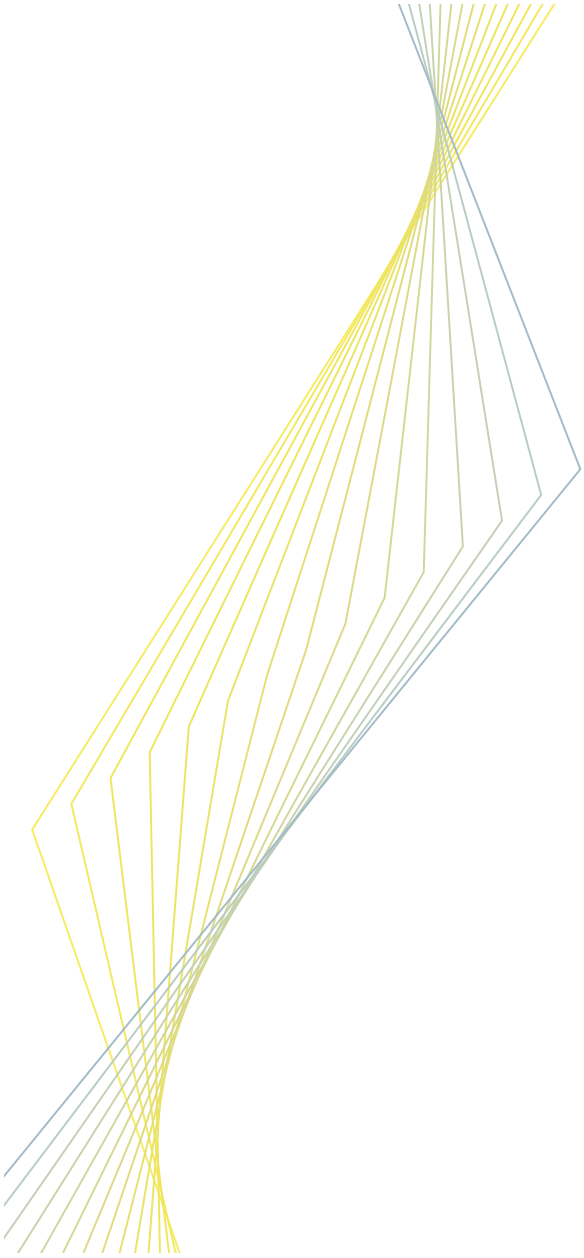
EUROPEAN CENTRAL BANK

ELECTRONIC MONEY SYSTEM SECURITY OBJECTIVES

ACCORDING TO THE COMMON CRITERIA METHODOLOGY

May 2003

EUROPEAN CENTRAL BANK



ELECTRONIC MONEY SYSTEM SECURITY OBJECTIVES

ACCORDING TO THE COMMON CRITERIA METHODOLOGY

May 2003

Address	**Kaiserstrasse 29**
	D-60311 Frankfurt am Main
	Germany
Postal address	**Postfach 16 03 19**
	D-60066 Frankfurt am Main
	Germany
Telephone	**+49 69 1344 0**
Internet	**http://www.ecb.int**
Fax	**+49 69 1344 6000**
Telex	**411 144 ecb d**

ISBN 92-9181-361-3 (print)
ISBN 92-9181-362-1 (online)

Table of contents

Introduction and executive summary

Electronic money (e-money) systems are gradually achieving some level of status as a means of payment in a number of countries. In the light of the possible impact of the development of e-money, in 1998 the Eurosystem issued the "Report on Electronic Money", addressing monetary policy effects, level playing field considerations and regulatory concerns, such as the smooth and efficient functioning of payment systems, confidence in payment instruments, protection of customers and merchants, stability of financial markets and protection against criminal abuse. As part of their oversight responsibility for payment systems, central banks have to ensure that all relevant e-money systems comply with the requirements of the 1998 report.[1]

Given the specific importance of IT security matters in relation to the conduct of an overall assessment of the reliability of e-money systems, on the issue of technical security on the 1998 report was further elaborated. The Eurosystem's investigations resulted in the Electronic Money System Security Objectives (EMSSO) report, which details the Eurosystem's expectations in this field. The EMSSO report contains a comprehensive risk analysis for e-money systems and a list of security objectives that should be fulfilled in order to cover these risks/threats in a given environment. In particular, the analysis provides an overall description of a typical e-money system and highlights the threats and organisational guidelines that arise on the basis of certain assumptions. The security objectives are defined broadly enough to cover both hardware and software-based e-money systems, including the newer server-based initiatives. The EMSSO report benefited from a market consultation in March 2002.

This final EMSSO report, which complements the 1998 report, will be used by the Eurosystem's central banks to assess the overall reliability and technical security of e-money schemes in the euro area. The Eurosystem's security objectives are also designed to level the regulatory playing field for the different schemes. Furthermore, the report could provide market participants with useful input for their own risk and security analyses and for the definition of their security policies.

The risk analysis and the definition/presentation of the security objectives in the EMSSO report are based on the "Common Criteria for Information Technology Security Evaluation (CC)" methodology. This internationally agreed and standardised methodology was selected because it provides a coherent framework for describing e-money systems and related assumptions, threats and organisational aspects and for deriving a definition of security objectives from this description. According to the CC methodology, the drafting process should also cover other steps, such as the definition of security requirements, which would result in the drafting of a Protection Profile and in the definition of evaluation and assurance requirements. However, these additional steps are not addressed in this document.

