the standard Smart Cards into the different DCCs that can be used in the DEP environment, the *DCC Personalisation System* is used. Only DEP AWL Security Officers are allowed to personalize the DCCs.

This tool performs the following actions:

- Bring the DCCs to the Banksys Authority level,
- Write the default Definition List on the DCCs.

Detailed information regarding this tool can be found in the *DCC Personalisation System User Manual*.

9.1.6.3.Labelling

For the Storage DCCs labels, following parameters are defined:

- Cust_ID: Customer identification.
- First STO: Number that is given to the first Storage DCC. The numbers for the following 3 DCCs are automatically incremented with 1.

For the List DCCs labels, following parameters are defined:

- Cust_ID: Customer identification.
- First List: Number that is given to the first List DCC. The numbers for the second DCC is automatically incremented with 1.

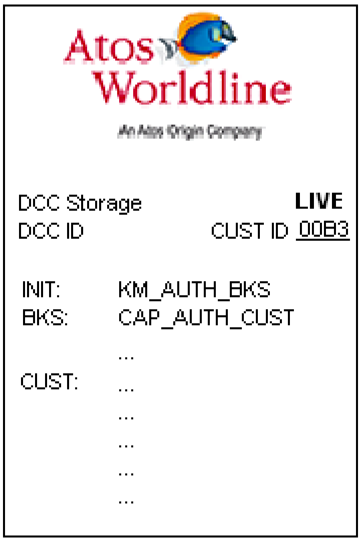
For the DCS labels, following parameters are defined:

- Cust_ID: Customer identification.
- First DCS: Number that is given to the first DCS. The numbers for the second DCS is automatically incremented with 1.

Note: If the labels are created for Test Mode DCCs, the Cust_IDs are always ‘0001’

Example of Live Storage label:

DEP Control Card

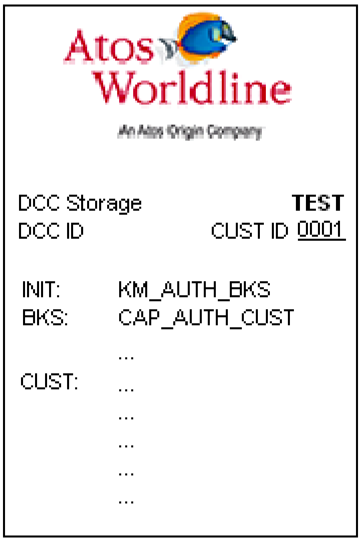


DCC Storage **LIVE**
DCC ID CUST ID 00B3

INIT: KM_AUTH_BKS
BKS: CAP_AUTH_CUST
...
CUST: ...
...
...
...
...

Example of Test Storage label:

DEP Control Card



DCC Storage **TEST**
DCC ID CUST ID 0001

INIT: KM_AUTH_BKS
BKS: CAP_AUTH_CUST
...
CUST: ...
...
...
...
...

9.1.7. Delivery Documentation

When the DEP technician delivers the DEP system, the hardware delivery report should be signed by both the Customer and the DEP Technician.

9.1.7.1.Hardware Delivery Report

A DEP Hardware Delivery Report document (see paragraph 11.3 on page 31) contains the following information:

- Client Name: name of the client,
- Customer ID: the Customer identification,
- Location/Site: location,
- Date and Time: the date and the time of the delivery,
- Item details
  - DEP/T6 Platform Serial Number: the serial number of the delivered DEP/T6,
  - DEP/T6 Platform Physical Key Serial Number: the serial number of physical key,
  - DEP/PCI Card
    - NON-FIPS / FIPS: indicated if the DEP/T6 is FIPS-certified or NON-FIPS (strikeout the non-applicable option),
    - TEST / LIVE: indicated the operation mode of the DEP/T6 (strikeout the non-applicable option),
    - Internal Serial Number: internal serial number,
    - External Serial Number: external serial number,
  - C-ZAM/DEP Serial Number: the serial number of C-ZAM-DEP,
  - # DCC: the number of DCCs,
  - # DCS: the number of DCSs,

- Incidents & Remarks: information about the incidents and additional remarks,
- Persons present at the deployment – Chain of Custody
  - Function: delivered by manufacturer hardware engineer and received by Customer,
  - Name: names of the Manufacturer Hardware Engineer and the Customer,
  - Signature: signatures of the Manufacturer Hardware Engineer and the Customer.

