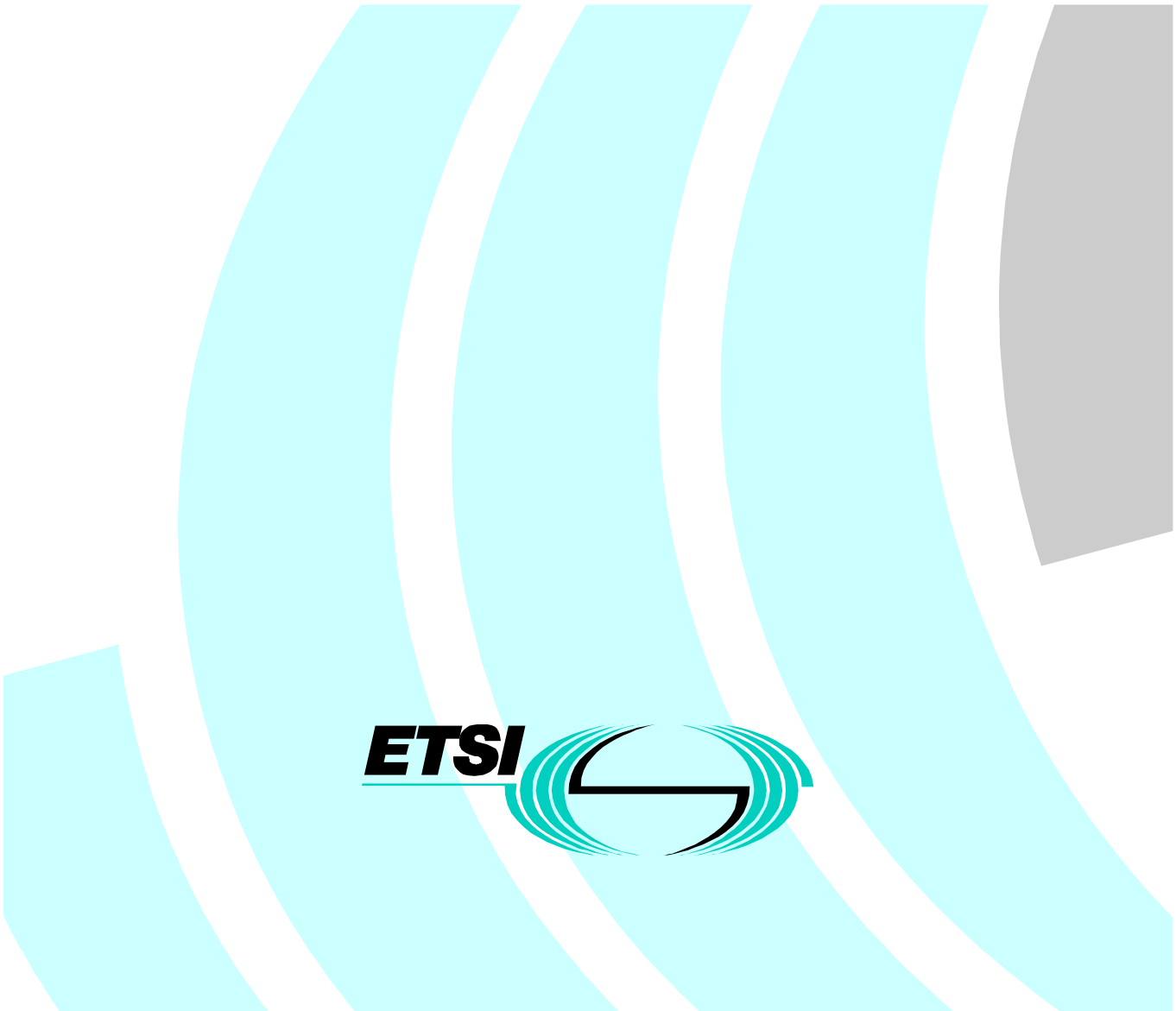
TS 101 209-2 V1.1.1 (1998-05)

Technical Specification

Identification card systems; Telecommunications IC cards and terminals; Interoperability with synchronous prepaid cards; Part 2: Security requirements



Reference
DTS/PTS-00209-2 (b70i0icr.PDF)

Keywords
Cards, payphone, interoperability, security

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
http://www.etsi.fr
http://www.etsi.org

Contents

Intellectual Property Rights

IPR's essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETR 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr or http://www.etsi.org/ipr).

Pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETR 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Project Pay Terminals and Systems (PTS).

1 Scope

The present document defines security requirements of the interoperability of synchronous prepaid cards in order to provide a common security level for compliant systems. It focuses mainly on the three elements of the complete system that are directly related to interoperability security. These three elements are:

- the Security Module (SM);
- the Secure Device (SD);
- the Trusted Third Party (TTP).

In the standard ES 201 209-1 [1], the following mechanisms are defined:

- acceptance of User Memory Cards (UMC) for payment purposes;
- claim of money for proven UMC usage from card issuers;
- key management between system operators and card issuer.

A security framework is necessary to support an interoperability scheme on the basis of ES 201 209-1 [1]. For card issuers who want to participate in such an interoperability scheme, trust in the security of the system is necessary, whereby two basic targets are most important:

- sufficient protection of the master keys of the card applications;
- correct billing.

These security targets are mostly reflected in the following two aspects of the architecture of the system described in [1], which are also described in annex A of [1].

- initial key download supported by the Trusted Third Party (TTP); and
- security requirements fulfilled by the Security Module (SM).

In the present document, the basic security requirements to reach the above mentioned security targets are specified. Systems can be evaluated against these requirements. This gives a common security level for systems in compliance with the present document.

In order to achieve this, the present document describes:

- the security architecture of the system;
- security targets to be achieved in the system;
- security requirements for the security relevant components;
- security requirements for the roles; and
- basic security requirements for the development and production of security products.

The present document does not imply the mandatory use of specific security mechanisms, if not already specified in ES 201 209-1 [1].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, subsequent revisions do apply.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ES 201 209-1 (V1.1.1): "Identification card systems; Telecommunications IC cards and terminals; interoperability with synchronous prepaid cards; Requirements for off-line and on-line configurations".

[2] ITSEC:"Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonised Criteria, Version 1.2, June 1991 (ISBN 92-826-3004-8)".

[3] ISO/IEC 7816-1 (1987): "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics".

[4] ISO/IEC 7816-2 (1988): "Identification cards - Integrated circuit(s) cards with contacts - Part 2: Contact locations and minimum size".

[5] ISO/IEC 7816-3 (1990) + Amendments 1 & 2: "Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".

[6] ISO/IEC 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter industry commands for interchange".

[7] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts - Part 5: Registration system for applications in IC cards".

[8] ISO/IEC 7816-6: "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Inter-industry data elements".

[9] ISO/IEC 7816-10 Draft: "Information technology -- Identification cards -- Integrated circuit(s) cards with contacts-- Part 10: Electronic signals and answer to reset for synchronous cards".

[10] EN 726-3 (1994): "Identification Card Systems - Telecommunication Integrated Circuit Cards and Terminals - Part 3: Application independent card requirements".

[11] EN 726-7: "Identification Card Systems - Telecommunication Integrated Circuit Cards and Terminals - Part 7: Security Module".

[12] ETR 115 (1994): "Terminal Equipment (TE); General concerns for the parties involved during the telecommunication integrated circuit card life cycle".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions apply:

application: An application can involve many hardware and software components interacting together to provide one or more services. E.g.: an SM management application can be composed of many components like computers, SM software, computer software, etc.

card issuer: The party that is responsible for the data on an UMC (including the secret key), and ultimately receives the payment for units when an UMC is purchased.

Card Management System (CMS): A system belonging to a card issuer which is used to maintain records which may include data related to UMCs issued by that party and payment claimed by the system operators. Data such as management information and secure details of revenue taken from UMCs may be exchanged with one, or more, Operator's Management Systems (OMS).

card manufacturer: The card manufacturer produces and tests cards. This operation consist in assembling a chip and a physical support (usually a card). Possibly the card manufacturer personalises electrically and logically the chip.

chip manufacturer: The chip manufacturer produces Integrated Circuits (IC) that will be later embedded in the IC Cards (ICC) and, if the integrated circuit has a Read-Only Memory (ROM), loads the ROM mask code into the ROM.

executable code: Executable code is a binary file (non-human readable form, e.g. exec or bin file) which has to be executed in conjunction with other files by a machine (computer, smart-card).

key: A sequence of symbols which controls the operations of encipherment and decipherment.

key management: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

Operator's Management System (OMS): A system belonging to a system operator which communicates with a number of terminals to distribute management information and collect data, such as secure details of revenue obtained from UMCs.

parameter: Parameter is a chain of characters (number, letter and/or symbol), generally stored within a file or entered by a human.

personnalisation: This phase applies to UMC, SM and SD. It prepares and sets these components in the usage phase. This operation consist in loading secret data, creating data structure.

pre-payment: A payment method using an IC card, where the card contains a pre-payment application. The pre-paid value is stored in the card and offers access to one, or more, applications. Pre-paid value means that payment is received in advance.

Secure Device (SD): A device which is used to securely store the key KTTP (which is pre-loaded by the Trusted Third Party) and to encrypt the card issuer loading key Kload. During operation, a loading key can also be stored and card issuer related keys can be encrypted. With the SD different key formats can be adopted.

Security Module (SM): A device containing logically and physically protected secrets - algorithm(s), related key(s), security procedures and information to protect applications in such a way that unauthorised access is not feasible. In order to achieve this the module may be further physically, electrically and logically protected (as in EN 726-7 [11]).

software: A software is a self-consistent computer program made-up of pieces of executable codes and static data.

static data: Descriptive file read by executable code or by human, to be used to run a software (e.g. Dynamic libraries).

SM/SD manufacturer: Is a card manufacturer which produces and tests SM and/or SD.

system operator: An organisation that operates a telecommunications system which accepts payment for access to its services by means of UMCs issued by card issuer(s).

terminal: A device which provides a user with access to the telecommunications system of a system operator, accepting payment by means of UMCs issued by a card issuer.

threat: An action or event that may prejudice security.

Trusted Third Party (TTP): A security authority, or its agent, trusted by other entities with respect to security related activities. In particular, a TTP is trusted for the purposes of key management.

TTP services: Shall be able to generate and store the keys (KTTP or KMttp) for the duration of the application life cycle. The TTP services shall be able to generate new components (SM and possibly SD) while using the initial keys (KTTP or KMttp).

The TTP services shall encrypt the SM downloadable software and compute the associated certificate to the SM software audit.

usage phase: Applies to UMC, SM and SD when they are used to provide a service to the final user. A component in operational phase cannot returned in personnalisation phase (see clause B.4).

