PROTECTION PROFILE

Version 1.00

AUTOMATIC CASH DISPENSERS/ TELLER MACHINES

Registered at the French Certification Body under the number PP/9907

CONTENTS

Participants:

BULL
Business Unit SST - Division Smart cards and Terminals
68, route de Versailles - BP45
78431 Louveciennes Cedex

DASSAULT A.T.
9,rue Elsa Triolet
Z.I. des Gâtines
B.P. 13
78373 Plaisir Cedex

DIEBOLD
5 bis, rue du Pont des Halles
94656 Rungis

NCR
1, square John J. Patterson
91749 Massy Cedex

SIEMENS NIXDORF
Retail and Banking Systems GmbH
Heinz - Nixdorf - Ring 1
D-33106 PADERBORN

WANG GLOBAL
rue de l'ancien marché
La Défense 9 - Puteaux
92047 Paris La Défense Cedex

This document has been compiled on the basis of version 2.0 of the Common Criteria dated May 1998. The final appendix lists the abbreviations and acronyms used in the Common Criteria, among which most of those coming from Common Criteria.

I. INTRODUCTION

I.1 Identification of the Protection Profile (PP)

Title: Automatic Cash Dispensers/Teller Machines

Version: 1.00

Reference: PP/9907

Keywords: ACD/ATM, chip card, mag stripe card, personal identification number (PIN), microcircuit, withdrawal

I.2 General outline of the PP

The Protection Profile focuses upon automatic cash dispensers/automatic teller machines: these machines enable holders of identification cards (chip cards or smart cards) who have a personal identification number with which they can authenticate themselves, to carry out various transactions on a banking product linked with the card, in particular cash withdrawal.

This Protection Profile has been developed to specify the requirements in terms of functionalities and levels of assurance applicable to ACDs/ATMs.

Many transactions can be carried out via an ACD/ATM. The target has therefore been deliberately restricted to matters connected with the use of a card, the identification of the cardholder (the confidentiality of the PIN, etc) and the dispensing of cash (the integrity of the interfaces with the server, etc).

The target assurance level is EAL4, augmented in respect of the penetration tests (AVA VLA.3 instead of AVA VLA.2). The target strength of function (SoF) is "SoF-medium".

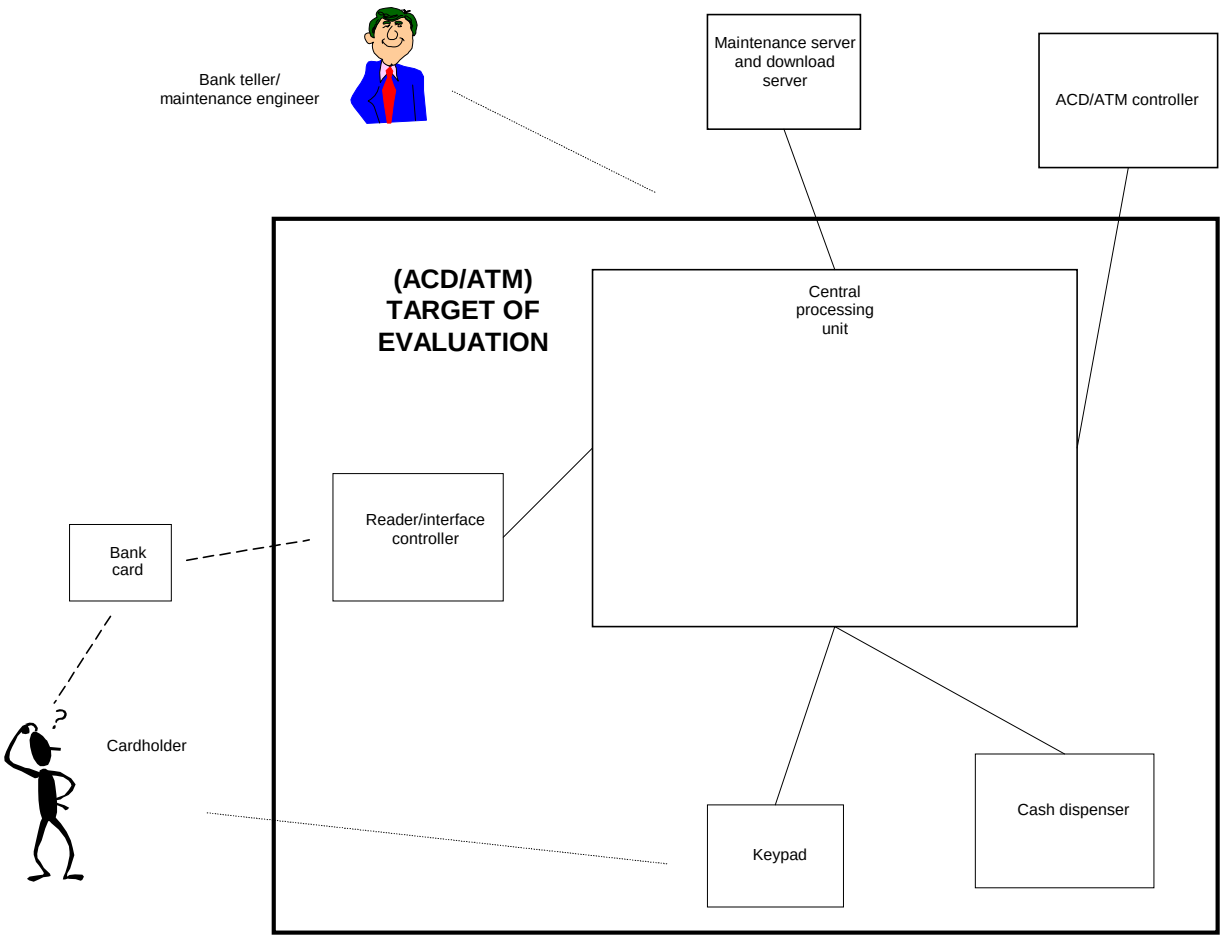
II. DESCRIPTION OF THE TARGET OF EVALUATION (TOE)

II.1 Definition

The target of evaluation relates to three different types of hardware:

- Automatic Cash Dispenser,
- Automatic Teller Machine (dispensing of banknotes and "self-service" transactions),
- Enquiry Terminal ("self-service" transactions).

For functional capabilities other than withdrawal, only those aspects which relate to the personal identification number are taken into account in the description of the PP.


Bank teller/
maintenance engineer
Maintenance server
and download
server
ACD/ATM controller
(ACD/ATM)
TARGET OF
EVALUATION
Central
processing
unit
Reader/interface
controller
Bank
card
Cardholder
Keypad
Cash dispenser

The target of evaluation comprises:

- a central processing unit (the "brain" which conditions or coordinates its overall operation),
- a cash dispenser (a hardware device for taking banknotes from cash cassettes and delivering them to the cardholder),
- a card reader (for smart cards and possibly stripe cards),
- an input device for the cardholder to use (subsequently termed the "keypad").