9.2. DELIVERY SOFTWARE

The software delivery consists of:

- DEP Application Software
- Software Authentication Code
- Hand Over Form document
- Delivery Confirmation Document

The role of the DEP AWL Security Officer is to guarantee the integrity (and confidentiality) of the Application Software.

Once the Software Authentication Code is calculated (and the Application Software is encrypted), the DEP AWL Security Officer gives the right to distribute/deliver the Application Software to the corresponding customer.

Before the Software Authentication Code File is transferred it has to be guaranteed that only the Software Authentication Codes for the dedicated customer are mentioned. Possibly other Software Authentication Codes must be deleted on the temporary copy.

It is not necessarily the DEP AWL Security Officer that sends the (encrypted) Application Software and Software Authentication Code to the Customer' Security Officer.

The media for distributing the (encrypted) Application Software and the SAC is not defined. Different alternatives are possible: encrypted e-mail, CD…

Together with the DEP Application Software and the SAC, a **Hand Over Form document** (see paragraph 11.2) is delivered to formalise the delivery of the DEP Software.

A **Delivery Confirmation Document (**see paragraph 11.1) is also forwarded to allow the customer to confirm the receipt of the delivery. When the customer receives the delivery, the customer should confirm the delivery by returning the **Delivery Confirmation Document**.

9.2.1. DEP Software Handover Form

A DEP Software Handover Form document (see paragraph 11.2 on page 30) contains the following information:

- Description
    - Software Name: name of the delivered software,
    - Date: finalization date of the software,
    - Project Leader: name of the Atos Worldline project leader,
    - Customer: name of the customer,
    - Short History: short history of the software,
    - Remarks: Additional remarks (optional)

- Acceptation Team
    - Release and Sub-Release Number tested: release and sub-release number that is tested,
    - Test Report: name of the Test Report,

- Software Details
    - Indicates if it is a Final or a Beta release,
    - Filename/Label: the file name of the software,
    - Version: software version,
    - File Date: Creation date of the software,
    - Size: Size of the software,
    - Support: How the software is delivered (e.g.CD-ROM, e-mail)

- Dependencies:
    - DEP PCI board: version number
    - Venus: version number
    - Alarm Software Version: version number
    - Boot Software Version: version number
    - Cloning Software Version: version number
    - DEP/NMS: version number
    - C-ZAM/DEP Version: version number

- Project and Team Leaders
    - Release Accepted: indicates if the current release accepted or no,
    - Replaces previous version: indicates if the previous version is replaced with the new one or no,
    - Date,
    - Names of the Project and Team leader.

9.2.2. Delivery Confirmation Document

A Delivery Confirmation document (see paragraph 11.1 on page 29) contains the following information:

- General information: general guidelines concerning the delivery.
- DEP Software information:
    - Software name: name of the delivered Software including the version number.
    - DEP Software Binary Name/Date: the file name and the delivery date of the Software.
    - Document references: this is an overview of all DFS/ADD documentation, which is delivered.
- Delivery Confirmation: confirmation of the receipt of the software, DEP Software Hand Over Form and documentation with the above references.
- Signature
- Company: the name of the company,
- Date,
- Customer’s Signature: customer signature.