User Memory Card (UMC): Is a memory card with a synchronous protocol and cryptographic security. The user pays the card issuer for units which may subsequently be used for access to a service from the terminal of a system operator. The UMC is therefore a pre-payment card. The UMC includes mechanisms which support:

- one way authentication of the UMCs identity (internal authentication);
- handling of a signed counter value, i.e. the counter value is included in the authentication;
- allowing only a decrease in the value of the counter.

An UMC is called a memory card because it is a type of ICC which contains read / write non-volatile memory and hard wired logic but which contains no microprocessor. ISO 7816 [3] to [8] specifies asynchronous ICCs. However, only certain aspects of [3] to [9] apply to UMCs because UMCs use a synchronous protocol.

UMC manufacturer: Is a card manufacturer which produces and tests UMC.

weak key: A value of a cipher key which gives to an algorithm some special properties that might in certain circumstances, weaken its security. The supposed weakness has to be related to a specific method of application of the algorithm.

NOTE 1: Concerning the DES algorithm, see D.W. Davies, W.L. "Price: Security for computer networks", Wiley and Sons, 1984, p 68f.

NOTE 2: There are no weak keys known for the TESA-7 algorithm.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Access Condition
Ax	Action number x
CHV	Card Holder Verification
CMS	Card Management System
EEPROM	Electrically Erasable and Programmable Read-Only Memory
IC	Integrated Circuit
ICC	Integrated Circuit Card
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
KTTP	Key TTP
OMS	Operator Management System
Ox	Object number x
PIN	Personal Identification Number

ROM	Read-Only Memory
SAM	Security Architecture Model
SD	Secure Device
SFx	Security Function number x
SM	Security Module
SOx	Security Objective number x
SRx	Security Requirement number x
STx	Security Target number x
Sx	Subject number x
TESA-7	Terminal Equipment Secret Algorithm 7
TOE	Target Of Evaluation
TTP	Trusted Third Party
ttp	trusted third party
Tx	Threat number x
UMC	User Memory Card

4 Security architecture and identification of security relevant components and roles

4.1 Introduction and overview

In ES 201 209-1 [1], a system is defined in order to set up the interoperability of UMC between partners. To reach that goal, the system has been divided in different entities which are connected together.

ES 201 209-1 [1] describes the process and the procedures which are necessary to obtain the interoperability of UMC and gives a description of the security of that system. The security is considered only in the interoperability aspect. The system is divided in some entities and the present document defines the security requirements between the entities for the interoperability. Some entity acts as a subcontractor of another and it is not directly involved in the interoperability process.

This document does not provide absolute security requirement for each entity, it only gives a relative confidence to the others entities (e.g. prevention of risks which are not connected to the interoperability).

As the security countermeasures are limited by physical limitations of the system, some threats are left due to this (e.g. limited size of the Blacklist).

4.2 Security architecture model

This subclause describes the Security Architecture Model (SAM) for synchronous pre-paid card scheme interoperability as defined in [1]. This Security Architecture Model describes the overall card scheme operation and provides the basis for a justification for the decomposition of the SAM in [11] into those components which are security enforcing, security relevant and not security relevant.

In [1] the following 5 main roles are involved:

- system operator;
- card issuer;
- SM manufacturer;
- user;
- Trusted Third Party.

In certain cases a single party may undertake several of the above roles.

The overall security architecture for a single card scheme is shown in figure 1.

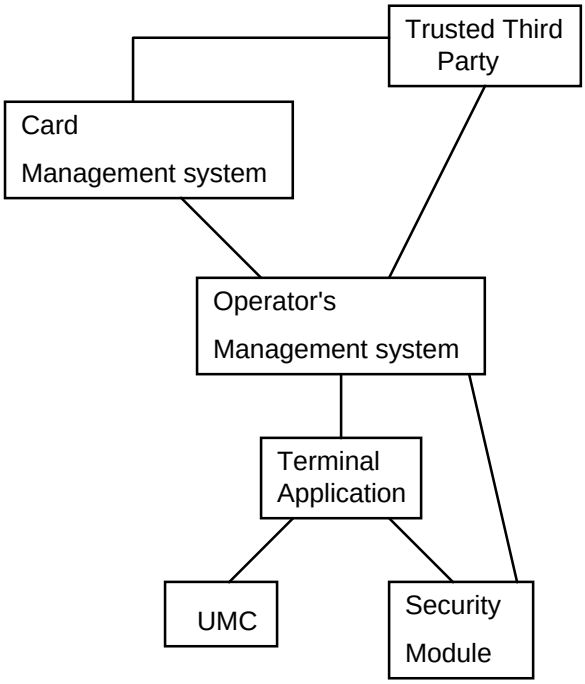


Figure 1: Single card scheme security architecture model

From a consideration of the SAM for the case of a single card scheme, a SAM can be determined which supports UMC Interoperability between multiple card schemes. A SAM for the case of two interoperating card schemes is shown in figure 2.

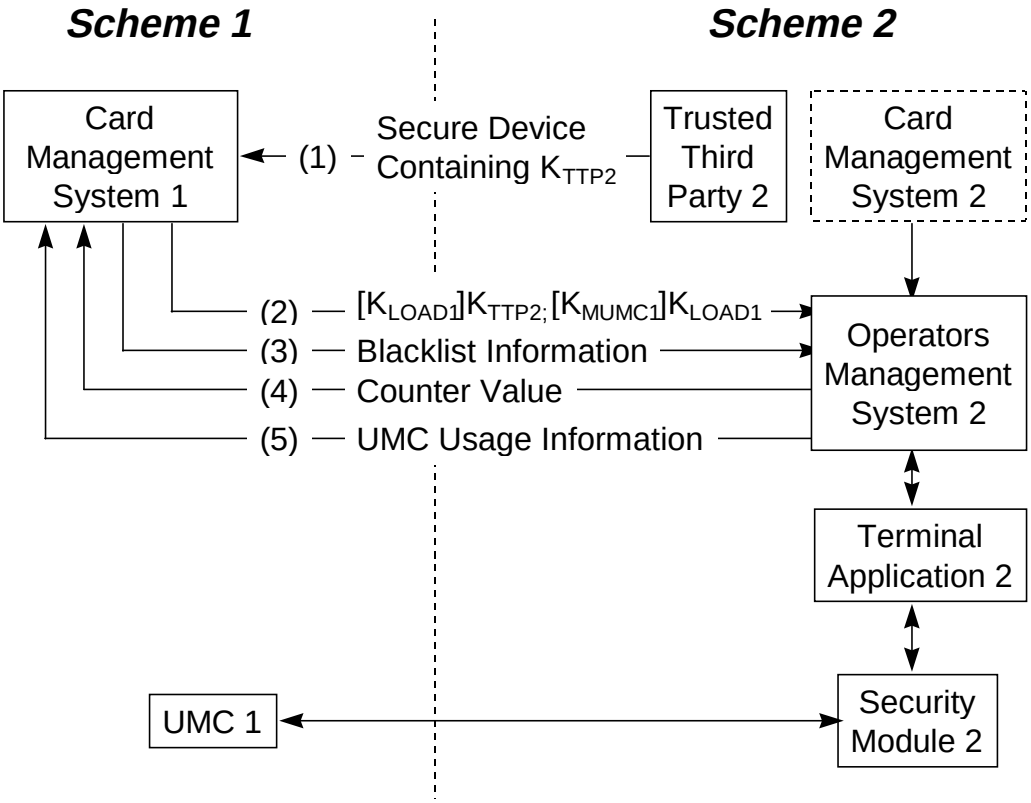


Figure 2: Interoperable card scheme security architecture model

The primary information flows which are necessary to ensure UMC interoperability between these two card schemes are:

1) transfer of Scheme 2 download encryption key to Scheme 1. The transfer of the Scheme 2 download encryption key to the Scheme 1 Card Management System may optionally make use of a Secure Device to protect the key from attack;

2) transfer of Scheme 1 K_{Mumc} key (and other keys e.g. K_{cer}, K_{MAC}) data to Scheme 2, using Scheme 2 download encryption key, confirmation by Scheme 2 to Scheme 1 that key data has been accurately received;

3) transfer of Scheme 1 blacklist information to Scheme 2;

4) transfer of Counter Value associated with scheme 1 UMCs from Scheme 2 to Scheme 1;

5) optionally transfer of UMC usage information from Scheme 2 to Scheme 1 (e.g. for fraud management).

4.3 General threat analysis

The threat analysis is based on the division of the system in several entities. For each entity, a list of identified threats is given in annex A.

For each entity, each threat is classified as one of three potential impact ratings (low, medium and high) and also whether it is directly involved in the interoperability process.

5 Security objectives

5.1 Scope

Only security objectives for two levels of security relevance are defined in the present document. The highest (SO-2) relates to components that have a significant number of high level threats directly related to interoperability. The lower objective (SO-1) relates to all other components.This is only the minimum suggested security objective and interoperability partners may request additional requirements for assurance of the security of a component.

5.2 Definition of security objectives

5.2.1 Security objective SO-1

SO-1 correspondents to no, low or medium level threat, with respect with the interoperability.

1) quality aspects of the component functionality are relevant;

2) no additional security assurance requirements are defined;

3) optionally additional security requirements (e.g. inspection of the operational environment) is subject to bilateral agreement, see [1] - annex E.

5.2.2 Security objective SO-2

SO-2 correspondents to the threat level high.

1) inspection of the development environment of the relevant component;

2) inspection of the delivery of the relevant component;

3) inspection of the operational environment of the relevant component;

4) evaluation of the component according ITSEC level E3, strength of mechanisms high or alternative suitable evaluation criteria in a comparable level of trust and strength of the security mechanisms.

5.2.3 Classification of the components related to the interoperability

Table 1 lists the security level that each components has to reach.

Table 1: Security level of each component

Component	SO	Level	Section
TTP services (The security relevant technical components of the TTP service has to be evaluated ITSEC level E3, strength of mechanisms high or alternative suitable evaluation criteria in a comparable level of trust and strength of the security mechanisms and the TTP service has to undergo an security assessment).	SO2	E3 - high	6.1
Security Module evaluation (However, the only reason to accept a SM evaluated ITSEC level E3, strength of mechanisms medium or alternative suitable evaluation criteria in a comparable level of trust and strength of the security mechanisms is due to the UMC signature length presented to the SM)	SO2	E3 - high	6.2
Secure Device (related to the symmetric algorithm)	SO2	E3 - high	6.3
UMC	SO1	-	Annex C
CMS	SO1 see Note	-	Annex E
OMS	SO1 see Note	-	Annex F
Terminal	SO1	-	Annex G
NOTE: As the result of the threats are high, it is recommended to have a higher level of evaluation, this has to be decided by the card issuer and/or the system operator respectively.			

Even if UMC is classified SO-1 due to the relevancy with respect to interoperability, its security is of central importance for the overall security of this payment method and an evaluation is recommended.

6 Security targets

6.1 Security targets of the TTP services

6.2 Component description

The TTP is a security authority, or its agent which is trusted by other entities with respect to security related activities. In particular, a TTP is trusted for the purposes of key management. It involves a product containing software and hardware aspects to achieve its role. The organisational aspects shall be described in the security target of the TTP services to be evaluated.