In Chapter 1, the EMSSO report focuses on several basic concepts, such as the e-money system, electronic value and sub-systems. The e-money system is a mechanism that facilitates payments – generally of limited value – in which e-money can be considered as an electronic surrogate for coins and banknotes. The e-money system is described on the basis of a model with a set of sub-systems through which electronic value (EV) is transferred, under the responsibility of a System Supervisor who monitors the security of EV creation, EV extinguishment and EV circulation within the system. In the context of this report, electronic value is defined as a

1 *See Annex E for the list of minimum requirements of the 1998 Report on Electronic Money.*

monetary value represented by a claim on an EV Issuer, which is: (i) stored on an electronic device; (ii) issued on receipt of funds for an amount not less in value than the monetary value issued; and (iii) accepted as a means of payment by undertakings other than the issuer.[2]

The notion of a sub-system is intentionally flexible, i.e. the model does not impose any restriction on the number of sub-systems that form an e-money system, and a sub-system is defined only by:

- its capacity to send or receive EV amounts;
- the System Supervisor's ability to monitor these amounts.

The sub-systems are capable of generating Reporting Data (RD) and of making this data available (either directly or indirectly via other sub-systems) to the System Supervisor on request, thereby allowing EV exchanges to be traced.

After describing the concepts, in Chapter 2 the EMSSO report defines the main threats related to the unsecured and untrusted environment in which an e-money system usually works and that this report is intended to cover. The operation of an e-money system requires an adequate handling of risks relating to counterfeits, damages and criminal events, which can be translated into main threats. Such threats, if not properly managed, can put issuers, merchants and customers at risk. The main threats against which protection is to be provided are:

- Creation of fake EV: Circumstances in which it might be possible for an attacker to use fake EV, i.e. EV that does not represent an EV Issuer debt.
- Illicit extinguishment of EV: Attacks or incidents that lead to an abnormal and irrevocable EV loss.
- Embezzlement of EV: Attacks in which one actor embezzles EV from its legitimate owner.
- EV theft: Opportunities for an attacker to steal EV.
- Abuse of the e-money system: Use of the e-money system to infringe regulations unrelated to the system.
- Interference with the operation of the e-money system: Accidental or intentional malfunction that may result in the system being totally or partially unavailable.

To counter the above threats, the following security objectives should be met by appropriate technical and organisational action. Further details on these objectives, which are listed below, can be found in Chapter 3 of the report.

- Access control: Unauthorised access to all assets is prohibited, even in the case of a malfunction in monitoring or in secrets management. Each identified actor has a clear set of access rights.
- Assessment: Important players are subject to assessment.
- Atomicity: Transactions are either completed or undone.
- Authentication: EV transactions and monitoring data exchanges are authenticated.
- Availability: The system ensures service availability, even during maintenance of part of the system.
- Commitment and validation: Transactions are conducted and validated under the terms of a commitment between the parties.
- Competence and responsibility: People involved in the system know and follow their own contractual obligations, and have sufficient means, training and information to perform their role.
- Confidentiality: Those assets that must remain confidential are preserved accordingly.
- Cryptography and protocols: State-of-the-art cryptography, protocols and security procedures are required.
- Detection: The system has the capability to:
  - detect abnormal events, including actual or attempted modification of assets and

2 *This definition is taken from Directive 2000/46/EC.*

counterfeiting of transaction attributes;
  - communicate all relevant information which traces these abnormal events to the System Supervisor.
- Identification: An unambiguous identification is required for some components of the e-money system.
- Integrity: The integrity of the assets is preserved, in particular EV amounts.
- Life cycle: State-of-the-art security procedures are used during the life cycle of the EV and sub-systems.
- Limitations: EV amounts are limited during the EV life cycle.
- Non-evaporation: Only authorised sub-systems can perform extinguishment transactions.
- Partition: When a sub-system uses applications other than the e-money application, separation is enforced between the applications.
- Qualification and tests: System components are tested before and/or during operation.
- Reaction: The system provides means to limit or undo the consequences of an abnormal or illicit action.
- Secret management: Correct generation, correct distribution, physical storage protection, limited life span and renewal all preserve the confidentiality and integrity of secrets.
- Security update: A periodic security update is required for all sensitive parts of the system.
- Traceability: The System Supervisor is able to trace and audit all strategic events (as defined in the report). Sub-systems record and keep the data required by the System Supervisor for as long as required. Trace data accurately reflect recorded events.
- Transaction order: Every transaction consists of a set of basic operations executed in a predefined order.
- Trusted location: A physically protected environment is required for sensitive security devices.
- Trusted path: Interaction with the system is achieved through protected communication means.

Additional information is provided in the annexes, such as the rationale for the model, a list of acronyms used in the document, a glossary, and a cross-reference table linking the security objectives with the relevant assumptions, threats and organisational issues.

1 Target of Evaluation description

The intention of this section is to define the Target of Evaluation (TOE), which is the part of the system that is to be evaluated (i.e. to which the security objectives are to be applied).

The TOE is defined in a rather generic manner, by using a high-level model for e-money systems, in order to cover as many e-money systems as possible and to be able to deal with interoperability situations, which are likely to arise in the euro area.

