Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0198-2003

for

Banksys DEP/PCI Version 3.0

from

Banksys N.V.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0198-2003

Banksys DEP/PCI Version 3.0

from

Banksys N.V.

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and approved/licensed evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6*, *Part 2 Version 1.0* for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL3 augmented by** ADV_FSP.2 (Functional Specification - Fully defined external interfaces)

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 certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 08. August 2003

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS-MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 9582-111

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.
Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the Certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

---

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium des Innern of 22nd September 2000 in the Bundesanzeiger p. 19445

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates based on the CC was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Banksys DEP/PCI Version 3.0 has undergone the certification procedure at BSI.

The evaluation of the product Banksys DEP/PCI Version 3.0 was conducted by TNO ITSEF BV which is an evaluation facility recognised by BSI (ITSEF)[6].

The sponsor and developer is:

Banksys N.V.
Haachtsesteenweg 14
1130 Brussels
Belgium.

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 8th August 2003.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-34.

The product Banksys DEP/PCI Version 3.0 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline 0228/9582-111.

Further copies of this Certification Report can be requested from the sponsor of the product. The Certification Report can also be downloaded from the above-mentioned website.

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

The Target of Evaluation (TOE) is Banksys DEP/PCI Version 3.0 (also named Banksys DEP/PCI in short). It 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. This 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 following list summarises the TOE components and defines the evaluated configuration of the TOE:

Hardware	DEP/PCI, Version 3.0: PCI Card, Version 701.2 and Alarm Card, Version 702.2
Software	Alarm Processor Software, Version 2.0.b
	Boot Software, Version 1.0.d: 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: EVAL Library

To ensure a secure usage, a set of guidance documents is provided together with the Banksys DEP/PCI. Details can be found in chapter 6 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 [6], chapter 2.2.

The TOE Security Functional Requirements (SFR) used in the Security Target are Common Criteria Part 2 extended as shown in the following table:

Security Functional Requirement	Functionality
Cryptographic Services	
FCS_CKM.1+1[7]	AES Key Generation
FCS_COP.1+1	AES encryption and decryption
FCS_COP.1+2	AES CBC-MAC generation
FCS_CKM.1+2	DES/3DES Key Generation
FCS_COP.1+3	DES/3DES encryption and decryption
FCS_COP.1+4	DES/3DES CBC-MAC generation
FCS_CKM.1+3	RSA Key Generation
FCS_COP.1+5	RSA encryption and decryption
FCS_COP.1+6	RSA signature generation and verification
FCS_COP.1+7	SHA-1, SHA-256 and MD5 hash generation
FCS_RND.1	Random Number Generation Note: This requirement is not part of the CC, Part 2.
Loading Applications	
FDP_ACC.1+1	Naming the Security Policy for the loading of an application
FDP_ACF.1+1	Definition of the Security Policy Rules
FDP_ITC.2	Loading of Software
FDP_DAU.2	Only Software from a trusted developer can be loaded
Loading, back-up, and deleting Application Keys	
FDP_ACC.1+2	Naming the Security Policy for the loading/backup/restore/erasing of application keys
FDP_ACF.1+2	Definition of the Security Policy Rules
FDP_ITC.1	Loading of application keys
FTP_ITC.1	Trusted channel between TOE and environment.

[7] Notation of SFR component iteration: FXX_XXX.y+n means nth iteration of the SFR FXX_XXX.y

Security Functional Requirement	Functionality
Management of the TOE	
FMT_SMR.1	Definition of administrative roles
FIA_UID.2	Identification of roles
FIA_UAU.2	Authentication of roles
FMT_MSA.1	Enable/disable operations by a certain role
FMT_SAE.1	Limit operations in time by a certain role
FMT_SAE.2	Limit number of times for an operation by a certain role Note: This requirement is not part of the CC, Part 2.
FDP_ACC.1+3	Naming the Security Policy for the access to operations
FDP_ACF.1+3	Definition of the Security Policy Rules
FMT_MSA.3	Default access to operations
FMT_SMF.1	Management operations of the TOE
FMT_MOF.1	Assignment of management operations to roles
Tampering and abnormal operating conditions	
FPT_PHP.3	Resistance to physical attacks
FAU_GEN.1	Logging of tamper events
FPT_STM.1	Generation of timestamp for logging
FAU_SAA.1	Detecting when a tamper event has taken place
FAU_ARP.1	Reacting on a detected tamper event (clearing the DEP/PCI)
FDP_RIP.1	Ensuring that when the DEP is cleared, the data cannot be retrieved
Architectural Security	
FPT_SEP.1	Resistance to logical attacks
FPT_RVM.1	Ensuring that the TSF cannot be bypassed

The TOE Banksys DEP/PCI was evaluated by:

TNO ITSEF BV
Oude Waalsdorperweg 63
PO Box 96864
2509 JG The Hague
The Netherlands.