This subclause only addresses key management for K_{TTP} or K_{Mttp}. The TTP shall never use the K_{TTP} or K_{Mttp}. keys to decrypt the cryptograms of a card issuer.

The TTP security constraint shall be added to national or regional regulation but the present document shall not replace these regulations.

The authorised TTP shall secure the download program code into the SM. In case of a download in the field, it shall be encrypted. After installation of the key K_{TTP} or K_{Mttp} in the SM, any further downloaded software in the SM shall be encrypted under the control of the TTP. This software shall be previously certified according to the security target defined for the SM.

6.2.1 Environment for usage

The TTP environment shall be highly secured. Physical, organisational and personal measures have to be considered in relation with the evaluation level required. Protection of buildings and rooms against criminal actions shall be ensured.

6.2.2 List of objectives - information assets

In this paragraph the keys referred to are the initial loading key (K_{TTP} or K_{Mttp}) and any others required. The objectives of the TTP services are:

- secure generation, administration, and storage of keys for a Partner and algorithms;
- secure hand over of keys to other parties (secure loading of keys into the Secure Devices if used);
- secure loading of keys into the Security Modules;
- physical protection of the TESA-7 or other algorithms;
- additional security measures for secure data handling (e.g. CHV and PIN creation and administration);
- management of the application identity and computation of the different public key certificate (In case of use of the asymmetric key scheme for the SM initialisation).

6.2.3 Required objectives

To fulfil its role the TTP has to use software and hardware. This software and hardware, and their physical location are subject to the following requirements:

- it shall be ensured, that only authorised persons are able to operate the personalisation software;
- in general any unauthorised modification of data or keys shall be prevented. It shall be possible to recognise unauthorised actions, e.g., audit trails;
- access control mechanisms shall guarantee the confidentiality of keys and other protected data. The logical and / or physical storage of keys shall be secure;
- the generation of keys (and the associated certificate in case of public key initialisation scheme) shall be secure. The use of weak keys shall be prevented. It shall be important to verify random number generator;
- every personalisation action shall be evident.

6.2.4 Objects

The different objects of the TTP services are:

O1	the keys (K_{Mttp} or K_{TTP}) and the associated certificate in case of public key initialisation scheme
O2	the cryptographic algorithm (TESA-7 or other)
O3	software to be downloaded in the SM

6.2.5 Subjects

The different subjects of the TTP services are:

S1	the TTP manager
S2	the TTP users

6.2.6 Actions

The different actions of the TTP services are:

A1	generation, administration and storage of keys
A2	encryption and integrity protection
A3	loading of keys in SM, SD
A4	data handling

6.2.7 Relation subjects-objects-actions

Table 2: Security targets for the TTP - relation subjects-objects-actions

	S1	**S2**
O1	A1, A3, A4	
O2	A2	A4
O3	A2	

6.2.8 Threat analysis

The following threats shall be assumed:

T1	disclosure of the keys (K_{TTP} or K_{Mttp})
T2	disclosure of the algorithms
T3	modification of keys (K_{TTP} or K_{Mttp}, if modified in the SM or SD) within the TTP environment
T4	unauthorised installation of key (K_{TTP} or K_{Mttp})
T5	insecure transmission of keys (K_{TTP} or K_{Mttp})
T6	unauthorised generation of keys (K_{TTP} or K_{Mttp})
T7	generation of weak key (K_{TTP} or K_{Mttp})
T8	unauthorised usage of K_{Mttp} or K_{TTP}
T9	weak diversification of keys (K_{TTP} or K_{Mttp})
T10	loss of exhaustive view on personalisation actions
T11	unauthorised encryption or integrity protection of the software to be downloaded

6.2.9 Security functions

A TTP shall provide the following security functions to resist to the threats.

SF1	identification and Authentication of the staff of the TTP before using the software and hardware of the TTP services
SF2	an access control shall be effective to protect the sensitive data; this security function shall enforce the physical and logical integrity of sensitive data
SF3	audit, each personalisation action shall be reported
SF4	data exchange - Secured transmission (encryption of sensitive data); the sensitive elements shall be transmitted securely. It is the case for transmission of software updates for the SM (encryption with K_{TTP} or K_{Mttp}) or secured loading of keys into the security modules (K_{TTP} or K_{Mttp})
SF5	the key generation tool shall avoid the weak keys
SF6	external counter-measures (TOE external environment); to prevent criminal actions with the TTP and/or the TTP services, some physical, organisational and personnel security measures shall be used; e.g. it shall be ensured that only trustworthy personnel is employed; e.g. protection of buildings and rooms against criminal actions shall be ensured
SF7	unauthorised external access to the personalisation software shall be prevented, e.g. the personalisation device shall not be connected to an external network. If a network solution is necessary the physical and therefore also the logical connection of the personalisation device shall be limited to the secure personalisation environment
SF8	the TTP shall keep an exhaustive list of the SMs and SDs personnalized
SF9	if the key K_{Mttp} is used, then its diversification method shall cryptographically strong

6.2.10 Correlation threats - security functions

Table 3 shows the correlation of the security functions against the different threats concerning the hardware and the software of the TTP.

Table 3: Security targets for the TTP: Correlation Threats - Security Functions

	SF1	**SF2**	**SF3**	**SF4**	**SF5**	**SF6**	**SF7**	**SF8**	**SF9**
T1	X	X		X		X	X		
T2	X	X				X	X		
T3	X	X				X	X		
T4	X	X				X	X		
T5				X					
T6	X	X				X	X		
T7					X				
T8	X	X				X	X		
T9									X
T10			X					X	
T11		X							

6.3 Security targets for the SM

6.3.1 Security targets for the SM before usage phase

6.3.1.1 Introduction

This subclause describes the SM initialisation process. It includes the K_{TTP}/K_{Mttp} initialisation and the SM personalisation. These operations are done when the SM is in the phase 2, 3 and 4 of its life cycle. A definition of the phases is given in annex B.

The SM personalisation process is shown in figure 3.

As described in [1], after the manufacturing phase, the SM is then passed to a Trusted Third Party. This role may be fulfilled by a logically separate part of the SM manufacture organisation, or by a completely different organisation. The TTP loads the applications from the card issuers and any specific applications for the client system operator (as specified by that client system operator), the required cryptographic algorithm code and the secret key(s) (K_{TTP} and/or K_{Mttp}). This stage is known as "personalisation".

It consists in tow steps:

1) before the installation of the TTP 's confidential data (e.g. K_{TTP} / K_{Mttp} key), this phase covers the SM manufacture up to the loading of the file structure (phase 2 as defined in clause B.2);

2) installation of the K_{TTP} / K_{Mttp} key and other TTP confidential data (phase 3 as defined in annex B3).

These actions follow a time dependant sequence and they are too different to be included in the same subclause (see figure 3).

In practice the personalisation involves two types of actions:

1) one consists in the loading of the secure operating system, application software and the formation of an empty file structure. Depending on the operation sequence, some operation may be done under the control of the TTP;

2) the other consists in the loading of the TTP confidential data (e.g. K_{TTP} / K_{Mttp} key).

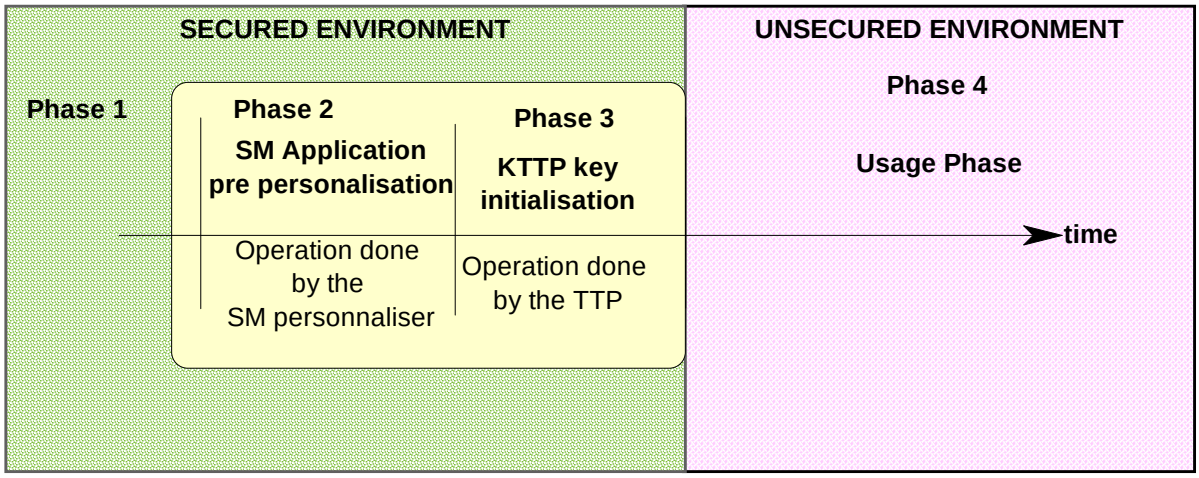


Figure 3: SM personalisation process

6.3.1.2 Security targets for the application pre-preparation (SM in phase 2)

6.3.1.2.1 Product definition

The product is the IC chip after manufacture. The TOE includes chip, mask, the environment and the procedures. The TOE shall comply with the one defined for the SM in usage phase (see subclause 6.2.2).

At the beginning of the process the SM IC shall be delivered by the IC manufacturer in phase 2 as defined in clause B.2.

This operation shall consist in:

1) check whether the SM is in phase 2;

2) if the SM is in phase 2, then loading of pre preparation data (e.g. creation of the file structure) in the SM;

3) controlling SM identity (verifying or loading) in respect for this manufacturer;

4) set definitively the SM in phase 3 as defined in clause B.3.

After this initialisation the SM shall change from phase 2 to phase 3. This transition from phase 2 to phase 3 shall be irreversible, the SM shall provide a physical and/or logical mechanism to enforce this transition.

6.3.1.2.2 Objects

O1	SM-PD: SM pre preparation data (e.g. file structure)

6.3.1.2.3 Subjects

S1	SMM: Security manufacturer

6.3.1.2.4 Actions

A1	L-PD: Loading of pre preparation data in the SM, the SM is in phase 2
A2	P-2→3: Change SM phase from phase 2 to phase 3

6.3.1.2.5 Relation Subjects - Objects-actions

Table 4: Security targets for the SM in phase 2 - relation Subjects - Objects - actions

	S1
O1	A1, A2

6.3.1.2.6 Threats analysis

The following threats shall be assumed:

T1	disclosure or modification of the confidential data
T2	non respect of the preparation sequence (phase 2 → phase 3)
T3	loading of an unauthorised additional software
T4	unauthorised generation of SM
T5	theft of non personalised SM (phase 2)
T6	loss of exhaustive view on pre preparation actions
T7	duplication of SM identity

6.3.1.2.7 Security functions

The SM and the organisational procedure shall provide the following security functions:

SF1	the SM shall provide a mechanism which identifies it
SF2	audit: every action shall be reported
SF3	an access control shall be effective to protect the confidential data and the SM component (e.g. secured environment, organisational procedures, the authorised persons employed and access control mechanism within the SM)
SF4	the SM shall have some physical and/or logical mechanisms which shall guarantee the irreversibility of the phase transition. The SM shall be able to indicate its actual phase.