Section 2.1 first introduces the model and the various concepts related to it. Section 2.2 then defines the TOE, which is a subset or part of this model, with clearly defined transactions and actors.

1.1 E-money system: model

This section defines the model and several concepts that will be relied upon in this report. The concepts are first defined formally, then illustrated by a practical example.

The three main elements which make up our e-money system model are EV, EV circulation between sub-systems and supervision. Put together, these elements constitute the core of the e-money system model. The notions of transactions, compensation, EV life cycle and actors then complete this model.

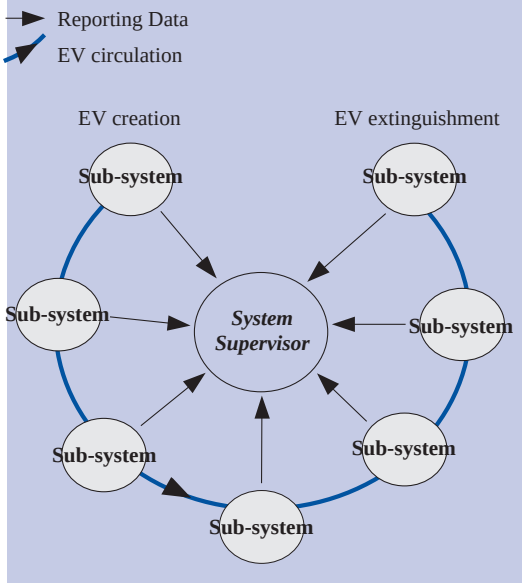
1.1.1 Main concepts of the model

The e-money system is modelled as a set of sub-systems through which the EV specific to the system is transferred, under the responsibility of a System Supervisor[3] who monitors the security of EV creation, EV extinguishment and EV circulation within the system.

EV[4] is a monetary value represented by a claim on an EV Issuer, which is:
- stored on an electronic device;
- issued on receipt of funds for an amount not less in value than the monetary value issued;
- accepted as a means of payment by undertakings other than the issuer.

The EV circulation starts with a first phase called EV creation, and ends with a final phase called EV extinguishment.

Figure 1
Model of an e-money system



This model does not impose any restriction on the number of sub-systems that form an e-money system.

3 *The term "System Supervisor" is used within the specific context of this document and does not relate to the Banking Supervision Authority.*

4 *This definition is taken from Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of business of electronic money institutions.*

The sub-system notion is intentionally flexible. A sub-system is generally defined by its capability to:[5]

- send or receive EV amounts;
- generate Reporting Data (RD);
- make this data available (directly, or indirectly via other sub-systems) to the System Supervisor on request, thereby allowing EV exchanges to be traced.[6]

Furthermore, the System Supervisor is responsible for monitoring the sub-systems.

A sub-system may be able to aggregate EV received into a single amount, the value of which equals the sum of the amounts received. Conversely, the EV amount stored in a sub-system may be broken into smaller amounts, the sum of which equals the value of the EV amount stored.

1.1.2 Examples of e-money systems

The general model is in principle applicable to any type of e-money system, whether card-based or software-based (including server-based/network-based types). An example of both types is illustrated below.

Card-based system

In a card-based system, the sub-systems which participate in the EV flow generally consist of four entities or functions: a loading agent, a customer, a merchant and a collecting agent. The loading and collecting agents are banks participating in the system and the customer uses a smart card to pay at the terminal of the merchant. The customer's purse (the smart card) is a simple, stand-alone sub-system, while the point-of-sale (POS) terminals and the central information systems to which they are connected constitute a more complex sub-system.

In this example, there is a central entity which issues EV and operates as a bookkeeping entity to which the creation and extinguishment of EV is reported via Accounting Data (AD)[7].

5 The sub-systems are also subject to other restrictions that will be explained in the section entitled "Transactions".

6 Sub-systems need only have the capability to do this upon request from the System Supervisor; there is no requirement to have full traceability at all times.