9.3. DELIVERY DOCUMENTATION

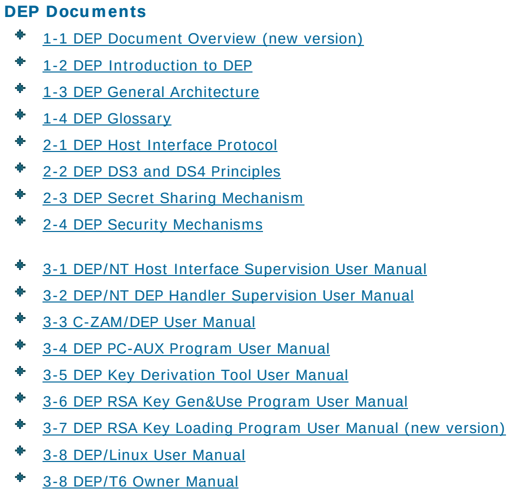
However, detailed information is available on the DEP and other Atos Worldline products from the following sources:

- The Atos Worldline internet site contains information on the full line of security products at www.atosworldline.com.

In order to properly install the DEP/PCI, the ATOS Worldline administrators have to read the documents on the site of the DEP products:

- http://www.banksys.com/

There are several documents as



DEP Documents

- 1-1 DEP Document Overview (new version)
- 1-2 DEP Introduction to DEP
- 1-3 DEP General Architecture
- 1-4 DEP Glossary
- 2-1 DEP Host Interface Protocol
- 2-2 DEP DS3 and DS4 Principles
- 2-3 DEP Secret Sharing Mechanism
- 2-4 DEP Security Mechanisms

- 3-1 DEP/NT Host Interface Supervision User Manual
- 3-2 DEP/NT DEP Handler Supervision User Manual
- 3-3 C-ZAM/DEP User Manual
- 3-4 DEP PC-AUX Program User Manual
- 3-5 DEP Key Derivation Tool User Manual
- 3-6 DEP RSA Key Gen&Use Program User Manual
- 3-7 DEP RSA Key Loading Program User Manual (new version)
- 3-8 DEP/Linux User Manual
- 3-8 DEP/T6 Owner Manual

- 3-8 DEP/NMS User Manual
- 3-8 DEP/EM User Manual
- 3-8 DEP/CTAP Certificate Generation User Manual
- 3-8 DEP/RSA Key Generation User Manual
- 3-8 DEP/RSA Key Import in Keytable Linux User Manual
- 3-8 DEP/NCR self-signed Certificate User Manual
- 3-8 STD Import Export Tool User Manual

- 4-1 DEP/NT Installation Guide
- 4-2 DEP Atos Worldline' Security Officer's Guide
- 4-3 DEP Customer's Security Officer's Guide
- 4-4 DEP Key Backup Conversion Guide
- 4-5 DEP Customer Host Programmers Guidelines
- 4-6 DEP Key Entry Guide
- 4-7 DEP QUICK load Guide
- 3-8 DEP/PCI Installation Guide
- 3-8 DEP Software Cloning Guide
- 4-10 DEP PKCS#11 User Guide