The Protection Profile relates mainly to interchanges between these various components, which are normally grouped together within a single hardware enclosure (see the diagram above), but any other architecture may be considered.

Comments:

- in most ACD/ATM, the central processing unit is a standard microcomputer enhanced with facilities for communicating with the AAC (see below) and for driving the dedicated peripheral devices,
- an ACD/ATM includes various devices: printers, etc. The characteristics of these are not needed for the present target of evaluation,
- the "cash dispenser" (or dispensing module) may consist of two separate modules (one for extracting banknotes and one for delivering them to the cardholder).

This general architectural scheme also includes various external parties who may be involved with operation of the target of evaluation: the AAC (ACD/ATM Controller), the cardholder, the operator (maintenance engineer or bank teller), the download server (which enables certain components to be modified remotely), the remote monitoring server (for accessing certain ACD/ATM information: the log file, device states, etc).

II.2 The parties

Withdrawal card: card enabling the target of evaluation to identify *the holder* of the card and then authenticate him.

Operator: A person responsible for maintaining, replenishing, etc the ACD/ATM. Two very different roles need to be distinguished:

- the maintenance engineer responsible for maintenance,
- the bank teller responsible for banking transactions.

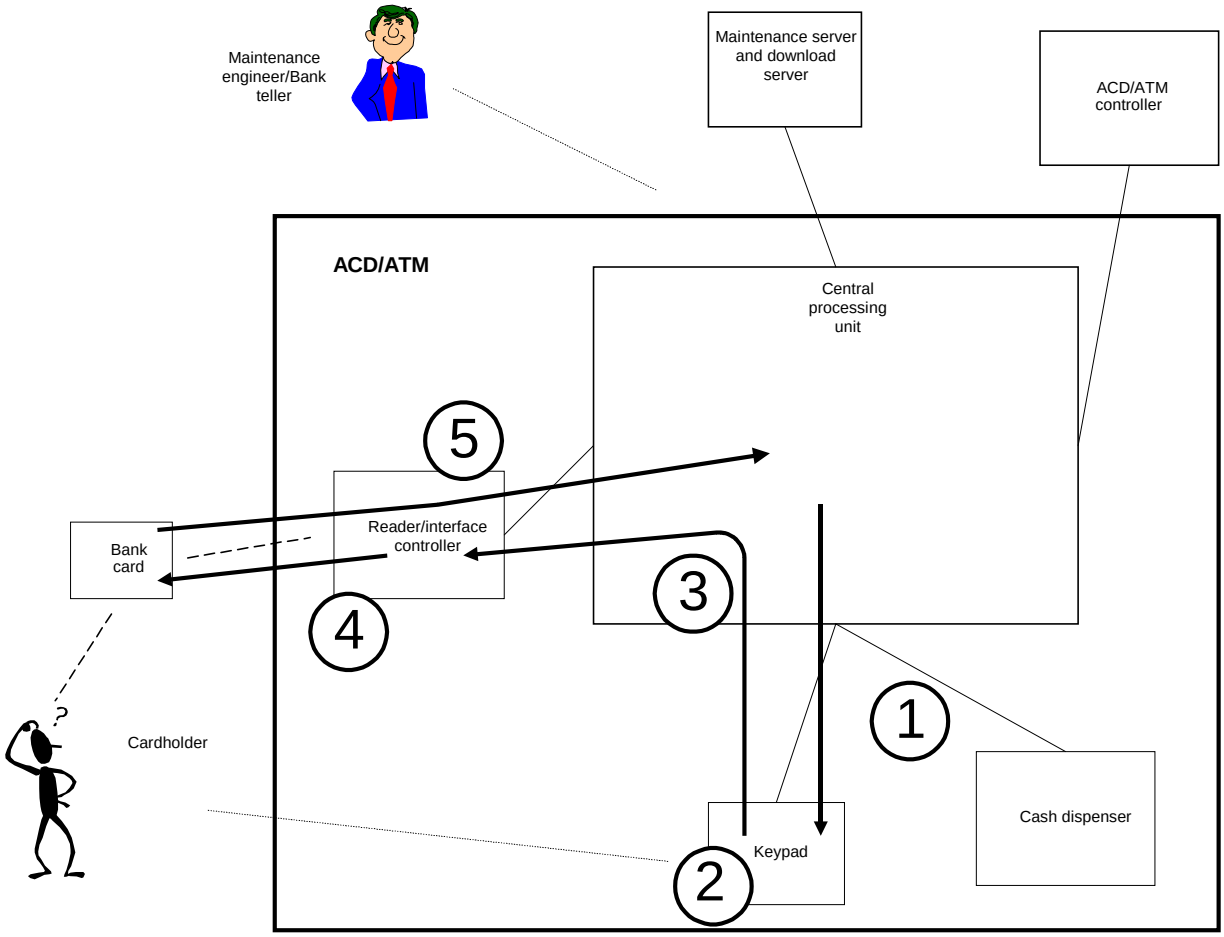
ACD/ATM controller (AAC): placed under the responsibility of the purchaser, this handles two main functions: control of the ACD/ATM (commissioning supervision, remote parameter setting, etc) and bank management (authorization, reporting on transactions, interface with the issuer, etc). The AAC is regarded as a trusted party.

Download server: this enables a new application, a new device driver or any other software item (firmware, etc) to be installed on the ACD/ATM. It is regarded as a trusted party. Other servers (or, at least, other functions) also need to be taken into account: remote monitoring server, etc.

Remote maintenance server: depending on the manufacturer, this can be used for remote management of fault conditions in the ACD/ATM, preventive maintenance, etc.

II.3 Dynamics of interchanges and flows

II.3.1 Transport and checking of the personal identification number off-line (from the microcircuit)