7 AD are data sent to the EV Issuer upon EV creation and extinguishment.

Figure 2

Example of a card-based system

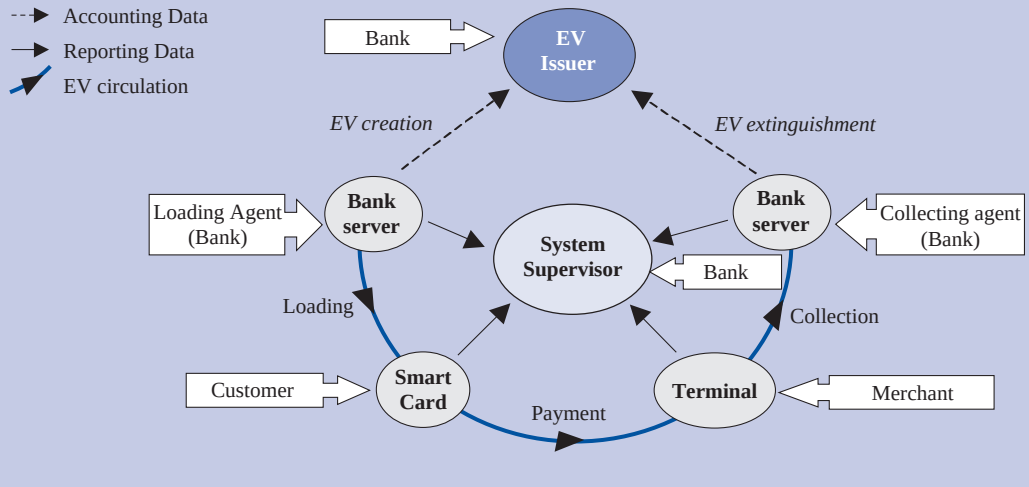
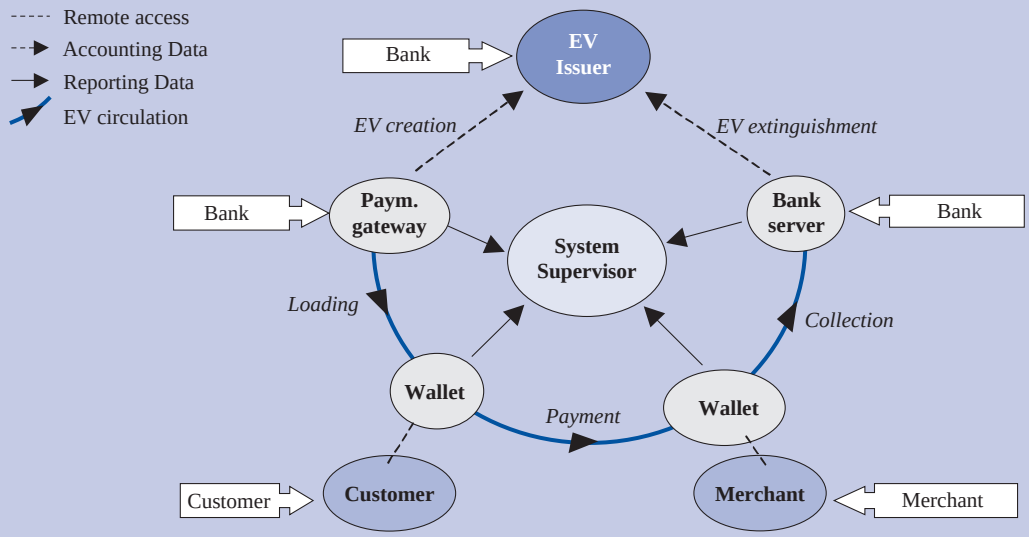


Figure 3

Example of a server-based system



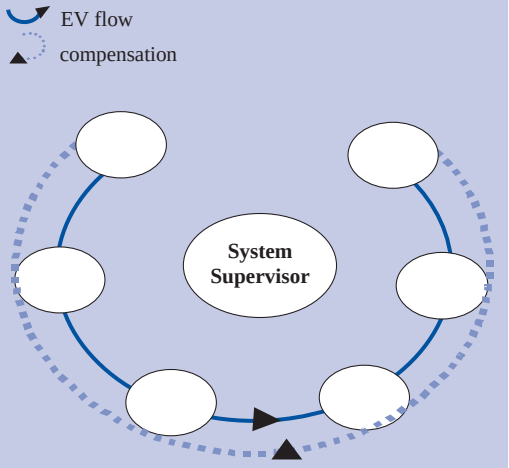
Server-based system

In a server-based system, the customer and the merchant do not keep the EV in devices held in their possession. The EV is stored in customer and merchant accounts on servers accessed via the internet. The customer and merchant sub-systems are therefore software processes running on the central server.

The general model also covers these types of e-money systems, in view of the specificity of the use of centrally stored accounts.

Figure 4

Flows of EV and compensation



1.1.3 Additional concepts: compensation, transactions, EV life cycle, roles, actors, and quasi-actors

Compensation (CP)

Typically, seen as a model, an e-money system has two flows, i.e. the flow of EV (the solid line from left to right in Figure 4) and the flow of value to compensate the EV (the dotted line from right to left).

The obligation to deliver CP may be fulfilled either immediately or at some prior point in the past or in the future. In the case of goods or services, the related amount might not be known from the start and may be defined, by joint agreement, in the course of the provision of these goods or services.

Transactions

A transaction is defined as a flow of EV.

The following basic operations and attributes constitute the minimum characteristics which must be present for transactions:

Basic operations constituting EV transactions[8]:

- initialisation;
- EV debiting;
- EV crediting;
- closure.

Attributes characterising a transaction:

- the transaction type (payment, loading, collection, etc.);
- the identifier of the sub-system from which EV is debited (hereafter "debited sub-system");
- the identifier of the sub-system to which EV is credited (hereafter "credited sub-system");
- the EV amount exchanged (debited and credited);[9]
- the existence of CP.

The RD generated upon request to allow the System Supervisor to monitor the system include at least the transaction attributes listed above.

Two types of transactions can be distinguished:

- A transaction which involves an interaction between flows of both exchanges of EV and CP is called a transaction with CP.

  Transactions with CP are generated against a flow of value in return. This may consist of a flow of fiduciary or scriptural money as well as of goods or services. A purchase transaction based on an e-money payment is an example of a transaction with CP.

- A transaction without this interaction between the two flows is called a transaction without CP.

  Transactions without CP involve an EV circulation that is not balanced by a corresponding flow of value. Recycling of EV is a typical example of a transaction without CP.