6.3.1.2.8 Correlation Threats / Security Functions

Table 5: Security targets for the SM in phase 2 - Correlation Threats - Security Functions

	SF1	SF2	SF3	SF4
T1	X	X	X	X
T2		X		X
T3	X	X	X	
T4		X	X	
T5		X	X	
T6		X	X	
T7		X	X	

6.3.1.3 Security targets for the card preparation (SM in phase 3) - Initialisation of K_{TTP}/K_{Mttp}

6.3.1.3.1 Product definition

The product is the SM in phase 3 (see annex C). The TOE shall include chip, mask, the environment and the procedures. The TOE shall comply with the one defined for the SM in usage phase (see annex C).

At the beginning of the process the SM is in phase 3 (see clause B.3).

This operation shall consist in:

1) check whether the SM is in phase 3;
2) if the SM is in phase 3, then:
    a) controlling that the SM identity is unique per manufacturer;
    b) loading of TTP confidential data (e.g. initialisation key K_{TTP} or K_{Mttp}) in the SM.
3) set definitively the SM in phase 4 (see annex E).

Theses operations shall be realised by the TTP.

At the end, the transition from phase 3 to phase 4 (usage phase) shall be irreversible, the SM shall provide physical and logical mechanisms to enforce this transition (see figure 3).

6.3.1.3.2 Objects

O1	TTP-K: TTP initialisation keys (K_{TTP} or K_{Mttp})
O2	SM-U-Id: SM Unique identity

6.3.1.3.3 Subjects

S1	TTP: Trusted Third Party

6.3.1.3.4 Actions

A1	LK-TTP: loading TTP's initialisation key(s) in the SM, the SM is in phase 3
A2	C-U-Id: control SM Unique identity
A3	P-3→4: change SM phase from phase 3 to phase 4

6.3.1.3.5 Relation Subjects - Objects - actions

Table 6: Security targets for the SM in phase 3 - relation Subjects - Objects - actions

	S1
O1	A1, A3
O2	A2

6.3.1.3.6 Threats analysis

The following threats shall be assumed:

T1	disclosure or modification of the TTP confidential data (e.g. keys K_{TTP} or K_{Mttp}) and cryptographic algorithm (e.g. TESA 7)
T2	manipulation of TTP confidential data
T3	non respect of the personalisation sequence (phase 3 → phase 4)
T4	loading of an unauthorised additional software
T5	unauthorised generation of SM
T6	theft of non personalised SM (phase 3)
T7	loss of exhaustive view on personalisation actions
T8	duplication of SM identity

6.3.1.3.7 Security Functions

The SM and the organisational procedure shall provide the following security functions:

SF1	an access control shall be effective to protect the confidential data and the SM component (e.g. secured environment, organisational procedures, the authorised persons employed and access control mechanism within the SM)
SF2	audit: every action shall be reported
SF3	an access control shall be effective to protect the confidential data and the SM component (e.g. secured environment, organisational procedures, the authorised personal employed and the access control mechanism within the SM)
SF4	the SM shall have some physical and logical mechanisms which shall guarantee the irreversibility of the phase transition. The SM shall be able to indicate its actual phase
SF5	the TTP shall control the uniqueness of the SM identity before loading any confidential data
SF6	the TESA 7 algorithm shall be physically protected

6.3.1.3.8 Correlation Threats / Security Functions

Table 7: Security targets for the SM in phase 3 - Correlation Threats - Security Functions

	SF1	**SF2**	**SF3**	**SF4**	**SF5**	**SF6**
T1		X	X			X
T2		X	X			X
T3		X		X		
T4	X	X	X			
T5	X	X	X			
T6		X	X			
T7		X	X			
T8	X	X	X		X	

6.3.2 Security targets for the SM in usage phase (SM in phase 4)

6.3.2.1 Component description

The main functions which can be executed with a SM are given in table 8:

Table 8: Security targets for the SM - SM functions

Functionnality	authenticate a User Memory Card (UMC)
	check User Memory Card certificate
	increase counter after at least two successful UMC authentication
	extract counters with an associated MAC
	download enciphered and signed keys
	diversify Master keys, select keys
	download of additional software
	download application software
	invalidate application software

6.3.2.1.1 Definition of the TOE

The Target Of Evaluation (TOE) includes chip, mask and additional downloaded software. The SM shall be in usage phase and it shall remain in this phase (see [12] subclause 4.4).

6.3.2.1.2 Type of use

The SM is used either in terminal equipment or the network to store and manage sensitive data, and to process the cryptographic functions necessary for UMC interoperability.

Security Module is used in interoperability scheme for the following purposes:

- UMC authentication. These mechanisms allow the System Operator to accept authenticated UMC from the Card Issuer without relevant algorithm and secret keys (K_{Mumc}, K_{MAC}, K_{cer}) disclosure;

- secured counters. These Security Module's mechanisms are necessary to provide the Card Issuer a convenient and reliable way for settlement of UMC usage in the System Operator's terminals. Internal Security Module counters are increased all through the communication after at least two successful UMC authentications. When the internal SM counters are read out of the SM, they are integrity protected using K_{MAC} key. These mechanisms lead to availability of cryptographically secured counters which can be verified (source and integrity) by the Card Issuer;

- encryption and integrity protection of data. Provide the Card Issuer with mechanisms for secured data exchanges with the Security Module (e.g. new keys downloading);

- secure storage of sensitive data. In order to process the previous mechanisms the Security Module shall store relevant sensitive data. These data include TTP keys (K_{Mtp}, K_{TTP}), Card Issuer keys (K_{LOAD}, K_{Mumc}, K_{MAC}, K_{cer}), as well as SM identification data, algorithms, counters and application software;

- in usage phase, the SM may include a state, where the SM is not yet ready to accept a Card Issuer UMC but all necessary preparatory steps (after phase 3) can be made when the SM is installed in the terminal or in the network (e.g. installation of Card Issuer keys).

6.3.2.2 Environment for usage

In this phase no special requirements to the environment can be supposed.

6.3.2.3 Objects

Objects which need to be protected:

O1	SM identification data
O2	counters
O3	card issuer keys (K_{Mumc}, K_{cer}, K_{MAC}, K_{load})
O4	others keys (K_{Mttp}, K_{TTP})
O5	UMC-algorithm
O6	executable code and file structure

6.3.2.4 Subjects

S1	system operator
S2	card issuer
S3	terminal / Operator's Management Systemv

6.3.2.5 Actions

Defined subjects can perform the following actions at trusted objects in usage phase:

A1	Read	(R)
A2	Execute/Use	(E)
A3	Increase	(I), while decrementing the counter of the UMC
A4	Write	(W), (overwrite)
A5	Invalidate/rehabilitate	(V)
A6	Download	(D)

the TTP shall ensure that the downloaded software is evaluated and fulfil all the security requirements of the SM.

6.3.2.6 Relation Subjects - Objects - actions

Table 9: Security targets for the SM - relation Subjects - Objects - actions in usage phase

	S1 system operator	**S2 card issuer**	**S3 UMC**	**S4 TTP**
O1 SM identity Data	A1	A1		
O2 Counters	A1	A1	A3	
O3 card issuer Keys	A5 A2	A2 A4	A2	
O4 Others Keys	A2	A2		A2 A4
O5 UMC algorithm	A2	A2	A2	
O6 Application software				A6

6.3.2.7 Threats analysis

The following threats shall be assumed:

T1	disclosure of keys
T2	disclosure of algorithms
T3	unauthorised executable code and file structure download
T4	unauthorised key download
T5	manipulation of counters
T6	denial of service
T7	manipulation of keys
T8	try to use an invalid UMC
T9	disclosure of operating systemv
T10	modification of the operating systemv

6.3.2.8 Security Functions (SF)

SF1: Identification and Authentication (I&A)

For the UMC handling, the authentication function shall be based on a Challenge/Response mechanism, where the response is a cryptographic parameter calculated with identification parameters and the relevant key as input.

Authentication is important for the communication between OMS and the SM and for the UMC handling.

SF2: Access Control (AC)

Data of the SM can only be accessed (physically and logically) when specific access conditions for the respective operations have been fulfilled (according to the conditions defined in table 10). Specially the cryptographic keys and algorithms shall not be accessible.

SF3: Encryption (ENC)

Confidential data to be downloaded into the SM shall be presented enciphered in order to ensure their confidentiality.

SF4: Integrity of Data (INT)

Any data (e.g. static data, software, application…) to be downloaded into the SM shall be integrity protected (e.g. signed with a MAC) in order to ensure their integrity.

Each UMC debit relative counters read out from the SM for billing shall be extracted signed
(see ES 201 209-1, [1], subclause 5.3.7).

SF5: Secure state (SST)

It shall not be possible in the usage phase to turn the SM into an insecure state (e.g. the SM in usage phase shall reject any attempt to turn it back in the personalisation stage), in order not to violate one of the security target defined above (see [1], subclause 4.5).

SF6: Secure Counter Management (SCM)

The increase of the counters shall be secured in that way, that an increase is only possible, when a corresponding UMC counter is decreased, ,whereby the decrease of the UMC counter is proofed by consecutive authentications (SF1).

SF7: SM active authentication (audit)

If the SM has the possibility to download executable software in phase 4 (usage phase), then the SM shall have function which shall prove the authenticity of the SM executable software (ROM, EEPROM). This function shall use an external parameter (challenge) and the SM executable software (ROM, EEPROM) as data and shall produce a certificate (e.g. TESA 7 in chaining mode). The computed certificate shall be dependant from the SM executable software and the external challenge. The TTP shall be able to recompute this certificate and verify the result.

This function may also be added as an audit function, even if the SM does not allow the download of executable software.

In any case, if this function is implemented then it shall be included in the SM evaluation.

6.3.2.9 Correlation Threats Security - Functions

The following table shows the applicability of the Security Functions against the different Threats identified previously.

Table 10: Security targets for the SM - Security Functions versus Threats

	SF1	SF2	SF3	SF4	SF5	SF6	SF7
T1		X	X		x		
T2		X			x		
T3	X	X		x	x		x
T4	X	X	X	X	X		
T5	X	X			X	X	
T6	X	X			x		
T7		X		x	X		
T8	X				x	x	
T9		X			x		x
T10		X			x		x

SF5 covers all the threats because it is related to the other security function.

6.4 Security targets for the SD

6.4.1 Component description

The Target Of Evaluation (TOE) includes chip and software (mask and EEPROM). Loading additional software shall not be possible.