1. The central processing unit instructs the keypad to initiate personal identification number entry.

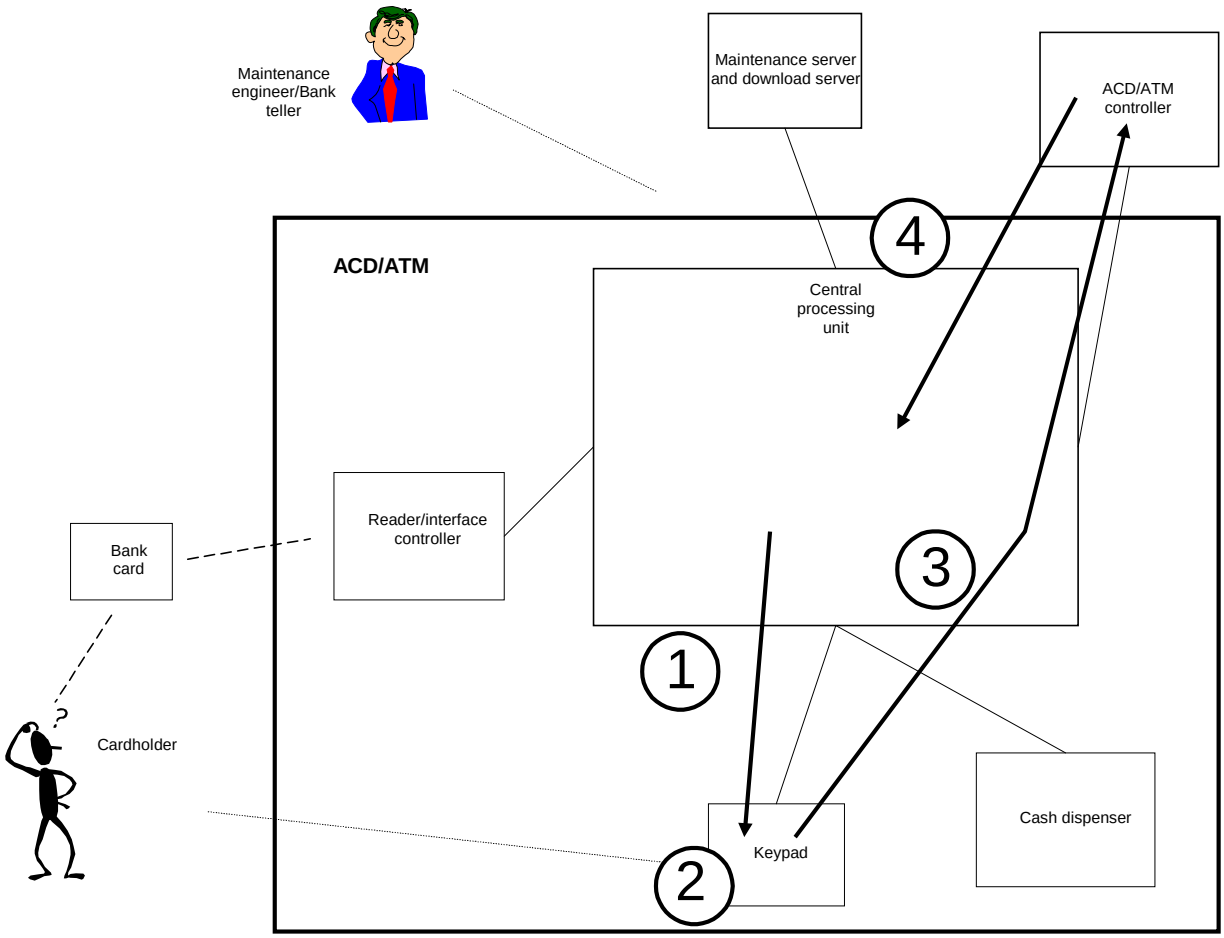
2. The cardholder enters his or her personal identification number.

3. The personal identification number is conveyed in a secure manner (to ensure its confidentiality) from the keypad to the reader/interface controller.

4. The personal identification number is conveyed from the reader/interface controller to the microcircuit. Note: depending on the card technology, the code may be forwarded to it unenciphered or encrypted.

5. The result of the check on the personal identification number is forwarded to the central processing unit by the microcircuit, via the reader/interface controller.

II.3.2 Transport and checking of the personal identification number on-line



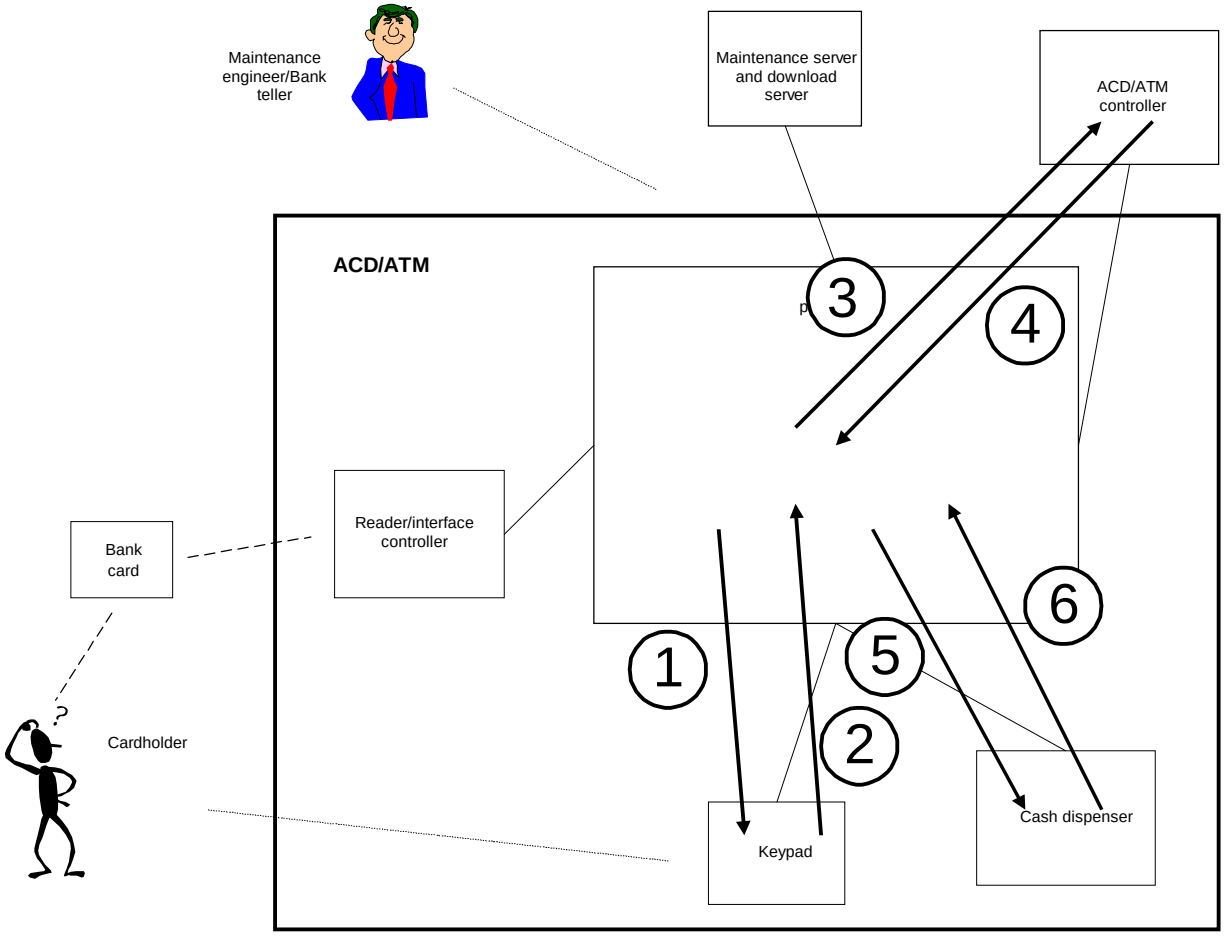
1. The central processing unit instructs the keypad to initiate personal identification number entry.