The table below presents, as a rough guide, a non-exhaustive list of the types of transactions that can occur in e-money systems:

Table 1

Examples of transactions in an e-money system

Transaction type	CP	Short description
Supply with creation	With CP	Supplies a loading device with EV
Loading	With CP	Loads stocked EV into a device
Loading with creation	With CP	Loads EV into a device without any need for the EV to have been previously supplied and stocked
Refund[10]	With CP	Unloads all the EV stored in a device
Payment	With CP	Pays for goods or services with EV stored in a device
Collection with extinguishment	With CP	Unloads and destroys EV received in payment for goods or services
Collection	With CP	Unloads EV received in payment for goods or services
Presentation with extinguishment	With CP	Redeems and destroys collected EV
Recycling	Without CP	Modifies collected EV so that it can be loaded into devices
Cancellation of payment transaction	With CP	Reloads paid EV

8 *Elementary operations are executed sequentially. No assumption is made about their order, other than those explicitly stated.*
9 *The EV amounts debited and credited are equal.*
10 *This refers to an e-money balance refund.*

A particular specification of the model is that the System Supervisor[11] must be able to monitor transactions between two sub-systems. Transactions inside a sub-system are not monitored by the system supervisor. Sub-systems must be defined so that flows with compensation are made outside of these sub-systems.

In an e-money system conforming to the model, the EV amount created is equal to the sum of the extinguished EV amount and the EV amount in circulation. If more EV is extinguished than the amount created, false EV is introduced into the system. One role of supervision is to try to detect such a situation; observing all transactions with compensation makes it easier to perform such supervision.

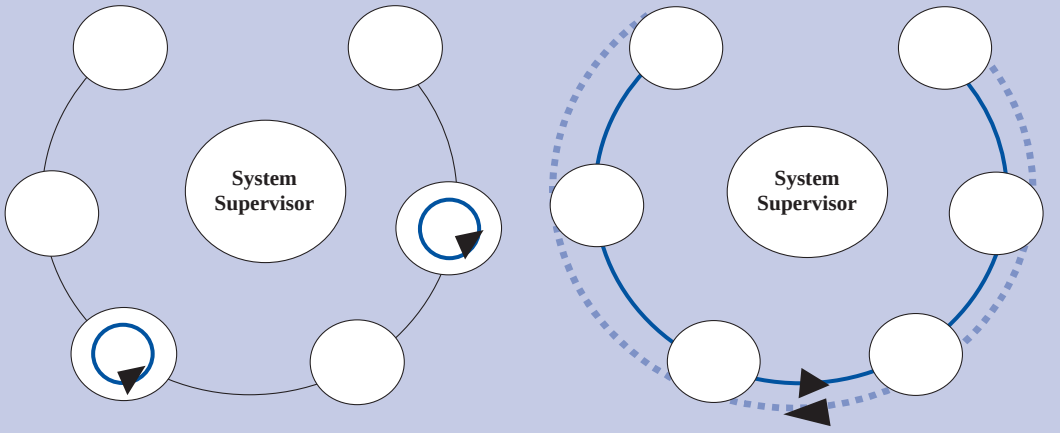
EV circulates inside a sub-system via transactions without CP. Generally, EV circulates between two sub-systems via transactions with CP.[12]

11 The existence of an obligation for the player credited to deliver, either immediately or later, represents a CP to the player debited, i.e. for every transaction with CP, a contractual commitment relates the CP to the exchanged EV amount.

12 Depending on the organisation of the e-money system, transactions between two sub-systems may also exist without CP.

Figure 5

Transactions inside and outside of sub-systems



EV life cycle

In the e-money system, the EV life cycle moves through the following EV states:

1. initial (or source) state, in which EV is injected in the system;

2. one or more active states, in which EV remains in the system;

3. final (or sink) state, in which EV is drained from the system.

The EV life cycle evolves through three state changes: creation, circulation and extinguishment, each of which is associated with a transaction.

- *EV creation*

  EV is created via specific transactions with CP, which include two additional basic operations:

– creation of an EV amount in the debited sub-system;[13]

– transmission, to a player called the EV Issuer, of AD, which report the EV creation and initiate the obligation of the actor whose sub-system created the EV to deliver an equivalent amount (i.e. the CP) to the EV Issuer.

  With this state change, EV enters the system and reaches an active state.

- *EV circulation*

  EV circulates inside a sub-system (via transactions without CP) and between two sub-systems via transactions with CP.

  With this state change, EV moves between two active states.

- *EV extinguishment*

  EV is extinguished via specific transactions with CP, which include two additional basic operations:

– extinguishment of an EV amount in the credited sub-system;

– transmission to the EV Issuer of AD, which report the EV extinguishment and give effect to the obligation for the EV Issuer to deliver an equivalent CP amount to the player whose sub-system extinguished EV.

  With this state change, EV leaves the system.

  Throughout the remainder of this document, transactions do not include EV creation or extinguishment unless this is explicitly stated.