The evaluation was completed on 17th June 2003. The TNO ITSEF BV is an evaluation facility recognised by BSI (ITSEF)[8].

The sponsor and developer is:

Banksys N.V.
Haachtsesteenweg 14
1130 Brussels
Belgium

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C of this report, or [1], part 3 for details).

The TOE meets the assurance requirements of assurance level EAL3+ (Evaluation Assurance Level 3 augmented). The assurance level is augmented by: ADV_FSP.2 – Fully defined external interfaces. Additionally the assurance component ATE_FUN.1 - Functional Testing was refined in the Security Target of the TOE (refer to [6], chapter 5.2).

1.2 Functionality

The TOE Banksys DEP/PCI provides the following Security Functions:

Name	Function
Cryptographic Security Functions	
KEY_1	AES cryptographic key generation service
CRYPT_1	AES encryption/decryption service
CRYPT_2	AES CBC-MAC generation service
KEY_2	DES/3DES cryptographic key generation service
CRYPT_3	DES/3DES encryption/decryption service
CRYPT_4	DES/3DES CBC-MAC generation service
KEY_3	RSA cryptographic key generation service
CRYPT_5	RSA encryption/decryption service
CRYPT_6	RSA signature creation/verification service
CRYPT_7	SHA-1, SHA-256 and MD5 hash generation service
RND_1	Random number generation service

[8] Information Technology Security Evaluation Facility

Name	Function
Loading and Saving Security Functions	
LOAD_1	Loading of signed applications via the PCI interface
LOAD_2	Loading of application keys via a trusted channel
BACKUP_1	Backup of application keys via the PCI interface
BACKUP_2	Restore applications keys previously backed-up
ERASE_1	Deletion of application software and all keys maintaining the authority level of the TOE
ERASE_2	Deletion of application keys maintaining the authority level of the TOE
Security Functions for the Management of the TOE	
CZAM_1	Trusted channel between TOE and smart card reader C-ZAM/DEP for identification and authentication of administrative roles.
MODE_1	Deletion of all application software and keys if TOE is brought to NONE level
MODE_2	Assignment of TOE to specific customer and setting of TOE mode
MODE_3	Entering authority level INIT
MODE_4	Entering authority level BKS by a certain role by using the trusted channel
MODE_5	Entering authority level CUST by a certain role by using the trusted channel
MANAGE_1	Enable/disable/limit (time/number of execution) of individual security functions.
MANAGE_2	Disable certain security functions by default
Tampering / Abnormal conditions Security Functions	
ALARM_1	The TOE is able to detect tamper events (physical penetration, chemical penetration, removal of the cover, unusual temperatures, unusual voltage, removal of the TOE from its PCI slot, unusual physical acceleration of the TOE)
LOG_1	Tamper events (refer to ALARM_1) are logged by the TOE
REACT_1	The TOE moves back to NONE state upon detection of a tamper event
PROT_1	The TOE is enclosed in a hard casing which is hard to penetrate (tamper resistant)

Name	Function
Architectural Security Functions	
ARCH_1	The internal code and data of the TOE cannot be modified
ARCH_2	Protection of application software and keys against modification
ARCH_3	Protection of application keys against disclosure
ARCH_4	No ability to bypass the security functions

Note: Only the titles of the SF and a short summary are provided here because they are very granular and almost self-explanatory. Please refer for a precise definition of the SF to the Security Target of the TOE ([6], chapter 6.1)

1.3 Strength of Function

No strength of function was claimed for the TOE.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

A summary of the threats defined in [6], chapter 3.3 is provided here. For the precise description of the threats and any subject, object and operation used in that description please refer to [6]:

T.UNAUT_APPLICATION_LOAD
An attacker tries to load/replace Application Software.