2. The cardholder enters his or her personal identification number.

3. The personal identification number is sent from the keypad to the AAC in a secure manner to ensure its confidentiality (the process of encryption between the ACD/ATM and the AAC is generally standardized).

4. The AAC informs the central processing unit of the results of the check.

II.3.3 Checking the amount



1. The central processing unit instructs the keypad to initiate a normal entry (for example from the numeric pad or the selection keys at the side).

2. Following entry, the central processing unit "retrieves" the amount.

3. The central processing unit sends the amount to the AAC as part of the authorization request.

   → amount requested

4. The AAC replies to the central processing unit.

   → amount authorized

5. The central processing unit sends the amount to the cash dispenser (dispensing module).

   → amount to be dispensed

6. The cash dispenser informs the central processing unit of the amount actually dispensed.

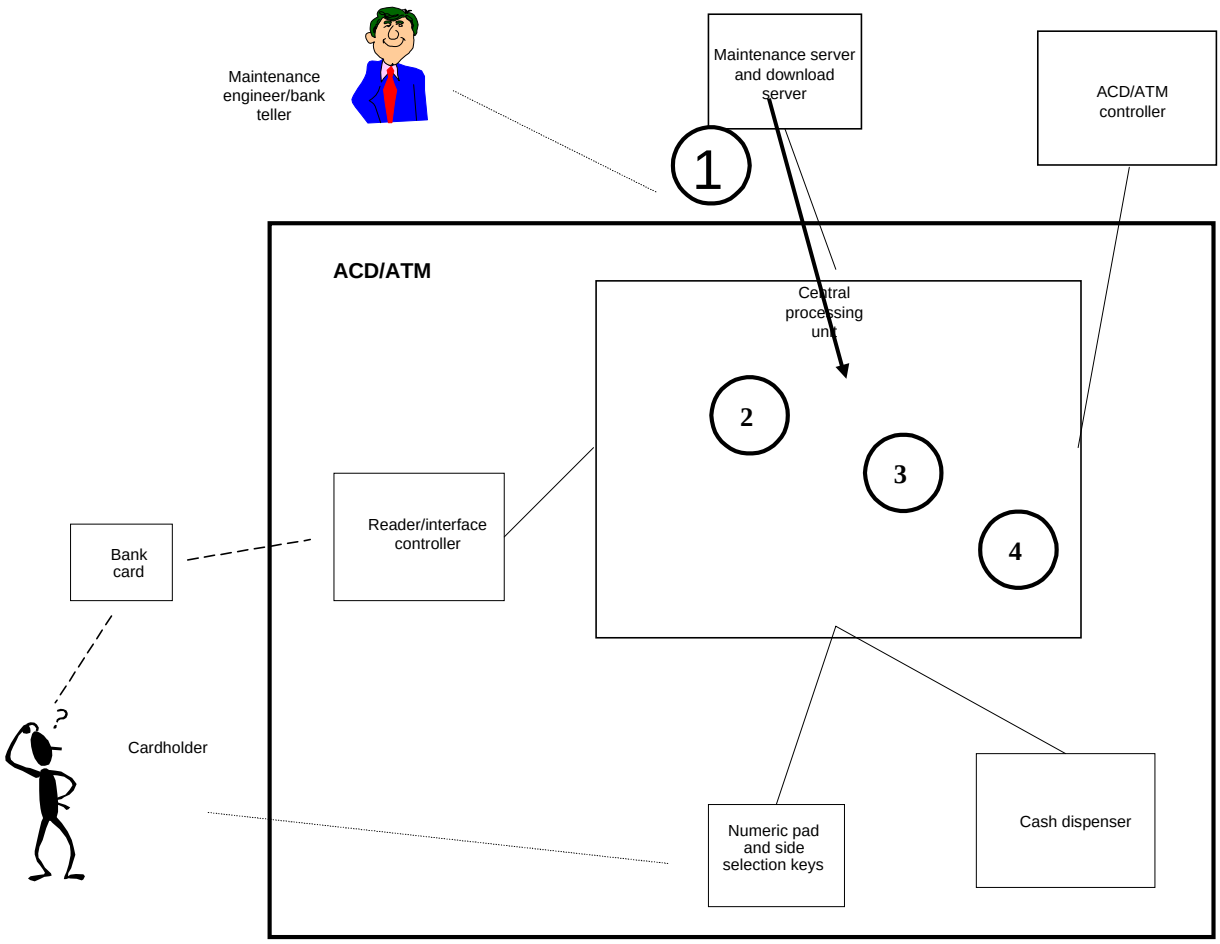
   → amount dispensed

This last phase may lead on to the issuing of a report to the AAC, a request for adjustment, etc.

Comments:

- The chain of events is not “that simple”: other actions may be undertaken, in particular following the response to the authorization request (return of the card, etc), and the extracting of the banknotes from the cassettes and their delivery to the customer may be carried out in two stages.
- As in the case of checking the personal identification number in chip mode, the integrity and authentication of the response to the authorization request can be checked. Other interchanges with a “black box” may therefore be necessary.