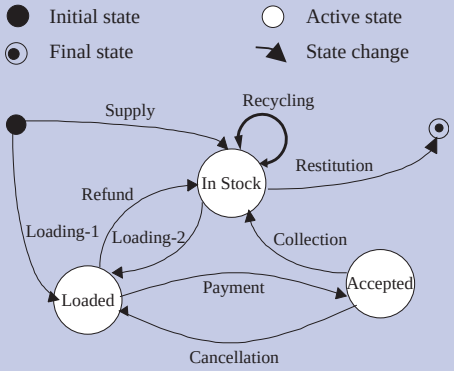
  Figure 6 describes, as a rough guide, the EV life cycle in an e-money system, i.e. the transitions from one state to another resulting from transactions with CP typical of an e-money system. The initial state is the creation of EV, after which this is loaded on the customer's purse (i.e. on a smart card or computer memory). This loading may take place directly from the issuer to the customer or, alternatively, through a bank or Electronic Money Institution (ELMI; as defined in Directive 2000/46/EC) where the EV may be kept in stock before being loaded on the purse. The customer can decide either to make payments with the EV or to refund the EV to the issuer. A payment may also be

13 The debited sub-system is the sub-system which will be debited. For example, in a card-based system, the first debited sub-system is the loading agent. In a loading transaction, the loading agent is debited and the purse is credited.

cancelled, after which the EV is transferred back to the purse. The acquiring bank or ELMI ultimately collects the EV and either keeps it in stock to recycle and reload on a purse or else extinguishes it and thereby completes its life cycle.

Figure 6

Different EV states in an e-money system



Transaction	State change
Supply	*EV creation*
Loading-1	*EV creation*
Loading-2	*EV circulation*
Refund	*EV circulation*
Payment	*EV circulation*
Cancellation	*EV circulation*
Collection	*EV circulation*
Recycling	*EV circulation*
Restitution	*EV extinguishment*

Roles, actors, quasi-actors

Setting objectives for an e-money system requires the definition of a general security framework, which includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

In this report this challenge is addressed by allocating responsibility to those who can most efficiently reduce the risk: system administrators and operators.

The model takes into account all players that are relevant for security and grants each a certain trust level. The co-operation of all players involved in the system is essential for globally effective security.

A player having responsibility[14] for a sub-system is referred to in this document as an actor. The model defines the responsibilities of the different actors, each being responsible for a sub-system in the EV circulation. An actor is directly involved in the exchange of EV (e.g. EV Issuer, Loading Agent, etc.).

A player that is not responsible for a sub-system is defined as a quasi-actor. A quasi-actor does not interact directly in the exchange of EV (e.g. IT provider, etc.).

Different roles for actors and quasi-actors are distinguished. The concept of role is related to players' responsibilities. Their respective roles depend on skills, business objectives and the level of risk that they assume. A specific task and a particular trust level are associated with each role.

The roles defined in this report are Administrator, Operator and User:

– Administrator

  The Administrator is responsible for defining and managing the overall security of the e-money system. This means defining the policy statement, identifying risks, selecting security controls and managing the implementation and operation thereof. Generally the Administrator bears all losses of the system and it is assumed that relevant legislation applies strict requirements to Administrators, for example as regards the company's activities, its financial stability, recruitment policy, accounting practices, access to its premises, access to data and data processing. Main risks incurred by an Administrator could be: i) liquidity risks[15]; ii) compliance risks[16] and iii) reputational risks[17]. The Administrator enjoys a high trust level because he bears the ultimate responsibility for security.

14 The player's responsibility for a sub-system implies that the he has control over, and takes care of, the sub-system concerned.

15 Liquidity risk refers to the risk that the institution is temporarily unable to meet its payment obligations.

16 Compliance risk refers to the risk associated with non-compliance with laws, rules, regulations, prescribed practices or ethical standards.

17 Reputation risk refers to the risk that the reputation of an institution might deteriorate following specific events.

– Operator

The Operator participates in implementing and operating the security of the e-money system. Generally the operator is bound to an Administrator by contractual obligations. Moreover an Operator must comply with relevant legislation and best practices, requirements that, although similar to those which apply to an Administrator, are less stringent. Main risks incurred by an Operator could be: i) operational risks[18]; ii) compliance risks and; iii) reputational risks. He enjoys a moderate trust level, because the operator is responsible for security implementation under the Administrator's co-ordination.

– User

A User is a customer of the e-money system contractually bound to an Operator. The contract does not require that the User implements procedures which contribute to technical security. However, it does require that he/she uses approved devices and follows the right security procedures. Main risks incurred by Users could be: i) frauds in EV transactions; ii) fraud in EV storage and iii) privacy breaches. To ensure simple, friendly and cost effective system usability, only a few, user-friendly security obligations should be assigned to the User. As a result, Users enjoy a low trust level, leaving the main security-related management and operating tasks to Administrators and Operators.

Thus, the trust level granted to Administrators is greater than that granted to Operators, which in turn is greater than that granted to Users.

When a player subcontracts part of his activity in the e-money system, he passes the relevant e-money system obligations on to his subcontractor.

A player may have more than one role in relation to the same device, depending on the transaction(s) being performed. In every instance, the player enjoys the trust level corresponding to the role he plays at a given time (i.e. the player's trust level must be consistent with his role at all times).

All roles are carried out by identified players, with the possible exception of the EV Holder, who can remain anonymous.

The tables below present, as a rough guide, a non-exhaustive list of actors and quasi-actors, together with their typical roles in card-based and software-based systems. A player may incorporate several actors/roles, e.g. a player may be both an EV Issuer (and play the role of Administrator) and an IT Provider (and enjoy the trust level of Operator).