T.UNAUT_KEY_LOAD
An attacker tries to load/replace Application Keys.

T.UNAUT_KEY_BACKUP
An attacker tries to backup/restore Application Keys.

T.UNAUT_BACKUP_DISCLOSURE
An attacker tries to get notice of backed-up Application Keys.

T.UNAUT_ERASE
An attacker tries to delete Application Software and/or Application Keys without resetting the TOE

T.PHYSICAL_TAMPER
An attacker tries to modify the TOE or the Application Software to read out Application Keys by physically tampering with the TOE.

T.LOGICAL_TAMPER
An attacker tries to modify the TOE or the Application Software to read out Application Keys by logically tampering with the TOE.

T.BAD_RANDOM

An attacker tries to predict information on random numbers and/or keys generated by the TOE (based on a poor random number generator).

T.IMPERSONATE

An attacker tries to impersonate as a certain administrative role. A certain administrative role tries to impersonate as another administrative role.

Note that not all threats are entirely averted by the TOE. Instead, additional support from the TOE's environment is needed. For information which parts are averted by the TOE and which by the environment of the TOE, please refer to [6], chapter 8.1 (Security Objective Rationale) and to chapter 4.3.

The TOE has to comply to the following Organisational Security Policies (OSPs). Note that only a summary of the policies is provided in this report. For the detailed and precise definition refer to [6], chapter 3.4:

P.SERVICES_EVAL

The subject S.HOST_APPL (Application Software residing on a host) can obtain the following services from the TOE:

- AES key generation, encryption, decryption and CBC-MAC generation
- DES/3DES key generation, encryption, decryption and CBC-MAC generation
- RSA key generation, encryption, decryption, signature creation, signature verification
- SHA-1, SHA-256 and MD5 hashing
- Random number generation

Keys can either be loaded into the TOE or generated by the TOE.

P.AUTHORITY_LEVELS

The TOE is always in exactly one of the following Authority Levels: NONE (non authority state), INIT (initialised state), BKS (personalised state) or CUST (operational state). For a detailed description of the Authority Levels refer to [6] chapter 2.5.

P.AUTHORITY_LEVEL_CHANGE

The following rules shall be enforced:

- Anyone with physical access to the TOE can move the TOE to authority level NONE (Note that the TOE is reset and sensitive data is erased).
- Anyone with logical access to the TOE can move the TOE from authority level NONE to INIT.

- Only the subject S.INIT_ADM can move the TOE from INIT to BKS authority level.
- Only the subject S.BKS_ADM can move the TOE from BKS to CUST authority level.

P.ADMIN

Once in CUST authority level the TOE can be managed as follows:

- Application Software (D.DEP_APPL) can be loaded into the TOE.
- Application Keys (D.APPL_KEYS) can be loaded by a certain administrator using a C-ZAM/DEP.
- Application Keys can be backed-up.
- Backed-up Application Keys can be restored.
- Application Keys and Application Software can be deleted without resetting the TOE.

1.5 Special configuration requirements

According to the Security Target ([6], 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 difference 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.

1.6 Assumptions about the operating environment

The TOE uses standard PC hardware 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) is needed for administrative purposes. Details can be found in the Security Target [6], chapter 2.2.

The following constraints concerning the operating environment are made in the Security Target.

The following constraints are based on the assumptions defined in [6], chapter 3.2. (Please refer to the Security Target for the precise definition):

A.ADMIN

Only trustworthy personnel administers the TOE. The personnel is adequately trained and keeps their confidential information (like PINs and passwords) secret.

A.ENABLE_PROTECT

Whenever an operation of the TOE is enabled, anyone with logical access to the TOE may use this operation. Therefore the environment has to ensure that only authorised use is made of that operation.

A.SIGN_SOFTWARE

The Administrator ensures that Application Software (i) is correct, (ii) has the right capabilities and (iii) suitably protects access to all cryptographic keys before the Application Software is signed.

A.SECURE_ROOM

The TOE is used in a “Server-Room” environment restricting physical access only to necessary personnel.

A.KEY_GEN

Any keys generated outside the TOE are generated in a confidential way, are unique with a high probability and cryptographically strong.