The SD shall be used for:

- storage of initialisation keys (K_{TTP} or K_{Mtp});
- storage of cryptographic keys (Card Issuer keys) for the interoperability partners;
- encryption of Card Issuer keys (Application keys from card issuer) which have to be delivered to interoperability Partners (System Operator).

The writing of keys in the SD has to be made in a organisationally and architecturally secured production-environment. Important is, that the key-handling outside the SD has to be done trustworthy (due to personnel, material and organisational aspects).

If the SD is an ICC, it may be based on EN 726-3 [10].

6.4.2 Environment of usage

No special requirements to the environment can be supposed.

6.4.3 Objects

O1	$K_{TTP:}$ Key generated by the TTP and stored in the SD and in the SMs of the System Operator
O2	K_{load}: Key generated by CI and processed in the SD and send encrypted with K_{TTP} to the System Operator who has to decrypt in his SMs and to store it in his SMs
O3	application software
O4	SD identityv

6.4.4 Subjects

S1	TTP: Trusted Third Party of a System Operator
S2	CI: card issuer and owner of the SD

6.4.5 Actions

A1	Write
A2	Read
A3	Execute
A4	encryption of card issuer key(s)

6.4.6 Relation Subjects - Objects - actions

Table 11: Security targets for the SD - Allowed Actions of Subjects at Objects in usage phase

	S1	**S2**
O1	A1, A3	A4
O2		A1, A3
O3	A3	A3
O4	A2	A2
NOTE: The Subject SO has no access to the SD		

It shall not be possible to download software in the SD once the key K_{Mtp} or K_{TTP} has been installed in the SD. If some code is downloaded before these action, then it shall be done under the control of the TTP.

6.4.7 Threat analysis

T1	disclosure of keys, stored in the SD
T2	modification / deletion of keys, stored in the SD
T3	manipulation of the functionality of the SD
T4	undetected manipulation of output data of the SD
T5	unauthorised usage of the SD (functionnalities and keys) access control

6.4.8 Security Functions

SF1	identification and authentication	A subject has to do an authentication before any action is possible
SF2	Access Control	Access to data fields shall only be possible via the application interface. The Access Conditions of the data fields shall ensure the data protection. (the functionality of the Source Code and the SD hardware shall be check). The SD shall use some physical protections
SF3	integrity protection	The output data of the SD shall be integrity protected
SF4	confidentiality	The keys shall always be output in an encrypted form
SF5	secure state (SST)	It shall not be possible in the usage phase to turn the SD into an insecure state (e.g. the SD in usage phase shall reject any attempt to turn it back in the personalisation stage), in order not to violate one of the security target defined above

6.4.9 Correlation Threats / Security Functions

Table 12: Security targets for the SD - Correlation Threats/ security functions(product))

	SF1	**SF2**	**SF3**	**SF4**	**SF5**
T1		X		X	X
T2	X	X	X		X
T3	X	X			X
T4			X	X	
T5	X	X			X

7 Compliance

In order to claim the compliance of a system with the present document, an evaluation for the two products is needed. The products are:

- Security Module (SM)→product;
- Secure Device (SD) (if used)→product.

To do so, security targets for the special product have to be set up. These security requirements shall contain as a compulsory subset the security targets described in clause 6 of the present document. The evaluation shall be done according to level E3 along the ITSEC criteria and with mechanism level high or along suitable evaluation criteria with the same level of trust, strength of the security mechanisms and evaluation depth (e.g. common criteria).

Concerning the TTP service, an assessment of the security concept of the TTP against the security requirements defined in subclause 6.1 compliant with the agreed code of practice in the area of security assessment shall be done. An evaluation of the relevant technical components of the TTP against ITSEC criteria (E3, mechanism strength high) or other suitable evaluation criteria with the same level of mechanism strength and evaluation depth shall be performed.

Annex A (informative): Security classification

The classification proposed in this annex is a guideline only which was used in the preparation of the present document and that the relevance and classification level of some of these risks may depended on various factors, e.g. the architecture of a particular system.

The assumption has been made that all mechanisms described in ES 201 209-1 [1] of the present document are already implemented. Thus an attack, where there is a clear countermeasure defined in ES 201 209-1 [1] is weighted lower, than an other attack, where there is no countermeasure defined in ES 201 209-1 [1], assumed impact, probability and so on are similar.

Many of the individual threats described in the threat analysis have the same impact and should thus get the same ranking. In the following list, the most important general threats/impacts are classified as either High, medium, low and whether it is relevant for interoperability:

Examples for the classification include:

high	loss of confidentiality of the master key for UMC
	unauthorized generation of a large amount of UMC personalisation data
medium	disclosure of secret algorithm of UMC
	clones of an individual UMC
	fraud on billing between card issuer and system operator
	modification of the blacklist
low	locally limited fraud, e.g. one payphone
	local modification of the blacklist
	local use of an unauthentic UMC

With this classifications, a lot of the threats in the following list are clearly defined. To classify each threat, the following symbols are used:

- ✓ this threat has a direct impact on interoperability;
- X level of the risk (high, medium or low);
- * the threat has a greater direct impact on one interoperability partner than the other. The relevance to interoperability may depend on any agreements for sharing risk defined in a bilateral agreement between the 2 parties;
- - means, no relevancy for the interoperability.

Table A1: Security classification: Security Module (SM) before the usage phase

Threats	high	med.	Low	Interoperability security relevant
disclosure of keys	X			✓
unauthorised modification of the file structure (e.g. AC's)	X			✓
duplication of serial numbers			X	✓
manipulation of keys (K_{TTP} and possibly card issuer keys)		X		✓
unauthorised production of SMs (as long as keys are unknown)			X	-
modification of personalisation system software		X		✓
personalisation of unauthorised SMs		X		✓
disclosure of algorithms		X		✓
manipulation of the SM operating system	X			✓

Table A2: Security classification: Security Module in the usage phase

Threats	high	med.	low	Interoperability security relevant
disclosure of keys	X			✓
disclosure of algorithms		X		✓
unauthorised application download (read out key functions can be downloaded)	X			✓
unauthorised key download (manipulation of counters can be done, but no access to keys)		X		✓
manipulation of counters (no interest of third parties, but by the system operator)		X		✓
denial of service		X		✓
manipulation of keys (manipulation of counters can be done, but no access to keys)		X		✓
try to use an invalid UMC			X	✓
disclosure of operating system		X		✓
modification of the operating system	X			✓

Table A3: Security classification: UMC in the usage phase

(in initialisation phase: see table A5)

Threats	high	med.	low	Interoperability security relevant
reverse engineering of the key K_{umc}		X		*
reverse engineering of the algorithm (change in threat analyses by dividing up between key and algorithm)		X		*
clones of a UMC		X		*
incrementation of the counter		X		*
failure during decrementation of the counter (UMC counter remains the same)		X		✓

Table A4: Security classification: Terminal application

Threats	high	med.	low	Interoperability security relevant
unauthorised decrementation of the counter (security relevant for the user and marketing aspect for the card issuer and the system operator)			X	✓
modification of the terminal software			X	✓
modification of blacklist/whitelist			X	✓
modification of tariff data (not relevant for interoperability)			X	-
modification of parameters			X	-
use of an unauthentic UMC			X	-
communicate with an unauthentic system operator management system (modification or unauthorised download of black list)			X	✓
communicate with an unauthentic Security Module (SM)			X	✓

The threats are classified low, as they have only local effect.

Table A6: Security classification: UMC manufacturer

(in the usage phase, see table A3)

Threats	high	med.	low	Interoperability security relevant
disclosure of personalisation data or transport keys (with a large amount of personalisation. Data, clones, which are difficult to detect, may be produced and with the transport key, one has access to the personalisation data for a longer time period.)	X			*
unauthorised production of UMCs (it is classified lower, than the general threat “clones of UMC”, as it is only one entity)			X	*
receiving unauthentic personalisation data			X	-
unauthorised modification of the personalisation software (as it may be a way to disclose personalisation data)		X		*
theft of cards			X	-

Table A7: Security classification: Card Management System (CMS)

The management and structure of the CMS databases as well as the generation of the UMC personalisation data are of internal importance to the CMS and card issuer.

The associated billing systems and their interfaces with the CMS are not considered as belonging to the CMS.

Threats	high	med.	low	Interoperability security relevant
inaccurate blacklist		X		*
manipulation of counter records		X		✓
manipulation of keys		X		*
manipulation of UMC personalisation data			X	*
receive unauthentic key from trusted third party	X			✓
unauthorized duplication of UMC personalisation data		X		*

Table A8: Security classification: Trusted Third Party (TTP)

Threats	high	med.	low	Interoperability security relevant
disclosure of keys by insecure storage	X			✓
disclosure of keys by storage in weak medium	X			✓
generate weak keys (definition from ETSI SAGE available?)	X			✓
unauthorised use of K_{Mttp}	X			✓
modification of keys (if modified in the SD and/or in an SM)	X			✓
weak diversification of keys	X			✓
unauthorised generation of keys	X			✓
unauthorised installation of keys	X			✓
insecure transmission of K_{TTP}	X			✓

Table A9: Security classification: Operator's Management System (OMS)

Threats	high	med.	low	Interoperability security relevant
delete billing data		X		-
modify billing data		X		*
communication with an unauthentic terminal (black list)			X	✓
communication with an unauthentic SM (here already cryptographic mechanisms are supposed to exist, such that an attacker cannot make much use of such a communication)			X	✓
communication with an unauthentic trusted third party (no mechanisms are described in part 2, but all actual implementations shall enforce this, e.g. on the organisational level)	X			✓
manipulation of applications			X	✓
manipulation of keys		X		-
manipulation of parameters			X	✓
manipulation of fraud detection		X		✓
manipulation of the SM handling			X	✓
disclosure of keys	X			✓

Annex B (normative): SM and SM life cycle denomination

The SM referring to that standard shall follow the life cycle defined in this normative annex.

Four different phases in the SM life cycle shall be distinguished:

- IC and SM-manufacturing phase (phase 1);
- application preparation (phase 2);
- SM preparation (issuing) phase (phase 3);
- usage phase (phase 4);
- termination of use (phase 5).

NOTE: This clause is based on ETR 115 [12].

B.1 IC- and SM- manufacturing phase (phase 1)

Phase 1 shall be characterised by:

- the development of the operating system, and the transport of the operating system to the IC manufacturer;
- the implementation of the operating system;
- the production of the IC, and the transport of the IC to the SM manufacturer;
- the production of the SM, and the transport to the SM issuer.

B.2 Application pre preparation (phase 2)

Phase 2 shall be characterised by:

- the allocation of the data structure (e.g. file structure).

Furthermore, there may be the generation of the transport code for the transport of the SM to the user.

B.3 SM preparation (issuing) phase (phase 3)

Phase 3 shall be characterised by:

- the initialisation and the pre-personalisation of the SM, the loading of the application independent data, functions and keys (data related to the TTP);
- the distribution of the SMs to the SM provider.