10. MANAGEMENT ISSUES

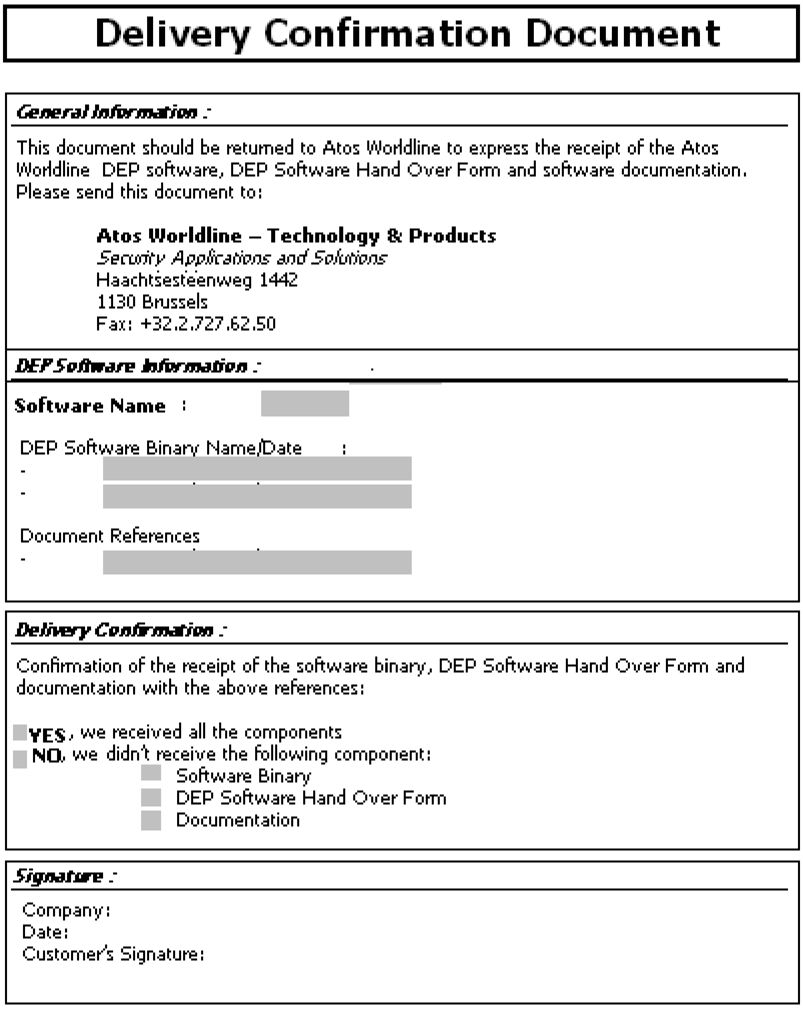
Because the DCC Personalisation contains a lot of sensitive and important information, the necessary precautions must be taken to avoid leakage loss of sensitive information.

Therefore it is important that the access to the DCC Personalisation System is limited and under control of the DEP AWL Security Officer.

Regular backup of the database are important to avoid loss of information.

11. ANNEXES

11.1. DELIVERY CONFIRMATION DOCUMENT



Delivery Confirmation Document

General Information :

This document should be returned to Atos Worldline to express the receipt of the Atos Worldline DEP software, DEP Software Hand Over Form and software documentation.
Please send this document to:

Atos Worldline – Technology & Products
Security Applications and Solutions
Haachtsesteenweg 1442
1130 Brussels
Fax: +32.2.727.62.50

DEP Software Information :

Software Name :

DEP Software Binary Name/Date :
-
-

Document References
-

Delivery Confirmation :