The following constraints are based on Security Objectives which have to be met by the TOE environment. Theses objectives are defined in [6], chapter 4.2. (Please refer to the Security Target for the precise definition):

OE.RANDOM_TEST

The quality of the random number generator of the TOE shall be tested by means implemented in the TOE environment

OE.TRAFFIC

The IT environment shall protect sensitive data in transit between the TOE and the Host Application using the TOE.

1.7 Disclaimers

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation is called:

Banksys DEP/PCI Version 3.0

The following list summarises the TOE components and defines the evaluated configuration of the TOE:

Hardware	DEP/PCI, Version 3.0: PCI Card, Version 701.2 and Alarm Card, Version 702.2
Software	Alarm Processor Software, Version 2.0.b
	Boot Software, Version 1.0.d: 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: EVAL Library

The following guidance documents are supplied together with the TOE. The Guidance have to be followed to ensure an evaluation conformant operation of the TOE.

Administrator Guidance	- DEP/NT Documentation – DEP/NT Installation Guide version 02.01 - DEP/PCI – Customer Security Officer: Guidelines version 1.0 (10) - DEP/PCI – Customer Host Programmers Guidelines version 1.0 (1) - DEP/NT Documentation – DEP/NT C-ZAM/DEP User Manual version 02.03 - DEP/NT Documentation – DEP/NT PC-AUX Program User Manual version 02.01 - DEP/NT Documentation – DEP/NT Host Interface Supervision User Manual version 02.01 - DEP/NT Documentation – DEP/NT DEP Handler Supervision User Manual version 02.03

Evaluated version specific user guidance	- Common Criteria Software – Integration Manual version 1.0 (10) - Subset of Eval Library for DEP – Reference DFS Manual version 2.0 (12) - DEP/PCI – Security Target version 1.1 (4) - DEP/PCI – Guidance Documentation – Erratum version 1.0 (1)
General user guidance	- Subset STD Library for DEP – Ref DFS Manual version 3.5 (8)

3 Security Policy

The TOE is a tamper-resistant and tamper-responsive host security module. Its main purpose is to provide cryptographic services and means to securely load an application and keys into it. Only authorised personnel can enable the loading of applications and/or keys.

Therefore the Security Policy of the TOE is defined by the following TOE security functional requirements:

- FDP_ACC.1+1 and FDP_ACF.1+1 defining the DEP Application Policy, a Security Policy for loading applications into the TOE.
- FDP_ACC.1+2 and FDP_ACF.1+2 defining the DEP Application Key Policy, a Security Policy for loading/backup/restore/erasing application keys into the TOE.
- FDP_ACC.1+3 and FDP_ACF.1+3 defining the DEP Executing Policy, a Security Policy that controls access to operations of the TOE.

A detailed description/definition of the Security Policy enforced by the TOE is given in the Security Target [6], chapter 5.1.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on the Organisational Security Policies to which the TOE complies the following usage assumptions arise (for the detailed and precise definition refer to [6], chapter 3.4):

- The subject S.HOST_APPL (Application Software residing on a host) can obtain the following services from the TOE:
  - AES key generation, encryption, decryption and CBC-MAC generation
  - DES/3DES key generation, encryption, decryption and CBC-MAC generation
  - RSA key generation, encryption, decryption, signature creation, signature verification
  - SHA-1, SHA-256 and MD5 hashing
  - Random number generation

  Keys can either be loaded into the TOE or generated by the TOE.
- The TOE is always in exactly one of the following Authority Levels: NONE (non authority state), INIT (initialised state), BKS (personalised state) or CUST (operational state). For a detailed description of the Authority Levels refer to [6] chapter 2.5.
- The following rules shall be enforced:
  - Anyone with physical access to the TOE can move the TOE to authority level NONE (Note that the TOE is reset and sensitive data is erased).
  - Anyone with logical access to the TOE can move the TOE from authority level NONE to INIT.
  - Only the subject S.INIT_ADM can move the TOE from INIT to BKS authority level.
  - Only the subject S.BKS_ADM can move the TOE from BKS to CUST authority level.
- Once in CUST authority level the TOE can be managed as follows:
  - Application Software (D.DEP_APPL) can be loaded into the TOE.
  - Application Keys (D.APPL_KEYS) can be loaded by a certain administrator using a C-ZAM/DEP.
  - Application Keys can be backed-up.