B.4 Usage phase (phase 4)

Phase 4 shall be characterised by:

- the use of the general SM functions;
- the access to the applications.

The following operations are done under the control of the TTP, it implies the use of cryptographic mechanism to secure this phase:

- the allocation of an application;
- the deletion of an application;
- download of any software in the SM (in an encrypted form).

B.5 Termination of use (phase 5)

Phase 5 shall be characterised by at least one of the following:

- the deletion of a SM application;
- the termination of the use of the IC on the SM.

Annex C (informative): Security targets to the UMC (in usage phase)

C.1 Component description

The UMC is used as prepaid phonecard. It can be used for billing purposes by the user at any terminal, which is accepting the UMC. The main characteristics of a UMC are described in detail in subclause 4.8 "UMC characteristics" in ES 201 209-1 [1]. Moreover in subclause 5.3 of [1], the normal operation of the terminal and the UMC handling are explained.

The main functions, which can be executed with an UMC are described in the table C1:

Table C1: Security targets for the UMC - UMC functions

Functionnality	Calculation of a response
	Input of a challenge
	Counter decrementation
	Reading of counter data
	Reading identification data
	Short number dialling

The product is a memory chip card. TOE is the chip card after the personalisation, i.e. the card contains at least one key and is in usage phase. The UMC shall be in usage phase and it shall remain in this phase (see [12] subclause 4.4).

The TOE can be used for payment at accepting terminals.

Technical suppositions for operation of the TOE are described in ES 201 209-1 [1].

After production of the plain chip card a personalisation needs to be performed. Regarding this personalisation, security requirements of the UMC manufacturer are necessary. After personalisation the UMC is during normal operation carried to whatever area, thus in this phase no special requirements to the environment can be supposed.

C.2 Objects

Objects which need to be protected:

O1	identification area of the UMC
O2	counter area of the UMC
O3	key(s)
O4	challenge
O5	response
O6	algorithm

C.3 Subjects

S1	Terminal / Security Module

C.4 Actions

Defined subjects can perform the following actions at trusted objects:

A1	Read	(R)
A2	Execute/Use	(E)
A3	Decrement	(D)
A4	Write	(W)

C.5 Relation Subjects - Objects - actions

Table C2: Security targets for the UMC - Allowed actions of Subjects at Objects

	S1 Terminal/SM
O1 ID	R
O2 Counter	R/D
O3 Key(s)	E
O4 Challenge	W
O5 Response	R
O6 Algorithm	E

C.6 Threat analysis

The following threats are resulting from to basic threats for IT products. Thus they are given ordered to the four basic categories of threats:

T1	disclosure of key'(s)
T2	disclosure of algorithm
T3	imitation of a genuine identity of a UMC
T4	manipulated readout of a counter
T5	fake of a counter decrement
T6	manaipulation of key(s)
T7	manipulation of the identification area
T8	unauthorised increment of the counter

The UMC shall assist to reach the following security objectives:

SO1	secured and confidential storage of key(s), algorithm and data
SO2	integrity secured transfer of values from the counter in the UMC to a counter in a SM (Includes the secured readout of the counter and integrity secured decrease of the counter)
SO3	secured identification of the UMC

C.7 Security Functions

None of the functionality classes of [2] covers the security functions of the UMC. To resist threats defined in the threat analysis effectively, the UMC is equipped with the security functions, which shall be specified in the following:

SF1: Identification and Authentication (I&A)

The authentication function is realised by a challenge/response mechanism, where the response is a cryptographic parameter after a calculation with the identification parameters, the UMC counter, the challenge and the key as input. As a part of the authentication process, the counter is also authenticated. Details of this mechanism are specific for the different products.

SF2: Access Control (AC)

As the ACs are fixed for all data and algorithms in the memory card. The ACs are usually realised in hardware. It has to be proven that the AC is in accordance with the table of the allowed actions (see table C2).

C.8 Correlation Threats - Security Functions

Table C3 shows the correlation of the security functions against the various threats. The detailed proof of effectiveness is part of the evaluation.

Table C3: Security targets for the UMC - Correlation Threats - Security Functions

	SF1 (I&A)	SF2 (ACs)
T1		X
T2		X
T3	X	
T4	X	
T5	X	
T6		X
T7		X
T8		X

As can be seen from table C3, there is no security function against unauthorised counter decrementation. If anybody has physical access to the UMC, he can decrease the counter. This threat is regarded not very serious, as you usually don't have access to any other UMC belonging to a user and the card issuer is the only party, who benefits from such an attack.

Annex D (informative): Security targets of the personalisation of the UMC

D.1 Component description

Personalisation of the UMC is the responsibility either of the manufacturer or of the card issuer. It is essential that responsibilities should be clearly defined.

In this clause, we consider only the first hypothesis: that personalisation is the responsibility of the manufacturer.

D.2 Objects

O1	UMC
O2	card personalisation data

D.3 Subjects

S1	chip manaufacturer
S2	UMC manufacturer
S3	card issuer

D.4 Actions

Chip manufacturer: provides the UMC manufacturer with the chip.

UMC manufacturer: embeds the chip and personalises it.

Card issuer: provides the UMC manufacturer with the card personalisation data, for example card serial numbers, diversified key(s), etc.

D.5 Threat analysis

During the development and production of UMC there are three types of threat:

T1	disclosure of sensitive personalisation data, for example K_{umc}
T2	disclosure of transport key(s) (if the transport locking code is used)
T3	manipulation of data and programs
T4	unauthorised modification of the personalisation software
T5	receipt of unauthorised personalisation data
T6	unauthorised production of UMC
T7	theft of cards
T8	personalisation of more than one UMC with the same K_{umc} and ID intended for only one card.

D.6 Administrative environment

The manufacturing process shall be carried out in a secure environment that is protected by means of controlled access. Storage and transport of UMC cards shall be physically protected and the chips may be logically protected (transport locking code). Similarly, the assembly process, the embedding process and the destruction of rejects shall all be logged.

D.7 Security Functions

SF1: Identification and Authentication (I&A)

Security-enforcing functions dedicated to I&A provide the means to establish and verify a claimed identity. These functions allow two different services: data-origin authentication and party-to-party authentication. Authentication functions can be provided through a challenge principle based, for example, on key sharing.

- data-origin authentication;
- this security function provides corroboration that the identity of the source of data received is what has been claimed;
- party-to-party authentication;
- this security function may enhance exchange of transport keys, for example between chip manufacturer and UMC manufacturer, system operator and UMC manufacturer.

SF2: Access Control (AC)

Security functions dedicated to access control shall provide protection against unauthorised operations on information or processes. They control the flow of information between users, processes, and objects, and the use of resources by them. They should comprise:

- security management system with procedural directives (linked to security policy);
- physical access control to buildings;
- access control to personalisation equipment;
- design control.

SF3: Accountability

Security functions dedicated to accountability shall provide that relevant information about critical actions performed during the card manufacturing phase be recorded. Thus, each person concerned should be accountable for its own actions. Measures include:

- secure trace file for personalised UMC;
- classification of data, documents and materials.

SF4: Audit

Security functions dedicated to audit shall provide the possibility of detecting and investigating breaches of security by permitting a subsequent security audit. A security audit is an independent review and examination of system records and activities in order to test for the adequacy of system controls so as to ensure compliance with established policy and operational procedures.

The card issuer shall have access to the result of the audit.

SF5: Integrity

Security functions dedicated to integrity shall provide protection against unauthorised modification or deletion of information. Two integrity services are distinguished:

- the integrity of file transfer shall be assumed;
- destruction of unused materials, data and documents.

SF6: Confidentiality

Security functions dedicated to confidentiality of data exchange shall provide protection against unauthorised availability or disclosure of information.

The first means of ensuring confidentiality of data is encryption. Once encrypted, the data are protected against unauthorised modification, because if data are modified after encryption, this will be detected during decryption. Another means is to restrict access to sensitive data so as to prevent unauthorised reading and modification. Measures can include:

- procedure to receive transport key(s) (if used);
- encrypted data file transfer (confidentiality);
- encrypted data file storage;
- secure environment for data file decryption.

D.8 Correlation between Threats and Security Functions

Table D1: Security targets for the UMC Manufacturer - Correlation Threats - Security Functions

	SF1	SF2	SF3	SF4	SF5	SF6
T1	X	X				X
T2	X	X				
T3	X	X	X		X	X
T4	X	X				
T5	X					X
T6	X		X	X		
T7		X				
T8			X	X		

Annex E (informative): Security targets of the Card Management System (CMS)

E.1 Overview of the CMS

E.1.1 Architecture

An overview of the CMS architecture is provided in figure E1. the CMS is constituted mainly by:

- -` the Keys Generation system;
- - the Management of Issued UMCs system;
- - the relevant data Encryption and Transfer System;
- - generation of UMC personalisation data.