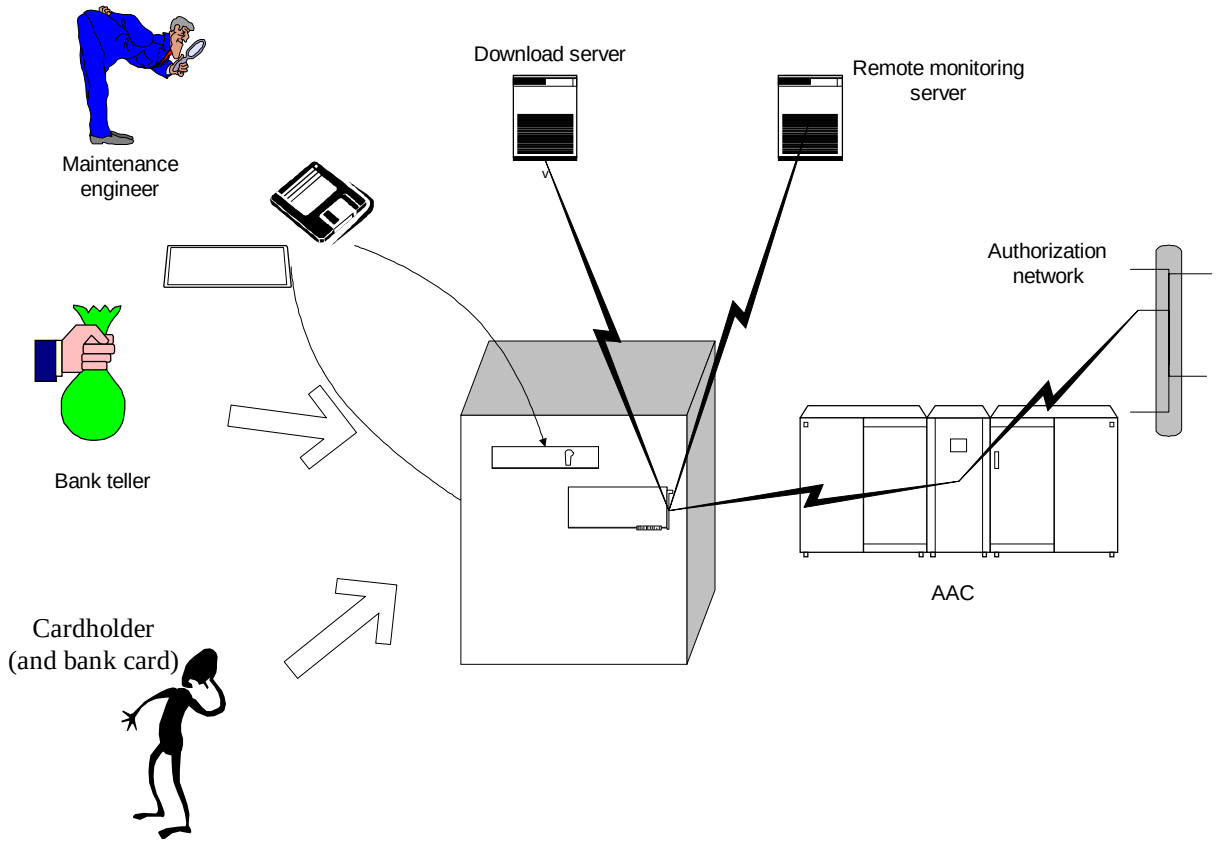
II.3.4 Downloading software



1. Transfer of the new software.
2. Authentication of the downloaded software by the ACD/ATM.
3. Checking of the integrity of the data transferred.
4. Starting up the new software.

Note: the term software means any file that may affect operation of the ACD/ATM (for example: application software, driver, parameter file, etc).

II.4 Direct interfaces with the target of evaluation



II.5 Scope of the Protection Profile

The outside agents mentioned in the diagram above are not included in the target of evaluation. In particular:

- the AAC,
- the Authorization Network and the issuing bank,
- the other servers (download and remote monitoring),
- the card.

Smart cards may be subject to separate evaluation.

The "customer" facilities other than withdrawal do not come under the present Protection Profile, apart from those aspects related to the personal identification number.

The "physical" factors (the safe, the capacity of the cash dispenser, etc) or "ergonomic" factors (the confidentiality of entry of the personal identification number, etc) likewise do not come under the present Protection Profile.

This Protection Profile may be upgraded so as to take into account an electronic purse.

III. SECURITY ENVIRONMENT

III.1 Identification of the assets to be protected

- Cardholder's personal identification number,
- Cryptographic keys:
    - Initial key or manufacturer key,
    - Encryption keys and integrity keys,
- Result of the withdrawal
- Cash balance
- Authorization data

III.2 Assumptions

H.RESP_ACQ	Each bank (purchasing bank) is responsible for its installed ACDs/ATMs from the time of installation. The bank is responsible for obtaining an assurance from the manufacturer that, when an ACD/ATM is installed, it complies with the manufacturer's specifications (as regards software, operating system, etc, and also hardware).
H.RESP_SERV	Each "owner of an authorized server" is responsible for that server and shall, in particular, guarantee its complete security. Therefore, any authorized server is regarded as a trusted party. The "authorized servers" will be defined in the ST.
H.RESP_GUICH	Purchasers are responsible for accredited personnel empowered to "maintain" ACDs/ATMs. Therefore, any accredited bank teller or maintenance engineer is regarded as a trusted party.
H.RESP_UTIL	Each "authorized" user is a cardholder who has been issued a personal identification number (PIN). In accordance with the rules in force relating to the handling of PINs, the cardholder shall take all necessary precautions to prevent its disclosure to a third party. The card issuer is responsible for bringing this to the attention of the cardholder.
H.INST_TOE	Once installed, the ACD/ATM shall enable the cardholder to enter his or her PIN in complete confidentiality. This assumption is the responsibility of the purchaser.
H.RESP_CARTE	Each cardholder is responsible for his or her bank card and shall take all necessary precautions not to mislay it, make it accessible or lend it to others.
H.REN_CLES	The integrity or data encryption keys used between the ACD/ATM and servers (AAC, download, remote monitoring) shall be renewed periodically.

H.CLES_INIT	The ACD and the various servers may have keys (called "manufacturer keys") used to initialize transport of the various encryption keys used in the normal life cycle of the machine. The confidentiality of these initial keys must be guaranteed even if they are kept outside the TOE.
H.INTERNET	ACDs/ATMs, if connected to open networks (the Internet, for example), must be so connected with sufficiently powerful protection to prevent intrusion and the reading (or deletion) of any files installed on the ACD/ATM. Such protection shall make it possible to authenticate the "remote party".

III.3 Threats

III.3.1 Hardware Trojan horse

M.CTM_PIN — PIN THEFT: Installation of a hardware device enabling the unenciphered PIN to be intercepted between its entry and its delivery to the system for checking.

III.3.2 Software Trojan horse

M.CTL_PIN — PIN THEFT: Installation of a software device enabling the unenciphered PIN to be intercepted between its entry and its delivery to the system for checking.

M.CTL_FAUX — FALSE ENTRY OF THE PIN: Installation of a software device prompting the user to enter his personal identification number without activating the keypad "security functions".

M.CTL_INTEG — ATTACK ON THE INTEGRITY OF DATA INTERCHANGED WITH THE AAC: Installation of a software device for modifying the data transmitted or received (authorization requests).

M.CTL_INTDIST — ATTACK ON THE INTEGRITY OF DATA INTERCHANGED WITH THE CASH DISPENSER: Installation of a software device for modifying the data interchanged (number of banknotes, etc) with this peripheral.

M.CTL_ESP — EAVESDROPPING SOFTWARE: Installation of a software device for accessing the ATM's memory or hard disk (electronic journal, cash balance, etc).

III.3.3 Intrusion into the telecommunications network

M.IRT_INTDA — ATTACK ON THE INTEGRITY OF DATA INTERCHANGED WITH THE AAC IN RESPECT OF AN AUTHORIZATION REQUEST: modification of the request or its response.

M.IRT_INTCR — ATTACK ON THE INTEGRITY OF DATA INTERCHANGED WITH THE AAC IN RESPECT OF A WITHDRAWAL REPORT (OR A REQUEST FOR ADJUSTMENT): modification of the message or its response.

M.IRT_GDG — MASQUERADING AAC: connection to a bogus AAC (substitution for the true AAC), enabling authorizations to be granted fraudulently.

M.IRT_RO — OPEN NETWORK (Internet) INTRUDER: connection of an unauthorized party.