- Backed-up Application Keys can be restored.
- Application Keys and Application Software can be deleted without resetting the TOE.

Based on personnel assumptions the following usage conditions exist:

- Only trustworthy personnel administers the TOE. The personnel is adequately trained and keeps their confidential information (like PINs and passwords) secret.
- Whenever an operation of the TOE is enabled, anyone with logical access to the TOE may use this operation. Therefore the environment has to ensure that only authorised used is made of that operation.
- The Administrator ensures that Application Software (i) is correct, (ii) has the right capabilities and (iii) suitably protects access to all cryptographic keys before the Application Software is signed.
- Any keys generated outside the TOE are generated in a confidential way, are unique with a high probability and cryptographically strong.
- The quality of the random number generator of the TOE shall be tested by means implemented in the TOE environment

For a detailed description of the usage assumptions refer to the Security Target [6], especially chapter 3.2 and 4.2

4.2 Environmental assumptions

The following assumptions about physical and connectivity aspects defined by the Security Target have to be met (refer to Security Target [6], chapter 3.2 and 4.2):

- The TOE is used in a “Server-Room” environment restricting physical access only to necessary personnel.
- The IT environment shall protect sensitive data in transit between the TOE and the Host Application using the TOE.

Please consider also the requirements for the evaluated configuration specified in chapter 8 of this report.

4.3 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 Security Target [6], 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

5 Architectural Information

TOE definition

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.

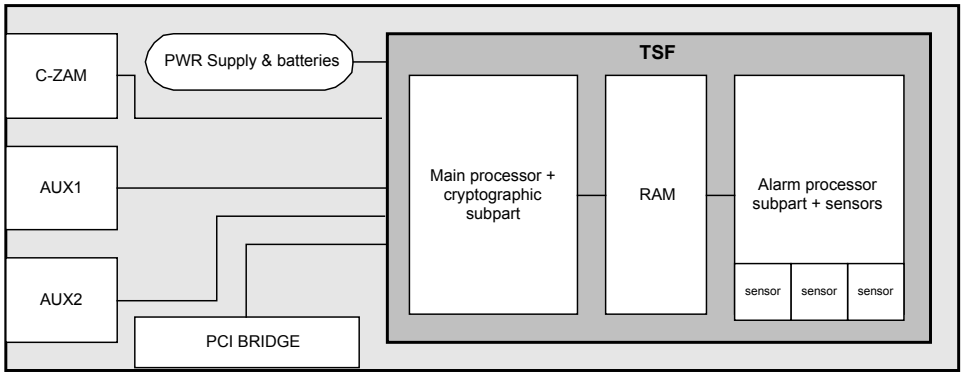

Figure 1: TOE-Hardware.

TOE functionality

The DEP/PCI delivers services to the environment depending on the software that is loaded. 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 delivered are AES/DES/RSA key generation and verification, hashing, and random number generation.

The confidentiality and integrity of all data in the DEP/PCI 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).

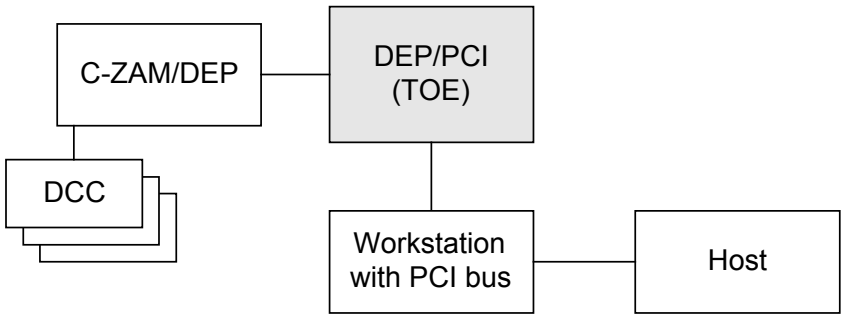

Figure 2: The TOE in its environment.

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 [6], chapter 2.2.

Components of the TOE

The TOE is Banksys DEP/PCI version 3.0, with:

- PCI card 701.2
- Alarm card 702.2
- Boot Software 1.0.d
- Alarm software 2.0.b

The software components are compiled in the file:

- Application Software 'Common Criteria' version 1.0.i

Additionally, the final documentation that was delivered as evaluation evidence (please refer to chapter 2 of this report for more detail).

