TNO CERTIFICATION

Laan van Westenenk 501
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

Phone +31 55 5493468
Fax +31 55 5493288
E-mail: Certification@certi.tno.nl

BTW/VAT NR NL8003.32.167.B01
Bank ING at Delft
Bank account 66.77.18.141
stating 'TNO Certification'
BIC of the ING Bank: INGBNL2A
IBAN: NL81INGB0667718141

Date
April 5, 2006

Reference
NSCIB-CC-05-6609-CR

Subject

Project number
6609

NSCIB-CC-05-6609

Certification Report

Banksys DEP/PCI, version 3.1

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TNO Certification is an independent body with access to the expertise of the entire TNO-organization

TNO Certification is a registered company with the Delft Chamber of Commerce under number 27241271

TNO CERTIFICATION
HEREBY DECLARES THAT EVALUATION
HAS DEMONSTRATED THAT THE PRODUCT

Banksys DEP/PCI, version 3.1, Assurance Package: EAL3 augmented with ADV_FSP.2
Product and version

FROM

N.V. Banksys at Brussels, Belgium
Sponsor's name and address

COMPLIES WITH THE

Common Criteria for Information Technology Security Evaluation (CC), Version 2.2 (ISO/IEC 15408)

Certification guidelines or standards

AS DEMONSTRATED BY / EVALUATION PERFORMED BY

TNO-ITSEF at Delft, the Netherlands
Testing Laboratory

APPLYING THE

Common Methodology for Information Technology Security Evaluation (CEM), Version 2.2

NSCIB-CC-05-6609-CR
Certification Report number

THE CERTIFICATE HAS BEEN ISSUED ON

April 10th, 2006
Date

April 10th, 2016
Expiry Date

ISSUED AT: Apeldoorn, the Netherlands

DIRECTOR TNO CERTIFICATION

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 2.2 for conformance to the Common Criteria for IT Security Evaluation version 2.2. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TNO Certification or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TNO Certification or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Table of contents

Document Information

Date of issue	5 April 2006
Author	R.T.M. Huisman
Version of report	1
Certification ID	NSCIB-CC-05-6609
Sponsor and Developer	Banksys
Evaluation Lab	TNO-ITSEF BV
TOE name	Banksys DEP/PCI, version 3.1
TOE reference name	DEP/PCI
Report title	Certification Report
Report reference name	NSCIB-CC-05-6609-CR

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TNO Certification has the task of issuing certificates for IT security products.

A part of the procedure is the technical examination (evaluation) of the product according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TNO Certification in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF is a commercial facility that has been licensed by TNO Certification to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories.

By awarding a Common Criteria certificate, TNO Certification asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Banksys Data Encryption Peripheral PCI, version 3.1 (DEP/PCI). The developer of this product is Banksys located in Brussels, Belgium and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The Banksys DEP/PCI (the TOE) is a tamper-resistant and tamper-responsive host security module, which can be used with standard PC hardware that supports a PCI interface. The cryptographic services provided by the TOE are AES/DES/RSA, key generation and verification, hashing, and random number generation. These services are meant to be used in application domains like e-commerce, Electronic Purse, PKI, etc. The TOE is mainly used at the host side (e.g. it is plugged into a workstation that is connected to a mainframe or server located in a computer room, or it is plugged into a server located in a computer room). The TOE provides means to securely load an application and keys. Only authorised personnel can enable the loading of applications and/or keys. The Banksys DEP/PCI includes hardware and software components and communicates with its environment via a PCI-bus and serial ports. The Banksys DEP/PCI detects tamper attacks (e.g. physical intrusion, temperature and chemical attacks) and takes appropriate measures to log the event and to protect all sensitive data.

The Banksys DEP/PCI, version 3.1 has been evaluated by TNO ITSEF B.V. located in Delft, The Netherlands and was completed on 6 December 2005, The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*. The certification was completed on 5 April 2006 with the preparation of this Certification Report.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Banksys DEP/PCI version 3.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Banksys DEP/PCI version 3.1 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that it meets the EAL 3+ (Evaluation Assurance Level 3 augmented) assurance requirements for the evaluated security functionality. The assurance level is augmented with: ADV_FSP.2 Functional Specification - Fully defined external interfaces. Additionally the assurance component ATE_FUN.1 - Functional Testing was refined in the Security Target of the TOE (refer to [ST], chapter 5.2).The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 2.2 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 2.2 *[CC]*.