M.IRT_TELECH MASQUERADING ON DOWNLOADING: connection of a bogus download server (to install one of the above software Trojan horses, for example).

M.IRT_CLES MASQUERADING ON TRANSFER OF TRANSPORT AND INTEGRITY KEYS: modification of the keys transferred from the AAC to the ACD/ATM (for sabotage purposes).

M.IRT_EXPLOIT ALTERING THE TRANSACTIONS (loading of the safe, account balancing, etc).

III.3.4 Intrusion during maintenance

M.IM_DOM SUBSTITUTING A DENOMINATION IN THE CASSETTE: "error" in loading the cassettes.

M.IM_DECL INCORRECT ACCOUNT STATEMENT: loading of an "incorrect" number of banknotes or declaration of an incorrect number of banknotes counted into the reject cassette.

M.IM_BILL BANKNOTE THEFT: ACD/ATM (cassettes, delivery/dispensing and reject path) accessed by an unauthorized party.

M.IM_CASS CASSETTE THEFT: cassettes accessed by an unauthorized party.

M.IM_LOG LOADING OF FRAUDULENT SOFTWARE: installation of fraudulent software on diskette (see Trojan horses, above).

M.IM_PROM BOGUS PROM: installation of a bogus PROM (together with bogus firmware): this threat is identical to certain software Trojan horses mentioned above.

III.3.5 Actions at the customer end

M.ACC_VOL THEFT OF THE BLACK BOX AND SECRETS: "snatching" the enclosure (and possibly the keypad) containing secret information.

M.ACC_FAUX BOGUS ACD OR FALSE FRONTAGE: Installation of a device (a bogus device entirely "external" to the ACD/ATM) which is designed to seize cards and their PINs.

III.3.6 Other threats

M.AM_VOL THEFT AND/OR DISCLOSURE OF INITIAL KEYS DURING THEIR INSTALLATION IN THE ATM.

III.4 Security policy

The Protection Profile has elected not to include any security policy.

IV. SECURITY OBJECTIVES

IV.1 Security objectives relating to the target of evaluation

OT.INT_DA	The ACD/ATM shall enable the AAC to verify the integrity of the elements of the authorization request.
OT.INT_RDA	Any modification of the elements (response code and authorization number) of the response to the authorization request while being transferred shall be detectable. The ACD/ATM shall ensure that the response corresponds to the withdrawal in progress.
OT.PIN	The PIN shall remain confidential. In particular, it shall not be possible to intercept it unenciphered between the device at which it is entered and the place where it is checked (microcircuit or AAC or issuer). However, the PIN may be input to the microcircuit either encrypted or unenciphered depending on the technology of the card.
OT.LECTCLES	It shall not be possible for any party to read the cryptographic keys.
OT.LOGICIELS	It shall not be possible for any unauthorized software to be installed on the ACD/ATM (authorized software will be defined in the ST).
OT.MAINT	Maintenance (and running) operations must be traced.

IV.2 Security objectives relating to the environment

OE.INT_CLES	Any modification of the cryptographic keys which occurs while they are being transferred over a network shall be detectable.
OE.CHIF_CLES	Any cryptographic key transferred over the telecommunication network shall be encrypted by a key transport key.
OE.INT_AUTO	Any modification of the card identification elements, of the amount of the authorization, of the number of the ACD/ATM and of the transaction number while they are being transferred over a communication network in respect of an authorization request shall be detectable.
OE.INT_CR	Any modification of messages notifying the server of a modification of the cash balance in the ACD/ATM while they are being transferred within the telecommunication network shall be detectable.
OE.ACCEPT	The AAC shall carry out or initiate the card acceptance checks appropriate to the technology of the card.
OE.MAINT	People responsible for the ACDs/ATMs shall employ trusted maintenance staff and bank tellers.
OE.PORT	Cardholders shall be responsible for their card and for the confidentiality of the PIN. However, purchases (via the ACD/ATM installation) shall enable them to enter their PIN in complete confidentiality.
OE.REN_CLES	Encryption keys shall be renewed frequently.
OE.CLES_INIT	Initial keys, whether kept or taken out of the TOE, shall be dealt with in a confidential manner.
OE.FIREWALL	If ACDs/ATMs are connected to an “open” type network, the firewall used shall be trusted so as to adequately prevent from open network intrusions.

V. TECHNICAL SECURITY REQUIREMENTS

V.1 Technical security requirements of the target of evaluation

V.1.1 Functional requirements

Traceability of the actions of maintenance staff and bank tellers (and auditing of requirements):

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [selection: minimum (see the table itemized by component below)] level of audit; and
c) [assignment: maintenance actions / bank teller activities].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*assignment: other audit relevant information*]

Dependencies: FPT_STM.1 Reliable time stamps

Table itemized by component

Component	Item to be audited
FMT_MTD.1	None (no read access possible)
FPT_ITC.1	No audit action identified
FPT_ITI.1 (1st oc)	Modification of the data transmitted
FPT_ITI.1 (2nd oc)	Modification of the data transmitted
FPT_ITI.1 (3rd oc)	Modification of the data transmitted
FPT_ITT.1	No audit action identified
FPT_PHP.3	No audit action identified
FPT_STM.1	Modification of the time stamp
FPT_TDC.1	Correct installation of software

No access to cryptographic keys:

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: [assignment: read]] the [assignment: cryptographic keys] to [assignment: NOBODY].

Dependencies: FMT_SMR.1 Security roles

Forwarding of the code to the AAC:

FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

Dependencies: No dependencies.

Refinement: The relevant "TSF data" are: the PIN. The "remote trusted IT product" is the AAC.

Integrity of the authorization request:

FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [*assignment: a defined modification metric*].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [*assignment: action to be taken*] if modifications are detected.

Dependencies: No dependencies.

Refinement: The "TSF data" are: the amount. These items may be extended in the ST. The "remote trusted IT product" is: the AAC.

Integrity of the response to the authorization request:

FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [*assignment: a defined modification metric*].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [*assignment: action to be taken*] if modifications are detected.

Dependencies: No dependencies.

Refinement: The relevant "TSF data" are: the authorization number and the response code. These items may be extended in the ST. The "remote trusted IT product" is: the AAC.

Integrity of the downloaded software:

FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [*assignment: a defined modification metric*].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [*assignment: action to be taken*] if modifications are detected.

Dependencies: No dependencies.

Refinement: The "remote trusted IT product" can be either: the AAC (for transferring parameter tables) or the download server.

Transferring the code from the keypad to the reader-interface controller / to the AAC:

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [selection: disclosure] when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies.
Refinement: The relevant "TSF data" are: the PIN.

Confidentiality of the cryptographic keys:

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist [*assignment: physical tampering scenarios*] to the [assignment: cryptographic keys] by responding automatically such that the TSP is not violated.

Dependencies: No dependencies.