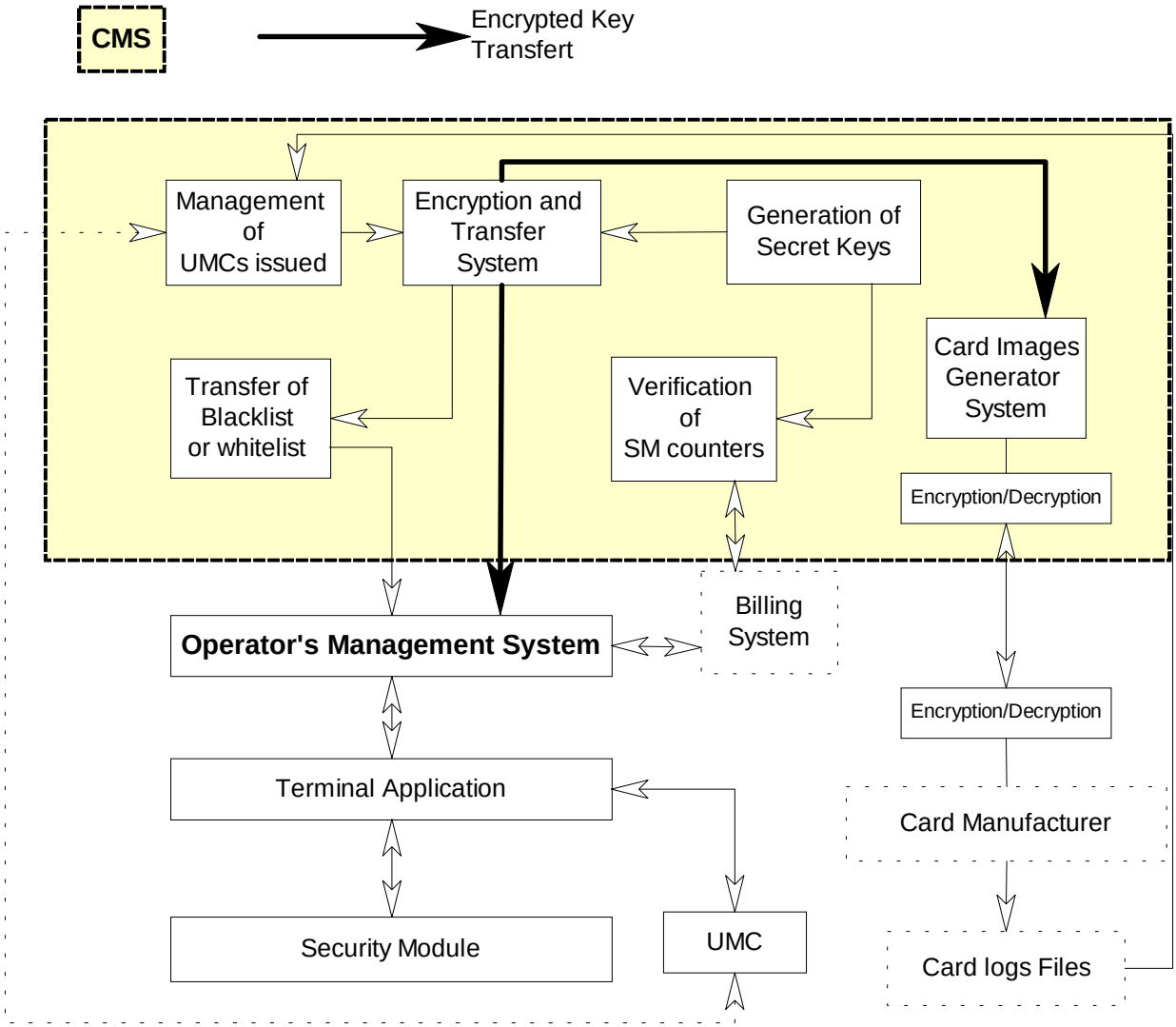


Figure E1: CMS architecture

E.1.2 CMS assets

The system assets contained within the CMS may include:

1) Card Management System (CMS) software;
2) databases containing sensitive information;
3) Secure Device (SD).

The functional assets of the CMS (may) include:

1) generation of keys;
2) encryption of Blacklist and/or keys;
3) reception of K_{TTP} (e.g. in a SD);
4) MAC check of counter records; and verification of billing data;
5) transfer of blacklist and/or keys to Terminal Application through Operator's Management System (OMS);
6) transfer of Keys to UMCs Images Generation device.

The information assets contained within the CMS include:

1) UMCs data and related management files;
2) blacklist and/or Whitelist;
3) billing Information and Counters Records (SM counter);
4) keys download data for SM (Key K_{MAC}, etc...);
5) transfer of interoperability relevant data.

E.1.3 Scope of the security target

This security target focuses upon the Card Management System (CMS).

With regards to synchronous Prepaid Cards Interoperability scheme, the scope of the security target therefore concerns:

1) generation of keys and reception of K_{TTP};
2) billing information and verification of SM Counter Data;
3) encryption and Transfer system of security relevant interoperability data (Keys, blacklist and / or Whitelist,...) to the Operator’s Management System (OMS).

E.2 Threat analysis

This clause describes the key top-level threats to the CMS system.

T1	unauthorized disclosure of Card Issuer data elements
T2	unauthorised access to Card Issuer databases
T3	unauthorized disclosure of Card Issuer data elements from and/or to further entities (K_{TTP} if a SD used)
T4	unauthorized modification of Card Issuer databases (keys, UMCs files, Billing system)v
T5	accidental or malicious modification of the information which associates SMs with Card Management counter records
T6	introduction of unauthorized aliens (e.g. Godzilla) data or functionality into CMS systems by Designers, administrators or third party supplier companies
T7	service denial through deliberate attempts to overload or prevent service delivery through modification of system management, operational or functional information
T8	generation of valid but unauthorized UMCs data elements with intent to defraud Card Issuer and/or Card Issuer partners
T9	unauthorized access to CMS information or functions with intent to defraud Card Issuer, Terminal Operator or Card Personalizer
T10	unauthorized access to CMS information or functions with intent to defraud Card Issuer, Terminal Operator or Card Personalizerunauthorized access to CMS information or functions with intent to defraud Card Issuer, Terminal Operator or Card Personalizer
T11	unauthorized introduction or exchange of sensitive information between the CMS and other systemsunauthorized introduction or exchange of sensitive information between the CMS and other systems

E.3 Security requirements

This clause identifies top-level technical security requirements for the CMS. In addition to these technical requirements, each CMS instantiation will require a system-specific Security Management Organization (SMO) and associated Secure Operating Procedures (SOPs).

As the CMS is system which not fully dedicated to the interoperability of UMC, the security functions described hereafter do not represent mandatory requirements.

SF1: Identification and Authentication (I&A)

CMS security function dedicated to the I&A should provide the means to establish and verify a claimed identity. These functions should cover:

- all individuals or systems which attempt to access the security relevant components of the CMS are required to provide a unique identifier and associated authentication data, before that individual or system is permitted to access into the CMS;
- all CMS-related authentication data, such as passwords, should be regularly changed and traced up within the system;
- all CMS-related security relevant components issued are required to be clearly identified and traced within the CMS system.

SF2: Access Control (AC)

Security functions dedicated to AC should provide protection against unauthorized operations on the CMS. These functions should cover:

- restricted access to the CMS management data and system;
- all unnecessary functionality which may exist within the supporting CMS operating systems and platforms is disabled;
- physical protection of the security relevant components of the CMS shall be provided;
- the CMS network shall be configured such that unrestricted access between the CMS and other networks shall not be allowed, and such that the only permitted connection paths shall be between the CMS network and associated, pre-agreed, client systems if any.

SF3 - Accountability

Security functions dedicated to the accountability should provide that relevant information. These functions should cover:

- any unauthorized attempt to access a security relevant of the CMS system should be recorded for potential further investigation;
- all transfers of sensitive data, including K_{TTP} or Secure Devices (SD), shall be logged and reviewed regularly.

E.4 Correlation between Threats and associated Security requirements

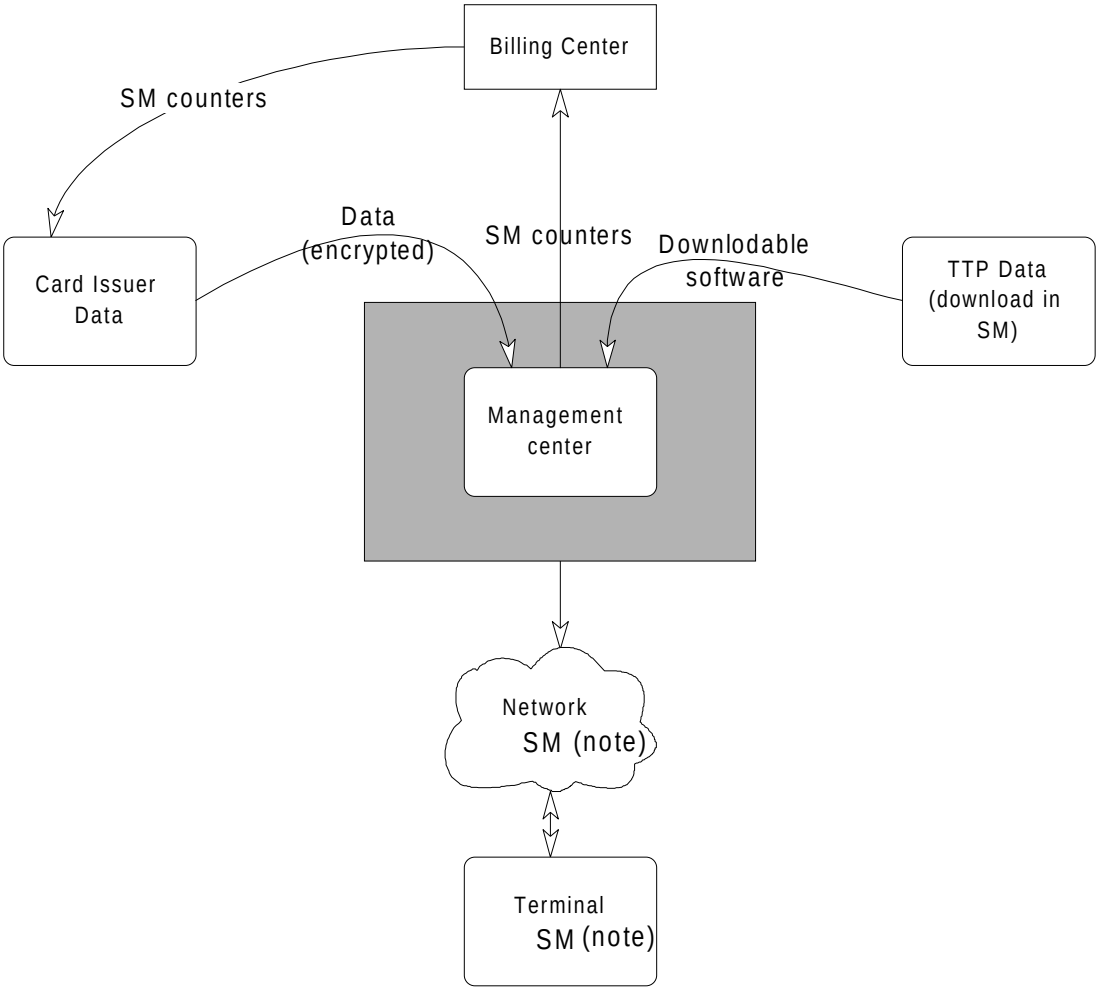
Table E1: Security targets for the CMS - Correlation Threats / Associated Security requirements

	SF1	SF2	SF3
T1	X	X	X
T2	X	X	
T3	X	X	X
T4	X	X	
T5	X	X	
T6	X	X	
T7	X	X	
T8	X	X	X
T9	X	X	
T10			X
T11	X	X	X

Annex F (informative): Security targets for the Operator Management System (OMS)

F.1 Architecture

An overview of the OMS architecture is provided in figure . The OMS communicates with four entities which are: the card issuer, the billing centre, the terminals and the TTP. The main components of the OMS include the SM handling, management of UMC information, UMC Blacklist or Whitelist, the card issuer data and the counter extraction. The SM can be located either in the network either in the terminal. No assumption is made on its location, it shall be specified when necessary.



NOTE: The SM can be located in the network or in the terminal.

Figure F1: OMS Architecture - Security targets for the OMS

F.2 Environment for usage

The OMS is a Central Management System where the terminals are connected via networks. The problem is for a card issuer to ensure that its UMC are correctly handled and the System Operator has to be sure to be paid for a service provided.

F.3 List of objectives - information assets

The information related to a card issuer contained within the OMS include:

- data related to UMC physical IDs, logical organisation of the UMC (counting procedure, identification area, fix number dialling ...);
- rate to charge a communication;
- UMC Blacklist or Whitelist;
- card issuer secret data to be downloaded in the SM;
- counter records (SM counter);
- SM downloadable program code, secured by the TTP.