TNO Certification, as the NSCIB Certification Body, declares that the Banksys DEP/PCI version 3.1 evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The evaluation technical report is a NSCIB document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3+ evaluation is the DEP/PCI version 3.1, from Banksys located in Brussels, Belgium.

This report pertains to the TOE, which is comprised of the following main components:

Hardware	DEP/PCI version 3.1: PCI Card, Version 701.3 and Alarm Card, Version 702.5
Software	Alarm Processor Software version 2.2.c
	Boot Software version 1.1.c: Boot Command Handler, Boot Library CZAM, Boot Library STD, Boot ToolBox
	Application Software version 1.0.i: Command Handler, Library CZAM, Library STD, ToolBox
	Application Software version 1.0.i (extra library): EVAL Library[2]

To ensure a secure usage, a set of guidance documents is provided together with the Banksys DEP/PCI. Details can be found in section 2.5 of this report.

The TOE uses the following hardware: Standard PC hardware that supports a PCI interface.

Note: A smart card reader/encoder called C-ZAM/DEP together with the respective smart cards (called DCCs = DEP Control Cards) is used for administrative purposes. Details can be found in the Security Target *[ST]*, chapter 2.2.

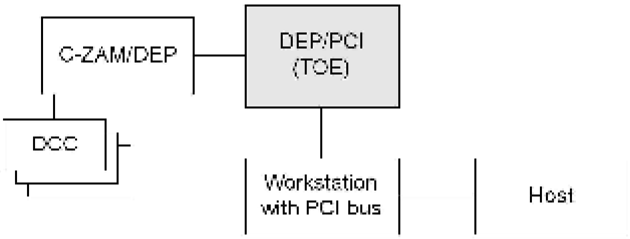

Figure 1, The TOE environment

2.2 Security Policy

The DEP/PCI is a generic platform providing cryptographic services, e.g. DES, Triple-DES (3DES), AES, RSA, CBC-MAC computation, hashing, digital signature computation, key generation, random generation. It is a tamper-resistant and tamper-responsive host security module, which can be used with standard PC hardware that supports a PCI interface and is meant to provide security services required by different application domains like EFT, Electronic Purse, e-commerce, PKI, etc.

[2] This part of the Application Software was created especially for the evaluation: it is designed to showcase all functionality of the TOE.

The main use of the DEP/PCI is at the host side (e.g. it is plugged into a workstation that is connected to a mainframe or server located in a computer room, or it is plugged into a server located in a computer room).

The DEP/PCI provides means to securely load an application and keys into it. Only authorised personnel (e.g. a security officer) can enable the loading of applications and/or keys.

The DEP/PCI detects tamper attacks (e.g. intrusion, temperature and chemical attacks) and takes appropriate measures to log the event and to protect all sensitive data.

The DEP/PCI delivers services to the environment depending on the software that is loaded. The evaluated DEP/PCI (the TOE) is a special implementation of the DEP/PCI, which delivers cryptographic services and protects the software and keys loaded against tampering. The cryptographic services that are implemented in the TOE are AES/DES/RSA, key generation and verification, hashing, and random number generation.

The confidentiality and integrity of all data in the TOE is protected:

- Physically, by tamper resistance and tamper responsive hardware,
- Logically, by only allowing well-defined interfaces and using access control (permissions to execute a specific task).

The TOE delivers cryptographic services as defined above. The generic DEP/PCI (not the TOE) is a device that delivers services according to customer specification. Banksys offers a variety of other libraries to customers. Examples of libraries are: PKI, EMV and customer specific libraries. However these libraries are not part of the evaluation.