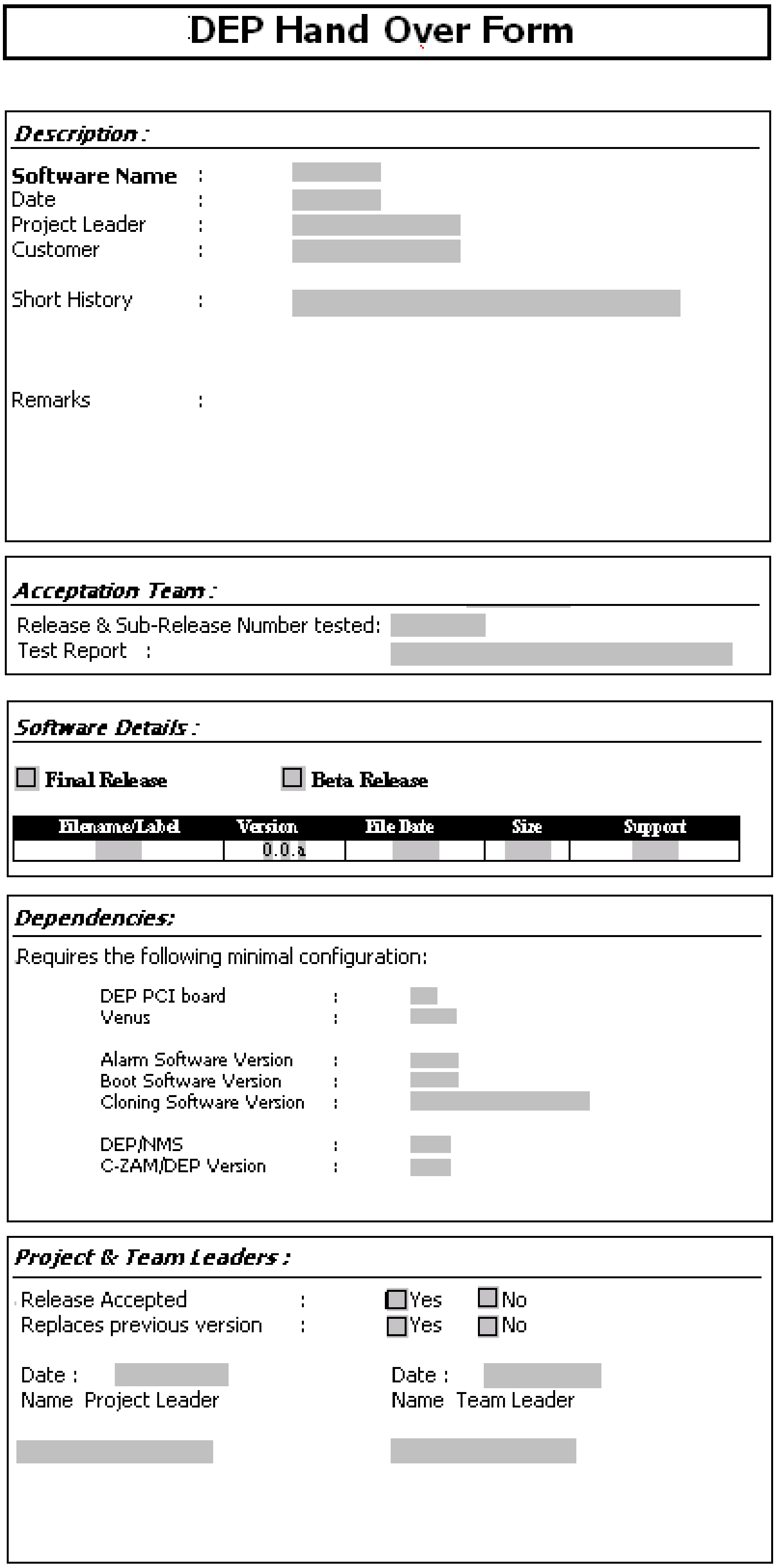
Confirmation of the receipt of the software binary, DEP Software Hand Over Form and documentation with the above references:

□ **YES**, we received all the components
□ **NO**, we didn't receive the following component:
□ Software Binary
□ DEP Software Hand Over Form
□ Documentation

Signature :

Company:
Date:
Customer's Signature:

11.2. DEP SOFTWARE HANDOVER FORM



DEP Hand Over Form

Description :

Software Name :
Date :
Project Leader :
Customer :

Short History :

Remarks :

Acceptation Team :

Release & Sub-Release Number tested:
Test Report :

Software Details :

□ **Final Release** □ **Beta Release**

Filename/Label	Version	File Date	Size	Support
	0.0.a			

Dependencies:

Requires the following minimal configuration:

DEP PCI board :
Venus :

Alarm Software Version :
Boot Software Version :
Cloning Software Version :

DEP/NMS :
C-ZAM/DEP Version :