F.4 Required objectives

The OMS of the System Operator should be subject to the following requirements:

- the system shall be designed and operated to ensure the confidentiality of keys and other protected data;
- the UMC Blacklist or Whitelist are correctly handled;
- the OMS indicates the location of the SM and the list of UMC used on each terminal;
- the OMS acquires the data necessary to the fraud detection.

F.5 Objects

The different objects of the OMS are:

O1	encrypted data provided by the card issuer
O2	encrypted data provided by the TTP
O3	the data used to operate the UMC (included Blacklist/Whitelist, tariff table...)
O4	the unit counter extracted from the SMs

F.6 Subjects

The different subjects of the OMS are:

S1	System Operator

F.7 Actions

A1	load encrypted data provided by the card issuer
A2	load encrypted data provided by the TTP
A3	load data used to handle the UMC
A4	read the SM counters
A5	maintaining a list of SMS IDs (introduce new SM, location etc.)
A6	fraud detection

F.8 Threat analysis

The following threats will be assumed:

T1	disclosure of sensitive data keys, downlodable software
T2	unauthorised modification of sensitive data or SM counters
T3	load unauthentic data to handle UMC (e.g. Blacklist, tariff data)
T4	denial of access to the SM counter
T5	to run the UMC with an invalid UMC management information (e.g. no update of the Blacklist)

F.9 Security Functions

The OMS contains the following Security Functions to resist to the Threats:

SF1	data exchange - secured transmission between the different elements of the OMS
SF2	the card issuer can make some “blind test” (check the Blacklist management)
SF3	the OMS shall provide tools to detect fraudulent usage UMCs
SF4	access control to the OMS

F.10 Correlation Threats - Security Functions

There is no table defined because the Threats and the Security Functions are not precise enough.

Annex G (informative): Security targets for the terminal application

G.1 Objects

O1	software of the terminal application
O2	parameter of the terminal application (including tariff data)
O3	UMC Card data (stored in the terminal)
O4	SM data (responses from the SM stored in the terminal)
O5	internal hardware of the terminal (including SM if located in the terminal)

G.2 Subjects

S1	user
S2	UMC
S3	OMS + Terminal Operator + System Operator + service staff
S4	Security Module (SM)

G.3 Actions

A1	R: Read
A2	E: Execute
A3	W: Write

G.4 Relation Subjects-Objects-Actions

Table G1: Security targets for the terminal - relation Subjects-Objects-Actions

	S1	**S2**	**S3**	**S4**
O1	A2	A2	A2, A3	A2
O2		A1	A1, A3	A1
O3	-	A3	A1	A1
O4	-	-		
O5			A1, A2, A3	A3

G.5 Threat analysis

T1	unauthorised phone calls (e.g. manipulation of terminal software, not authentic card)
T2	manipulation of software, data on the transmission path in the network between the OMS and the terminal application
T3	manipulation of software and data within the terminal application

G.6 Security Functions

As the terminal is considered insecure, no security function are defined. This is up to the System Operator (SO) and Card Issuer (CI) to define in the bilateral agreement (see [1], annex E) to define which security functions are required (e.g. blacklist or collection of data for fraud detection).

Annex H (informative): Initialisation process

H.1 Preamble

Interoperability starts with secret initialisation.

H.1.1 Notation

A and B are system operators, both issue UMC.

Hosting system operator	System operator which own the terminals, the SM and the management system
Hosted system operator	System operator which use the network and the terminal of the hosting system operator.

H.1.2 Principle

The SD is a chip card which is dedicated to initialise a SM. To do so the SD and the SM share a key which is used to initialise an system operator.

The initialisation scheme consists in the encryption of a hosted card issuer secret data according to the hosting system operator specification.

A and B use the UMC active authentication function to check the validity of the UMC.

From here the following case shall be studied: **B is hosted by A**.

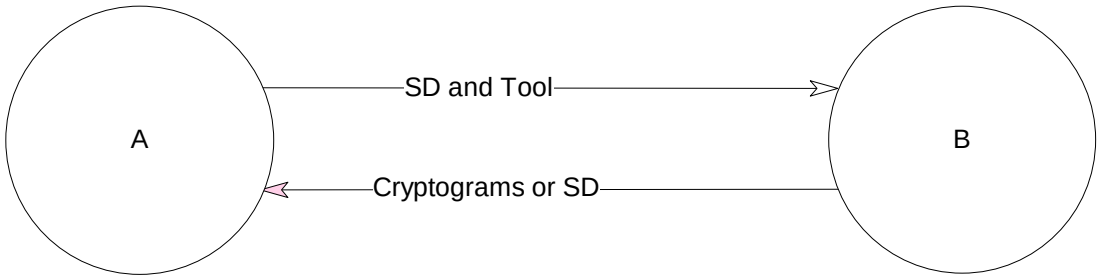
H.2 Secret initialisation

H.2.1 A and B use a symmetric algorithm SD

The K_{load} key is performed with a symmetric algorithm.

H.2.1.1 The tool to operate the SD is provided by another system operator

The scheme exists if A's and B's SM and SD are different ($K_{TTP\ A}$ and $K_{TTP\ B}$ are different and/or the SD interface). B do not want to develop a new tool to operate the foreign SD, it uses A's tool.

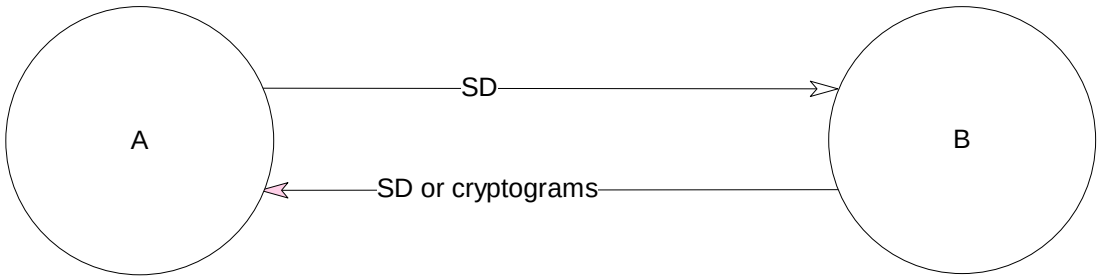


NOTE: B can send to A cryptograms or the SD itself.

Confidence required: SD and tool

H.2.1.2 The tool to operate the SD is self provided by the system operator

The scheme exists if A's and B's SM and SD are different ($K_{TTP\ A}$ and $K_{TTP\ B}$ are different and/or the SD interface).
B develops or modifies a tool to operate the foreign SD.

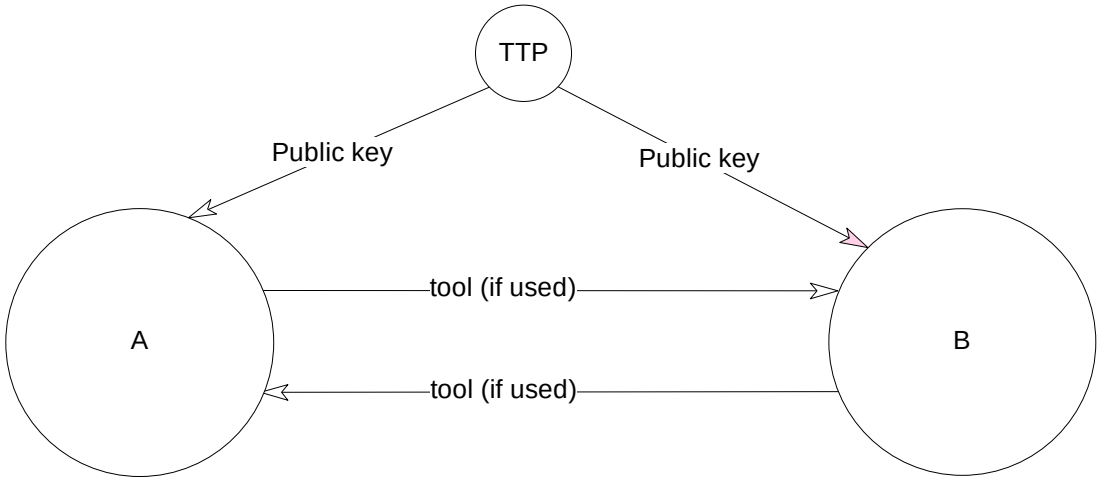


Confidence required: SD

H.2.2 A uses a public key scheme

The K_{load} key is performed with an asymmetric algorithm.

In that case A and B receive the K_{TTP} public key from the TTP. The problem is reduced to the tool exchange: is it developed once or developed by each parties.



Confidence required: tool if used by different system operators.

H.2.3 Data exchanged

The secret data (e.g. keys) are always encrypted. The modification of one cryptogram is easy but normally without any security effect, the only impact is to make the cryptograms unusable. The cryptographic inspection of the cryptograms should be very difficult. It relies on the strength of the crypto algorithm and on the strength of the device which store these data in plain text.

As the SM is the heart of the system, the hosted system operator must have a good confidence. the terminal, the management system are considered transparent.

Problem: exhaustive search of secret data on a specific tool (the hosting system operator knows the cryptograms).

Solution: We can only define a kind of charter between the system operators (including the management system, terminal and the people).

H.2.4 Billing aspect

A has no interest to attempt to the billing counter because he would never be paid for the services provided.

The terminal may waste too much units or money of a card but it is more a matter of customer complain.

The list management is critical because B must have a great confidence in A's list management: in case of UMC blacklisted in B's network but not on A's one, it means that B shall pay for UMC which would have been blocked on its own network. The list management is complicated with the size of memory allotted to the list management.

At the beginning of an application such lists are small and their size shall increase and the total memory allotted to this purpose is limited.

Annex I (informative): Security policy for development, production and personalisation for UMC, SD, SM and TTP

The SM, SD and UMC manufacturer and the TTP should have a security management system with the following elements:

Element	Content
Element 1	Responsibilities of top management Security policy Organisation responsibility of an authority resources representative of the top management Assessment of a security management system by the top management
Element 2	Security management system procedural directives, security planning
Element 3	Contract review
Element 4	Design control (requirements during development)
Element 5	Classification and control of data, documents and materials
Element 6	Purchasing, employment and judgement of subcontractors ,security measures required for procurement
Element 7	Trustworthy personnel, training
Element 8	Audit trail, Handling of materials
Element 9	Destruction of materials, data, documents
Element 10	Date processing security
Element 11	Personalisation
Element 12	External security (constructional arrangement, protection of buildings, entry permission)

Bibliography

The following material, thought not specifically referenced in the body of the present document, gives supporting information.

- EG 201 057 (V1.1.1): "Telecommunications Security ; Trusted Third Parties (TTP) ; Requirements for TTP services".

- D.W. Davies, W.L. Price: "Security for computer networks", Wiley and Sons, 1984.

History

Document history		
V1.1.1	May 1998	Publication

ISBN 2-7437-2176-6
Dépôt légal : Mai 1998