Refinement: The "TSFs for which resistance to physical attack" is relevant: are restricted to the elements (black boxes) which can hold keys.

FAU_GEN dependencies:

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies.

Authentication of the downloaded software:

FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [*assignment: list of TSF data types*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [*assignment: list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.

Dependencies: No dependencies.

Refinement: the "another trusted IT product" is: the download server. The "TSF data types" are: the downloaded software. The items may be extended in the ST.

V.1.2 Assurance requirements

The target assurance level is "EAL4", with augmented assurance requirements upon penetration tests (AVA VLA.3 instead of AVA VLA.2).

Note: At risk of weighing down the Protection Profile, the assurance requirements are described below in the appendices to satisfy the needs of non-specialist readers of the Common Criteria.

AVA_VLA.3 Moderately resistant

Dependencies:

ADV_FSP.1	Informal functional specification
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.1	Subset of the implementation of the TSF
ADV_LLD.1	Descriptive low-level design
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance

Developer action elements:

AVA_VLA.3.1D	The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.
AVA_VLA.3.2D	The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.3.1C	The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.3.2C	The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.
AVA_VLA.3.3.C	The evidence shall show that the search for vulnerabilities is systematic.

Evaluator action elements:

AVA_VLA.3.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.3.2E	The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.
AVA_VLA.3.3E	The evaluator shall perform an independent vulnerability analysis.
AVA_VLA.3.4E	The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the

	exploitability of additional identified vulnerabilities in the intended environment.
AVA_VLA.3.5E	The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a moderate attack potential.

V.2 Security requirements relating to the technical environment

The Protection Profile has elected not to include any requirement relating to the technical environment.

VI. APPLICATION NOTES

The various checks provided for by card issuers, in particular cardholder authentication (by entering the personal identification number) are to be carried out. They may be specified in the ST.

In order to satisfy the environment-related assumptions and the environment-related security objectives, the user documentation must contain the corresponding recommendations. Distribution of these recommendations shall be relatively restricted or confidential so as not to jeopardize overall security!

It should be noted that the checks provided for by card issuers may take the place of certain functions implemented (for example, in EMV mode, if the card produces a "trusted" certificate, the production of special certifying stamps is unnecessary).

Furthermore, the ST shall include cryptographic key management.

Cryptographic management may be specific to each manufacturer, but :

- all the devices and algorithms used for encryption shall be specified in the ST,
- data transport and integrity keys used internally by the ACD-ATM shall be renewed periodically,
- any attempted theft to the keys used by the ACD/ATM shall result in their destruction.

To some extent security relies on the specifications of the cards and all interbank matters (prepared by the issuers), which "add" numerous checks, and on the ACD/ATM controller (in other words, the "banking network"), which is responsible for implementing numerous security procedures (in particular, those imposed by the technology of the card).

VII. APPENDICES

VII.1 Glossary

VII.1.1 "Banking Terms"

ACD/ATM application: Application software which directly or indirectly controls the operation of the ACD/ATM. It is normally developed by the ACD/ATM manufacturer, but may also be developed by outside companies or directly by banking establishments. It may be installed on the ACD/ATM by maintenance staff (diskette) or by the download server.

ACD/ATM controller (AAC): Placed under the responsibility of the purchaser, this handles two main functions: control of the ACD/ATM and bank management (authorization, transaction reports, relations with the issuer, etc).

Bank teller: More accurately, this is the ACD/ATM "operator", responsible for "account" management (account balancing, replenishment of banknotes, repossession of seized cards, etc) and day-to-day operations (replacement of supplies, etc). Two very differerent roles need to be distinguished:

- the bank teller responsible for banking operations,
- the maintenance engineer responsible for maintenance.

Black box: This is a secure enclosure for safeguarding secrets and protecting sensitive information (personal identification number and encryption keys), in particular information interchanged between the ACD/ATM and the AAC (ACD/ATM controller).

Card: Card enabling the target of evaluation to identify and then authenticate the cardholder.

Cardholder: The holder of a bank card issued by an issuer.

Cash dispenser: This is a module used to extract banknotes from their cassettes and deliver them to the customer (and "swallow" them if left by the cardholder).

Device drivers: These are programs (often in the form of an API and sometimes included in the ACD/ATM application) for controlling the peripheral devices (floppy drives, printers, etc). They may be installed on the ACD/ATM by the maintenance engineer (diskette) or by the download server.

Download server: Normally the responsibility of the purchaser, this is used to install new applications, new device drivers or any other software (firmware, etc) on the ACD/ATM. Other servers (or, at least, other functions) must also be taken into account: remote monitoring server, etc.

Firmware: This is "software" which is built into the peripheral devices. It is normally installed by the manufacturer and updated by the maintenance engineer (PROM), but may sometimes be downloaded.

Issuer: This is the banking organization that supplies the card to the cardholder.

Keypad: This is a device used by the cardholder to enter his or her personal identification number and select an operation, an account, an amount, etc or enter the amount, account number, telephone number, etc. The keypad and the black box may be combined within the same device.

Maintenance engineer: Broadly speaking this is the person responsible for ensuring that the ACD/ATM is available (repairs, servicing, software updates, replacing of components, etc). The maintenance engineer may need to use the machine's floppy drive to access particular items (statistics files, etc) or to install software.

Manufacturer: designs and builds the ACD/ATM, often by assembling elements (peripherals, microcomputer) sourced from various suppliers. The manufacturer also designs and maintains the device driver, firmware, etc and often designs and maintains the ACD/ATM software.

Operating system: This is normally a standard off-the-shelf system

Operator: A person responsible for maintaining, replenishing, etc the ACD/ATM. Two very different roles need to be distinguished:

- the maintenance engineer responsible for maintenance,
- the bank teller responsible for banking transactions.

Parameter file: A set of files used by the purchasing bank to customize the operation of the ACD/ATM on the basis of ACD/ATM software (operations available, chain of events, advertising screens, etc). Customization is the responsibility of the purchasing bank which sometimes delegates the task to different partners, particularly the manufacturer. Customization can be updated via a diskette, by remote parameter setting (AAC) or by downloading (download server).

Purchaser: The organization with responsibility for the ACD/ATM and for the fiduciary currency placed in the ACD/ATM, for the ACD/ATM controller and for its operation. The purchaser often develops the ACD/ATM application and normally manages the parameter files (customization).

Reader / Reader interface controler: Peripheral device which can read a card (various kinds of technology: B0' chip, EMV, ISO2 stripe), write information (chip), disable an application or the chip, submit the personal identification number to the chip and optionally seize the card.

Telecommunication drivers: Generally added to a telecommunication card, these enable the ACD/ATM to communicate with the AAC (ACD/ATM controller), and, where appropriate, with other servers (maintenance, downloading, etc). ACDs/ATMs normally communicate in X25 mode via leased lines etc, but other solutions will probably soon emerge (TCP/IP, Internet, etc).