Table 2

Examples of players in a card-based e-money system

Actor	Role	Short description
EV Issuer	Administrator	Issues and guarantees EV
Loading Agent	Operator	Loads EV onto a device
Acquirer	Operator	Collects EV from Service Providers
EV Holder (Purse Holder)	User	Pays in EV through a device (Customer)
Service Provider (Merchant)	User	Accepts payments in EV (Merchant)
Quasi-actors	**Role**	**Short description**
System Supervisor	Administrator	Monitors the flow of EV
IT Provider	Operator	Provides IT infrastructure to the e-money system

18 *Operational risk refers to the risk that deficiencies in internal controls and information systems might result in unexpected losses.*

Table 3

Examples of players in a software-based e-money system (see also Figure 3)

Actor	Role	Brief description
EV Issuer	Administrator	Issues and guarantees EV
Loading Agent	Operator	Loads EV onto a device
Acquirer	Operator	Collects EV from Service Providers
EV Holder (Customer account)	Operator	Pays in EV through its account (Customer)
Service Provider (Merchant account)	Operator	Accepts EV payments in its account (Merchant)
Quasi-actors	**Role**	**Short description**
System Supervisor	Administrator	Monitors the flow of EV
IT Provider	Operator	Provides IT infrastructure to the e-money system
Customer	(outside of the TOE)	The Customer accesses his/her account from outside the system
Merchant	(outside of the TOE)	The Merchant accesses his/her account from outside the system

Generally, the IT Provider provides the actors with a functional e-money system, i.e. he provides the Information Technologies (IT) for all of the sub-systems, especially the Purse Holder's device application.

The System Supervisor and the IT Provider are quasi-actors, as they are not responsible for sub-systems through which EV circulates. Nevertheless, the System Supervisor enjoys an Administrator trust level, and the IT Provider an Operator trust level.

1.1.4 Interoperability of two e-money systems

This section explains how to apply the model defined above in cases where several e-money systems interoperate. Two possible cases are considered: composition of systems, and sharing of a sub-system between e-money systems.

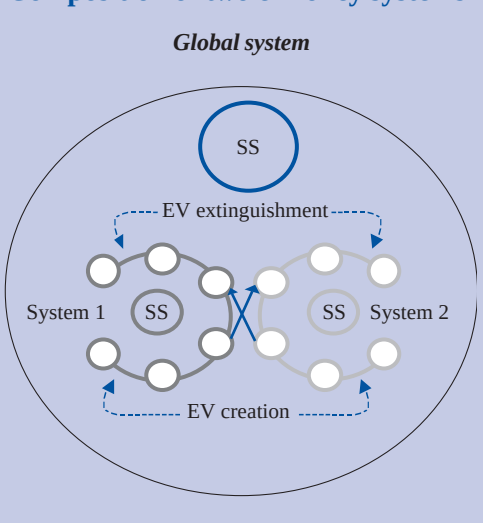
Composition of two e-money systems

In a situation where EV circulates between several sub-systems which belong to different e-money systems, the set of all sub-systems belonging to each e-money system should be regarded as another e-money system under the responsibility of a System Supervisor.

Thus, this situation is covered by the model and will not be mentioned further in this document.

Figure 7

Composition of two e-money systems



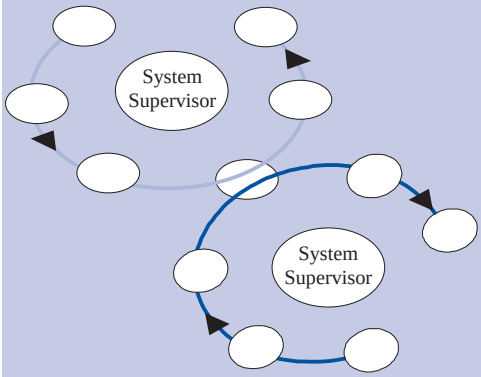
When there is commercial interoperability between several e-money systems, which all comply with the definition given in this EMSSO, the interoperable elements of the systems constitute another e-money system compliant with this EMSSO only if there is a "global" System Supervisor who monitors the security of all EV. In practice, the System Supervisors could carry out "global" supervision jointly, either on a co-operative basis or by mutual acceptance of an appropriate contractual agreement.

Sharing of a sub-system

A sub-system may be shared with one or several other systems, not all of which need necessarily be e-money systems. In such circumstances, the shared sub-system is regarded as any other sub-system, regardless of the other system(s) in which it takes part.

For example, the terminal infrastructure could be shared by two or more different card-based e-money systems that use the same technology but do not share the EV.[19]

Figure 8
Shared sub-system



1.2 Target Of Evaluation

The Target Of Evaluation (TOE) is generally defined as the part of the system that will be evaluated. The definition of the Target Of Evaluation is based on the e-money system as elaborated in the previous section.

According to the Common Criteria, the elements that are not part of the TOE (but are necessary to the TOE to satisfy its security objectives) are called the TOE environment. For evaluation, the TOE must be run in an environment that is compliant with the security objectives for the environment.

1.2.1 Elements that are part of the TOE

Model

The model, as defined in the previous section, is part of the TOE:

- Sub-systems
- EV circulation[20]
- RD flows and system supervision

A sub-system can be composed of one or more hardware and/or software device(s).

For each device in each sub-system, the TOE includes the following phases: initialisation (including the personalisation and activation of the device), operation and termination.