2.3 Assumptions and Clarification of Scope

2.3.1 Usage assumptions

Based on the assumptions which are relevant for the TOE the following usage assumptions arise (for the detailed and precise definition of the assumptions refer to the *[ST]*, chapter 3.2):

- The TOE assumes to be administered in a secure manner by trustworthy personnel that is adequately trained, keeps their own confidential information, such as passwords, keys, or PINs secret. Administering the TOE is done with C-ZAM/DEP configured in the appropriate mode for authenticating the administrators.
- Whenever an operation is enabled, anyone with logical access to the TOE can perform that operation. The environment must therefore ensure that only authorised use is made of that operation. This means that the administrator should only enable some operations in an environment where unauthorised physical access and unauthorised logical access to the PCI-bridge are impossible.
- The Banksys administrator ensures that the Application Software loaded in the TOE:
  - is correct
  - has the right Capabilities LOADED/UNLOADED
  - and suitably protects access to all cryptographic keys before signing it.

2.3.2 Environmental assumptions

The following assumptions about the environmental aspects defined by the Security Target have to be met (for the detailed and precise definition of the assumptions refer to the *[ST]*, chapter 3.2):

- The TOE will be deployed in a server or workstation in a “server-room” environment that restricts physical access to only necessary personnel. The physical security of the room will be similar to a typical banking/financial institution computer server room. The environmental conditions will be similar to a typical computer server room.
- Any keys generated outside the TOE that are subsequently loaded in the TOE are generated in a confidential way, be unique with a very high probability and cryptographically strong.

2.3.3 Clarification of scope

The threats listed below are not (entirely) averted by the TOE. Additional support from the operating environment of the TOE is necessary (for detailed information about the threats and how the environment may cover them refer to the *[ST]*, especially chapter 3.3 and chapter 8.1).

- T.UNAUT_APPLICATION_LOAD
- T.UNAUT_KEY_LOAD
- T.UNAUT_KEY_BACKUP
- T.UNAUT_ERASE
- T.BAD_RANDOM
- T.EAVESDROP

2.4 Architectural Information

Physically the TOE consists of a PCI card with a main processor and an alarm processor. Wired paper, epoxy potting and a steel enclosure shield both processors:

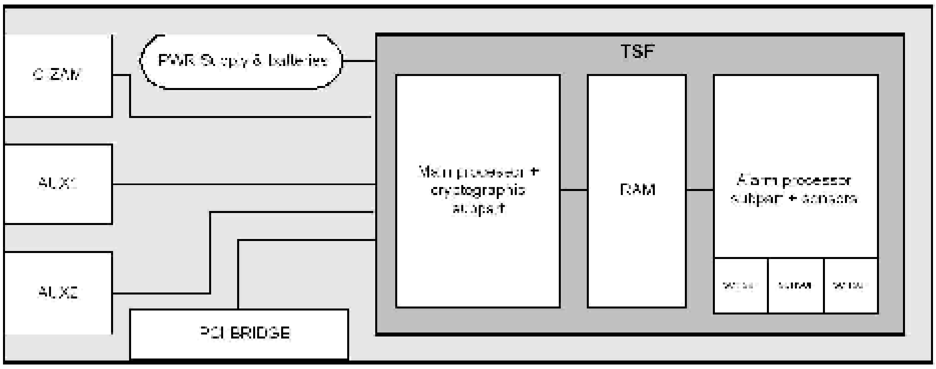
C-ZAM
PWR Supply & batteries
TSF
AUX1
Main processor + cryptographic subpart
RAM
Alarm processor subpart + sensors
AUX2
sensor
sensor
sensor
PCI BRIDGE

Figure 2, The TOE Hardware

Two main parts of the TOE can be distinguished:

- a secured module (the TSF), containing mainly:
  - the main processor and cryptographic co-processors,
  - an alarm processor,
  - RAM that can be accessed by both processors,
  - alarm sensors.
- the PCI module, containing mainly:
  - power supply and batteries

- the PCI bridge,
- serial line ‘C-ZAM’: to connect a C-ZAM/DEP (an external chip card encoder/reader that is used for administrative purposes),
- serial line ‘AUX1’: is not used,

The logical boundaries of the TOE are shown in Figure 3:

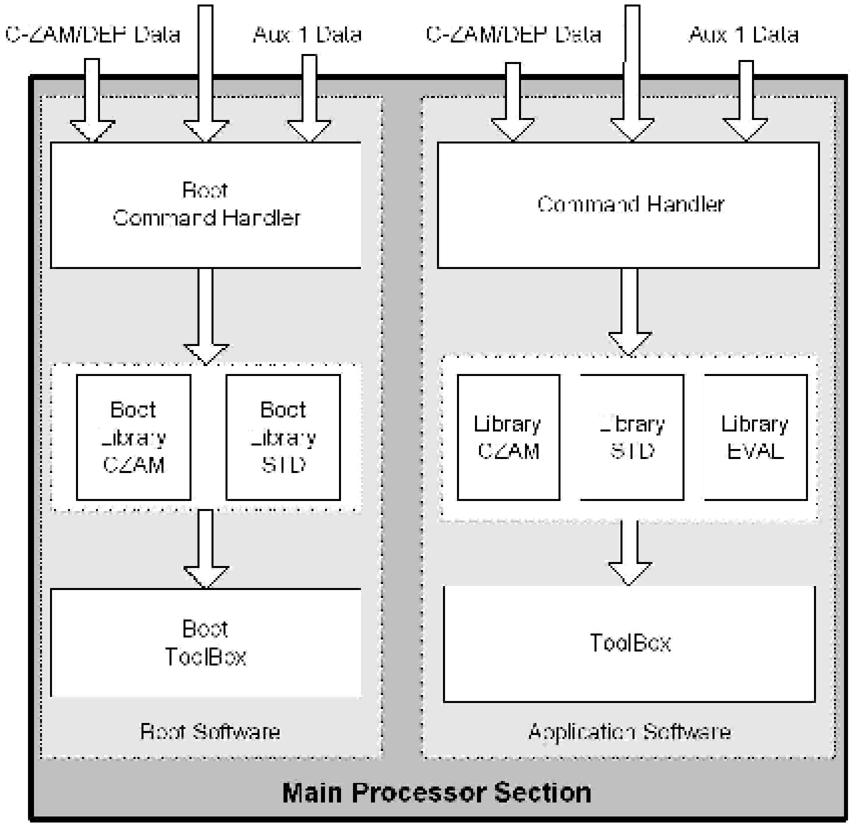

Figure 3, The TOE Software

The DEP/PCI contains three major software parts:

- the Boot Software (in EEPROM). This part executes while 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;
- the Application Software (in RAM). This part executes when it is loaded, and provides the operational cryptographic services of the TOE;
- the Alarm Processor Software (in EEPROM). This part executes concurrently with the other two, and continuously monitors the various sensors of the TOE for alarms. If an alarm is triggered, it removes the Application Software, and transfers back control to the Boot Software, effectively resetting the TOE completely.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Administrator guidance	Ø DEP/NT Documentation – DEP/NT Installation Guide version 02.01 Ø DEP/PCI – Customer Security Officer: Guidelines version 1.0 (10) Ø DEP/PCI – Customer Host Programmers Guidelines version 1.0 (1) Ø DEP/NT Documentation – DEP/NT C-ZAM/DEP User Manual version 02.03 Ø DEP/NT Documentation – DEP/NT PC-AUX Program User Manual version 02.01 Ø DEP/NT Documentation – DEP/NT Host Interface Supervision User Manual version 02.01 Ø DEP/NT Documentation – DEP/NT DEP Handler Supervision User Manual version 02.03
Evaluated version specific user guidance	Ø Common Criteria Software – Integration Manual version 1.0 (10) Ø Subset of Eval Library for DEP – Reference DFS Manual version 3.0 (13) Ø DEP/PCI – Security Target version 1.1 (6) Ø DEP/PCI – Guidance Documentation – Erratum version 1.0 (1)
General user guidance	Ø Subset STD Library for DEP – Ref DFS Manual version 3.5 (8)

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer’s testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach

The developer has highly automated the software testing. The evaluators repeated all software testing using the test tools, as they were made available by the developer.

Restrictions: the TOE was tested in TST mode only. The other modes of the TOE are DEV (for the developer) and LIV (in which the TOE operates).

The operational mode LIV does not permit testing of the interfaces. The difference between the LIV mode and TST mode is only the set of keys that is used, so all testing in TST mode is extendable to LIV mode.

2.6.2 Test Configuration

The test configuration was a rack-mountable PC running the Windows NT 4.0 Workstation SP4 operating system. The TOE was mounted in the PCI interface of the PC. On the PC, the following additional applications were installed:

- Ø TheSteamFactory Script Writer
- Ø TheSteamFactory Scenario Player
- Ø Banksys DEP/PCI Supervision Handler

The test configuration for independent testing is the same as used for the Developer Vulnerability Analysis.