External interfaces of the TOE

The TOE has four hardware interfaces:

PCI-bridge interface
This is used for communication (through the Command Handler) with the Boot Library STD, the Library STD and the Library EVAL.

CZAM/DEP interface
This is used for communication (through the Command Handler) with the CZAM Boot Library and the CZAM library.

AUX 1 is not used**.**
The Library EVAL does not use the AUX1 interface.

AUX 2 is used for:
- Authentication of the DEP/PCI Alarm Processor Section hardware,
- Reading of alarm status and alarm logging,
- Alarm processor administration purposes.

Additionally, the TOE has a number of sensors that trigger an alarm. These sensors are: light sensor, temperature sensor, motion sensor, voltage sensor, and additionally copper & silver wiring against physical and chemical penetration.

Finally, the enclosure of the logic parts in epoxy potting and a steel enclosure are security functions of the TOE.

Software components

The software components available are:

- (Boot) C-ZAM/DEP Library (also known as CZD or DS3)
- (Boot) STanDard Library (also known as STD)
- Application Library EVAL
- (Boot) Command Handler
- Alarm Software

Some components are available during boot of the TOE and during operation. The application library EVAL is only available once the TOE is in operation (Authority Level CUST, TST mode, Application loaded).

6 Documentation

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

[8] DEP/NT Documentation – DEP/NT Installation Guide, banksys, Version 02.01

[9] DEP/PCI – Customer Security Officer: Guidelines, banksys, Version 1.0 (10)

[10] DEP/PCI – Customer Host Programmers Guidelines, banksys, Version 1.0 (1)

[11] DEP/NT Documentation – DEP/NT C-ZAM/DEP User Manual, banksys, Version 02.03

[12] DEP/NT Documentation – DEP/NT PC-AUX Program User Manual, banksys, Version 02.01

[13] DEP/NT Documentation – DEP/NT Host Interface Supervision User Manual, banksys, Version 02.01

[14] DEP/NT Documentation – DEP/NT DEP Handler Supervision User Manual, banksys, Version 02.03

[15] Common Criteria Software – Integration Manual, banksys, Version 1.0 (10)

[16] Subset of Eval Library for DEP – Reference DFS Manual, banksys, Version 2.0 (12)

[17] DEP/PCI – Security Target, banksys, Version 1.1 (4)

[18] DEP/PCI – Guidance Documentation – Erratum, banksys, Version 1.0 (1)

[19] Subset STD Library for DEP – Ref DFS Manual, banksys, Version 3.5 (8)

7 IT Product Testing

Test Schedule

Testing took place during 21 October 2002 and 28 February 2003.

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. A dedicated Test Suite was installed on the PC to enable the automated test scripts to be run.

For the independent evaluator testing as well as for the penetration testing the same test configuration was used by evaluation lab.

Note: The TOE was tested in TST mode, the modes DEV (developer mode) and LIV (operational mode) were not tested. The only difference between DEV, LIV and TST mode is the (initial) set of keys that is used. Please refer to chapter 1.5 for more details.

Depth/Coverage of Testing

The developer has done substantial functional testing of all externally visible interfaces, including tests that check out-of-range values. The evaluators repeated most of the developer tests (because of the highly automated testing approach of the developer) and conducted additional independent tests and penetrations tests.

Summary of Developer Testing Effort

Test configuration:

All the tests have been performed on the configuration defined above.

Testing approach:

The developer has highly automated the software testing by using scripts which can be run in a dedicated test suite. These automatic test were supplemented by manual tests for the TOE hardware and the random number generator.

Testing results:

The results of the tests are that all test cases show the expected behaviour in the evaluated configuration.

Summary of Evaluator Testing Effort

Test configuration

All the tests have been performed on the configuration defined above.

Testing approach:

Since the developer has automated his tests to a great extent, the evaluation lab repeated almost all tests. These developer tests have been supplemented by test cases generated by the evaluation lab (including supplementary test for the random number generator and the key generation).

Evaluator penetration testing:

Penetration tests have been performed by the evaluation lab to assess possible vulnerabilities found during the evaluation of the different CC assurance classes. Furthermore some penetration tests have been carried out to verify some of the claims the developer made in its vulnerability assessment.