VII.1.2 "CC" terms - Abbreviations and definitions

Assurance: Ground for confidence that an entity meets its security objectives.

Authorized user: A user who may, in accordance with the TSP, perform an operation.

CC: Common Criteria for Information Technology Security Evaluation"

CM: Configuration Management

Dependency: A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

EAL: Evaluation Assurance Level

Evaluation: Assessment of a PP, an ST or a TOE, against defined criteria.

Evaluation Assurance Level (EAL): A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

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.

External IT entity: Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Internal communication channel: A communication channel between separated parts of TOE.

Internal TOE transfer: Communicating data between separated parts of the TOE.

Inter-TSF transfers: Communicating data between the TOE and the security functions of other trusted IT products.

IT: Information Technology

Iteration: The use of a component more than once with varying operations.

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

Organizational security policies: One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

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

Refinement: The addition of details to a component.

Security attribute: Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

Security Function (SF): 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 Function Policy (SFP): The security policy enforced by an SF.

Security objective: A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.

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

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.

Strength of Function (SOF): 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.

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

TOE Security Functions (TSF): 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 (TSP): A set of rules that regulate how assets are managed, protected and distributed within a TOE.

Trusted channel: A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

Trusted path: A means by which a user and a TSF can communicate with necessary confidence to support the TSP.

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

VII.2 Assurance requirements

ACM_AUT.1 Partial CM automation

Dependencies:

ACM_CAP.3 Authorization controls

Developer action elements:

ACM_AUT.1.1D The developer shall use a CM system.
ACM_AUT.1.2D The developer shall provide a CM plan.

Content and presentation of evidence elements:

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.
ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.
ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.
ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements:

ACM_AUT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_CAP.4 Generation support and acceptance procedures

Dependencies:

ACM_SCP.1	TOE CM coverage
ALC_DVS.1	Identification of security measures

Developer action elements:

ACM_CAP.4.1D	The developer shall provide a reference for the TOE.
ACM_CAP.4.2D	The developer shall use a CM system.
ACM_CAP.4.3D	The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.4.1C	The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.4.2C	The TOE shall be labelled with its reference.
ACM_CAP.4.3C	The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.
ACM_CAP.4.4C	The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.4.5C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.4.6C	The CM system shall uniquely identify all configuration items.
ACM_CAP.4.7C	The CM plan shall describe how the CM system is used.
ACM_CAP.4.8C	The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.4.9C	The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.4.10C	The CM system shall provide measures such that only authorized changes are made to the configuration items.
ACM_CAP.4.11C	The CM system shall support the generation of the TOE.
ACM_CAP.4.12C	The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements:

ACM_CAP.4.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.2 Problem tracking CM coverage

Dependencies:

ACM_CAP.3 Authorization controls

Developer action elements:

ACM_SCP.2.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_DEL.2 Detection of modification

Dependencies:

ACM_CAP.3 Authorization controls

Developer action elements:

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action elements:

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation, and start-up procedures

Dependencies:

AGD_ADM.1 Administrator guidance

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

ADV_FSP.2 Fully defined external interfaces

Dependencies:

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.2.2C The functional specification shall be internally consistent.
ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.
ADV_FSP.2.4C The functional specification shall completely represent the TSF.
ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements:

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.2 Security enforcing high-level design

Dependencies:

ADV_FSP.1	Informal functional specification
ADV_RCR.1	Informal correspondence demonstration

Developer action elements:

ADV_HLD.2.1D	The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C	The presentation of the high-level design shall be informal.
ADV_HLD.2.2C	The high-level design shall be internally consistent.
ADV_HLD.2.3C	The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.2.4C	The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.2.5C	The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.2.6C	The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.2.7C	The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.2.8C	The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.
ADV_HLD.2.9C	The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements:

ADV_HLD.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.2.2E	The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_IMP.1 Subset of the implementation of the TSF

Dependencies:

ADV_LLD.1	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ALC_TAT.1	Well-defined development tools

Developer action elements:

ADV_IMP.1.1D	The developer shall provide the implementation representation for a selected subset of the TSF.

Content and presentation of evidence elements:

ADV_IMP.1.1C	The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.
ADV_IMP.1.2C	The implementation representation shall be internally consistent.

Evaluator action elements:

ADV_IMP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_IMP.1.2E	The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

ADV_LLD.1 Descriptive low-level design

Dependencies:

ADV_HLD.2	Security enforcing high-level design
ADV_RCR.1	Informal correspondence demonstration

Developer action elements:

ADV_LLD.1.1D	The developer shall provide the low-level design of the TSF.

Content and presentation of evidence elements:

ADV_LLD.1.1C	The presentation of the low-level design shall be informal.
ADV_LLD.1.2C	The low-level design shall be internally consistent.
ADV_LLD.1.3C	The low-level design shall describe the TSF in terms of modules.
ADV_LLD.1.4C	The low-level design shall describe the purpose of each module.
ADV_LLD.1.5C	The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.
ADV_LLD.1.6C	The low-level design shall describe how each TSP-enforcing function is provided.
ADV_LLD.1.7C	The low-level design shall identify all interfaces to the modules of the TSF.
ADV_LLD.1.8C	The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.
ADV_LLD.1.9C	The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.
ADV_LLD.1.10C	The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

Evaluator action elements:

ADV_LLD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_LLD.1.2E	The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

Dependencies:

No dependencies.

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_SPM.1 Informal TOE security policy model

Dependencies:

ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_SPM.1.1D The developer shall provide a TSP model.
ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.
ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.
ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.
ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ADM.1Administrator guidance

Dependencies:

ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User guidance

Dependencies:

ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1 Identification of security measures

Dependencies:

No dependencies.

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_LCD.1 Developer defined life-cycle model

Dependencies:

No dependencies.

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation of evidence elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.1 Well-defined development tools

Dependencies:

ADV_IMP.1 Subset of the implementation of the TSF

Developer action elements:

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

Content and presentation of evidence elements:

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_COV.2 Analysis of coverage

Dependencies:

ADV_FSP.1 Informal functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 Testing: high-level design

Dependencies:

ADV_HLD.1	Descriptive high-level design
ATE_FUN.1	Functional testing

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements:

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Dependencies:

No dependencies.

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.
ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

Dependencies:

ADV_FSP.1	Informal functional specification
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_FUN.1	Functional testing

Developer action elements:

ATE_IND.2.1D	The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E	The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3E	The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

AVA_MSU.2 Validation of analysis

Dependencies:

ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance

Developer action elements:

AVA_MSU.2.1D	The developer shall provide guidance documentation.
AVA_MSU.2.2D	The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C	The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AVA_MSU.2.2C	The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.2.3C	The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.2.4C	The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.2.5C	The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

AVA_MSU.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.2.2E	The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.2.3E	The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.
AVA_MSU.2.4E	The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

AVA_SOF.1 Strength of TOE security function evaluation

Dependencies:

ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.