2.6.3 Depth

Testing corresponded with the depth of the high-level design. The developer has done substantial functional testing of all externally visible interfaces, including tests that check out-of-range values. The functional testing was automated to an extent that allowed the evaluators to repeat all tests but two.

As the (extensive) sample taken did not lead to questions or doubts about the tests the evaluators deemed it unnecessary to repeat these two tests.

The tests that were not reproduced by the evaluators are those that were not possible due to constraints of the test environment. Two tests require the TOE to be disconnected from the power. However, this requires a test environment where the test program runs on a separate machine that is not powered off. This was not the case, and therefore the tests that required power switch-off were not reproduced.

2.6.4 Independent Penetration Testing

Based on the examination of the developer's vulnerability analysis and test activities, and also on the evaluators own vulnerability analysis, a number of possible vulnerabilities were revealed.

Penetration tests have been performed by the evaluation lab to assess those identified possible vulnerabilities.

2.6.5 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with a references to the documents containing the full details.

The developer’s tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its ST and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The evaluated configuration of the TOE consists of:

- A standard PC hardware platform that supports a PCI interface.
- A smart card reader/encoder called C-ZAM/DEP together with the respective smart cards (called DCCs = DEP Control Cards) which is needed for administrative purposes.

According to the *[ST]*, chapter 2.5.2, the TOE supports three different modes of operation: DEV, TST and LIV. It is claimed in the ST that the functionality the TOE provides in each mode is exactly the same. The differences between the modes are the initial secrets which were chosen in each mode.

The TOE that was evaluated is the DEP/PCI using the application EVAL, that was developed as dedicated software for the evaluation. The evaluated mode is the TST mode; the other modes were not evaluated.

For setting up / configuring the TOE all guidance documents was followed (refer to section 2.5 of this report).

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[3] which references several Intermediate Reports. The verdict of each Intermediate Report is given in the following table:

Intermediate Report	Verdict
Security Target	PASS
Configuration Management	PASS
Delivery and Operation	PASS
Functional Specification	PASS
High-level Design	PASS
Representation Correspondence	PASS
Guidance Documentation	PASS
Life Cycle Support	PASS
Test	PASS
Vulnerability Assessment	PASS

Based on the above evaluation results the evaluation lab concluded the Banksys DEP/PCI version 3.1 to be **CC Part 2 extended**, **CC Part 3 conformant**, and to meet the requirements of **EAL 3 augmented by ADV_FSP.2**. This implies that the product satisfies the security technical requirements specified in DEP/PCI Security Target version 1.1 (6), Document date: 14 July 2005.

Note that no strength of function claim has been made in the Security Target. Hence the requirements of AVA_SOF.1 were implicitly fulfilled

2.9 Evaluator Comments/Recommendations

The development documentation consists of an introduction and the in-depth documentation. The introductions provide easy access to the principles as laid out in the in-depth documentation.

In addition, some more documentation was provided which is not to be regarded as evidence. This information is available to the user and provides useful insights that help understanding the TOE.

[3] The evaluation technical report is a NSCIB document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

3 Security Target

The ST, DEP/PCI Security Target version 1.1 (6), Document date: 14 July 2005 is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
CC	Common Criteria
DCC	DEP Control Card
DEP/PCI	Data Encryption Peripheral PCI
DES	Data Encryption Standard
ITSEF	IT Security Evaluation Facility
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
PP	Protection Profile
TNO	Netherlands Organization for Applied Scientific Research
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, version 2.2.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, January 2004, Version 2.2, Revision 256, CCIMB-2004-01-004.

[ETR] Evaluation Technical Report, Banksys DEP/PCI version 3.1 (ETR-DEP/PCI-EAL(3+)-1), Version 1, 6 December 2005.

[NSCIB] Nederlands schema voor certificatie op het gebied van IT-beveiliging, Versie 1.2, 22 maart 2004.

[ST] DEP/PCI Security Target version 1.1 (6), Document date: 14 July 2005.

[TOE] Banksys DEP/PCI version 3.1.