8 Evaluated Configuration

According to the Security Target the evaluated configuration of the TOE (as specified in chapter 2 of this report) is defined as follows (refer to Security Target [6]):

- The TOE uses standard PC hardware 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) is needed for administrative purposes.

According to the Security Target ([6], 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 difference 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.

The TOE is used in a “Server-Room” environment restricting physical access only to necessary personnel.

The IT environment shall protect sensitive data in transit between the TOE and the Host Application using the TOE.

For setting up / configuring the TOE all guidance documents have to be followed (refer to chapter 6 of this report).

9 Results of the Evaluation

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Common Evaluation Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL3 augmented by ADV_FSP.2, the refined ATE_FUN.1 component and the Security Target evaluation) are summarised in the following table:

Assurance Classes and Components		**Verdict**
Security Target	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Authorisation Control	ACM_CAP.3	PASS
TOE CM coverage	ACM_SCP.1	PASS
Delivery and Operation	CC Class ADO	PASS
Delivery Procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Examination of Guidance	AVA_MSU.1	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

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

The results of the evaluation are only applicable to the product Banksys DEP/PCI Version 3.0 in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [6] and the chapters 2, 4 and 8 of this report). The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, and if the evaluation of the modified product does not reveal any security deficiencies.

10 Evaluator Comments/Recommendations

The User Guidance documentation (refer to chapter 6) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [6] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
BKS	Banksys Authority Level of the TOE
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CBC	Cyber Block Chaining
CC	Common Criteria for IT Security Evaluation
CCRA	Common Criteria Recognition Arrangement
CUST	Customer Authority Level of the TOE
DCC	DEP Control Card
DEP	Data Encryption Peripheral
DES	Data Encryption Standard
DEV	Development mode of the DEP/PCI
EAL	Evaluation Assurance Level
INIT	Initial Authority Level of the TOE
IT	Information Technology
LIV	Live mode of the DEP/PCI
MAC	Message Authentication Code
MD	Message Digest
NONE	None Authority Level of the TOE
OSP	Organisational Security Policy
PCI	Peripheral Component Interconnect
PP	Protection Profile
RSA	Rivest, Shamir and Adleman
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOF	Strength of Function

ST	Security Target
TOE	Target of Evaluation
TP	TSF Protection
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TST	TST mode of the DEP/PCI

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[3] BSI certification: Procedural Description (BSI 7125)

[4] Applicaton Notes and Interpretations of the Scheme (AIS) as relevant for the TOE:

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] DEP/PCI Security Target BSI-DSZ-CC-0198, Version 1.1 (4), banksys, 2003-05-08

[7] Evaluation Technical Report BSI-DSZ-CC-0198, Version 3.0, TNO-ITSEF BV, 2003-06-17 (confidential document)

User Guidance Documentation:

[8] DEP/NT Documentation – DEP/NT Installation Guide, banksys, Version 02.01

[9] DEP/PCI – Customer Security Officer: Guidelines, banksys, Version 1.0 (10)

[10] DEP/PCI – Customer Host Programmers Guidelines, banksys, Version 1.0 (1)

[11] DEP/NT Documentation – DEP/NT C-ZAM/DEP User Manual, banksys, Version 02.03

[12] DEP/NT Documentation – DEP/NT PC-AUX Program User Manual, banksys, Version 02.01

[13] DEP/NT Documentation – DEP/NT Host Interface Supervision User Manual, banksys, Version 02.01

[14] DEP/NT Documentation – DEP/NT DEP Handler Supervision User Manual, banksys, Version 02.03

[15] Common Criteria Software – Integration Manual, banksys, Version 1.0 (10)

[16] Subset of Eval Library for DEP – Reference DFS Manual, banksys, Version 2.0 (12)

[17] DEP/PCI – Security Target, banksys, Version 1.1 (4)

[18] DEP/PCI – Guidance Documentation – Erratum, banksys, Version 1.0 (1)

[19] Subset STD Library for DEP – Ref DFS Manual, banksys, Version 3.5 (8)

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

CC Part 3:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

Evaluation assurance level (EAL) overview (chapter 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation“ allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component“ is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

„Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.“

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 6.2.3)

„Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.“

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 6.2.4)

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous,

do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.“

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

„Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.“

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

„Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.“

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 6.2.7)

„Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

„Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.“

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

„Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.“

„Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.“

„Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“