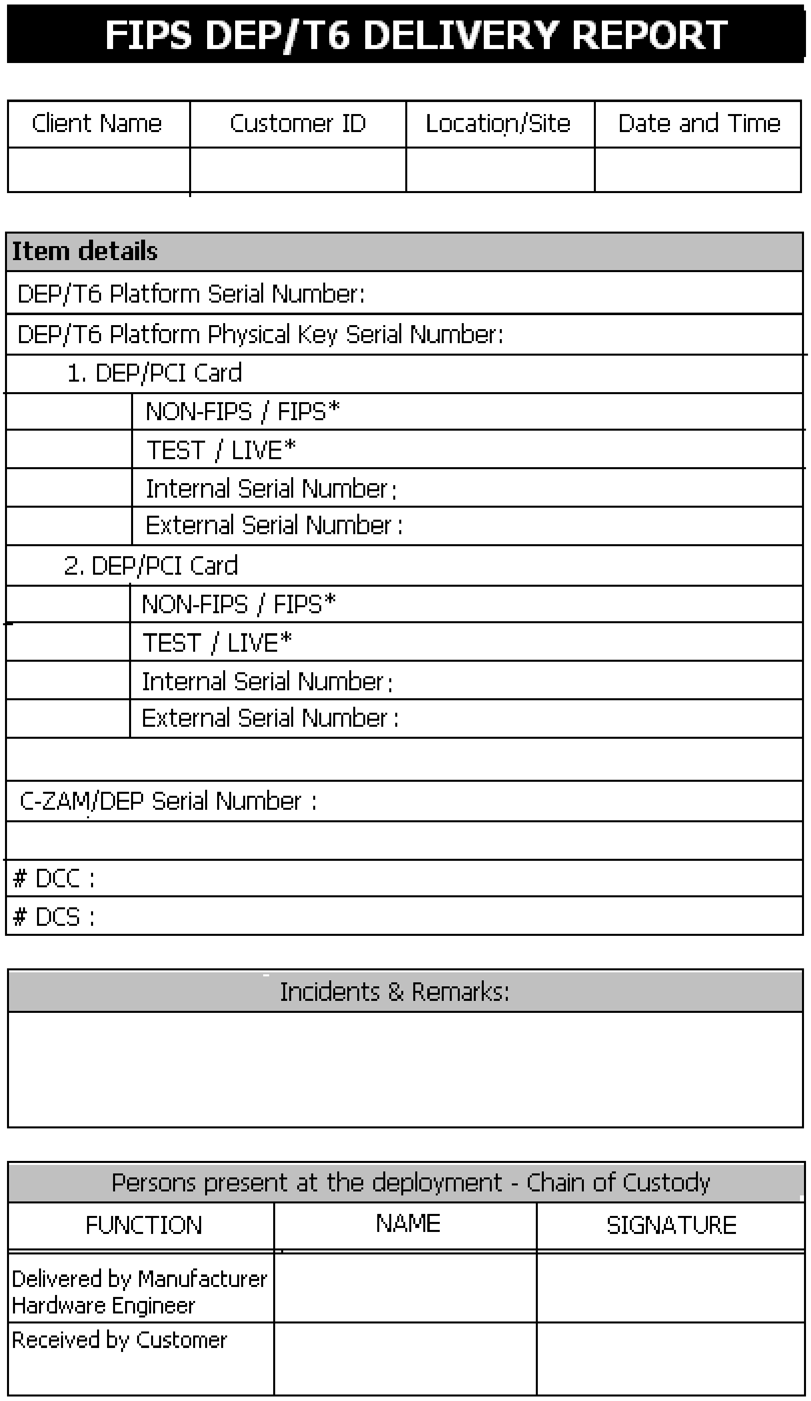
Project & Team Leaders :

Release Accepted : □ Yes □ No
Replaces previous version : □ Yes □ No

Date :
Name Project Leader

Date :
Name Team Leader

11.3. DEP Hardware Delivery Report



FIPS DEP/T6 DELIVERY REPORT

Client Name	Customer ID	Location/Site	Date and Time

Item details	
DEP/T6 Platform Serial Number:	
DEP/T6 Platform Physical Key Serial Number:	
1. DEP/PCI Card	
	NON-FIPS / FIPS*
	TEST / LIVE*
	Internal Serial Number:
	External Serial Number :
2. DEP/PCI Card	
	NON-FIPS / FIPS*
	TEST / LIVE*
	Internal Serial Number:
	External Serial Number :
C-ZAM/DEP Serial Number :	
# DCC :	
# DCS :	

Incidents & Remarks:

Persons present at the deployment - Chain of Custody		
FUNCTION	NAME	SIGNATURE
Delivered by Manufacturer Hardware Engineer		
Received by Customer		