Several kinds of security devices can be identified:

- the security module of the servers that store and process sensitive data relating to the whole e-money system (e.g. personal data, secrets) which must be kept secure;
- the devices that store and process sensitive data which relate to only one sub-system (e.g. derived keys);
- the security enclosures of intermediary devices, such as manned or self-service terminals, that store and process sensitive data which may relate to the whole e-money system or to only one sub-system.

Transactions

The TOE comprises the following transactions:

- creation;
- loading;
- payment;
- collection;
- refund;
- exinguishment.

19 *Interoperability with shared sub-systems may be achieved by defining the security and functional aspects of the sub-systems. For example, the Common Electronic Purse Standards (CEPS) specifications describe the technical (functional) interoperability requirements for sub-systems of card-based systems.*

20 *Including the links between the sub-systems.*

Actors and quasi-actors

The TOE includes the following actors/quasi-actors:

- the Loading Agent;
- the Acquirer;
- the EV Holder;
- the Service Provider;
- the System Supervisor;
- the EV Issuer;
- the IT Provider.

1.2.2 Elements that are outside the TOE

In general, all aspects that are not in the TOE are part of the TOE environment.

System development and manufacturing (before EV creation), together with the clearing and settlement procedures (which take place after EV extinguishment), are outside the scope of the TOE, and are also not considered part of the environment. Development and manufacturing may be covered by dedicated PPs.

The compensation flows are not part of the TOE.

2 TOE security environment

This section aims to describe the TOE security environment, which, as defined in the Common Criteria[21], describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed.

The TOE security environment description includes:

- a statement of assumptions that are to be met by the TOE environment in order for the TOE to be considered secure. This statement can be accepted as axiomatic for the TOE evaluation.

- a statement of threats to the security of the assets, identifying all the threats perceived by the security analysis as relevant to the TOE.

  The CC characterise a threat in terms of a threat agent, a presumed attack method, any vulnerabilities that form the foundation for the attack, and identification of the asset under attack. An assessment of risks to security would qualify each threat with an assessment of the likelihood of such a threat developing into an actual attack, the likelihood of such an attack proving successful, and the consequences of any damage that may result.

- a statement of applicable organisational security policies, identifying relevant policies and rules.

In order to establish the TOE security environment the following have to be taken into account: the TOE physical environment, the assets requiring protection by the elements of the TOE to which security requirements or policies will apply and the TOE purpose, which would address the product type and the intended usage of the TOE.

The assets to be protected are:

- all hardware and software that are related to the TOE Security Function (TSF) (e.g. chip of a smart card);

- data used by the end-user (User data)[22] (data for the normal operation of the system):
  - the data which result in EV creation and the data which result from its extinguishment;
    For example, these could be the data relating to a request for authorisation to create EV in real time while loading an e-money system; they could also be the data that define, within a sub-system dedicated to EV creation, the terms and conditions applying to supplying EV to a loading sub-system.

  - the attributes of a transaction, especially the EV exchanged between two sub-systems and stored in a sub-system;

  - the Accounting Data (AD);

  - the parameters of the sub-systems, including access data where these are relevant;
    These are the data that define the limits within that a device operates (for example, the frequency of a periodic process or limits such as the maximum and minimum amounts). Access data allows access to the sub-system (e.g. identification data);

21 *Source: Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model (1998), paragraph 120.*

22 *Source: Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model (1998), Paragraph 71: Data created by and for the User that does not affect the operation of the TSF.*

  - the System Supervisor information.
    These are the data obtained from RD processing and centralised by the System Supervisor, some of which might be sensitive in terms of a malicious or excessive use of the system;

- TSF data[23] (data for security mechanisms):
  - the RD intended for the System Supervisor;
  - the secrets.
    Secrets refers to cryptographic keys, passwords, authentication data, etc.

2.1 Assumptions

Assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used. This includes the following:

- information about the intended usage of the TOE, including such aspects as the intended application, potential asset value and possible limitations of use;
- information about the environment of use of the TOE, including physical, personnel and connectivity aspects.

The following assumptions are made:

- All actors and quasi-actors know and fulfil their own contractual obligations (as well as their reciprocal obligations) with regard to regulations, finances and security. [A.Responsibility]
  For example, the card-based system is not required to protect the Purse Holder against theft of his card. A contract describes the Purse Holder's obligations and benefits.
- All actors and quasi-actors have sufficient means, training and information to perform their functions. [A.Competence]
  This heading would typically include documentation (specifications, user manual, maintenance manual, operational rules, etc.), regular updates of the documentation, regular training and regular drills simulating exceptional events.
- When a sub-system under the responsibility of an Administrator or System Supervisor includes security devices, those devices are located in a physically protected (or trusted) environment. [A.Trusted_Location]
- RD accurately reflect transactions with CP. AD accurately reflect transactions with EV creation or extinguishment. [A.Data]
  Coherence is required between the various data relating to a single event in the system. It is assumed that specific security measures enforce coherence between transaction data and corresponding RD and AD.
- All security relevant events within a sub-system are traced.[24] [A.Log]

2.2 Threats

This section describes the threats to the assets against which specific protection within the TOE or its environment is required. Note that not all possible threats that may be encountered in the environment need to be listed, only those that are relevant for secure TOE operation.

2.2.1 Threat agents

The e-money system must protect itself against all types of attackers, regardless of whether they are staff, users or parties external to the system.

23 Source: Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model (1998), Paragraph 68: Data created by and for the TOE that might affect the operation of the TOE.

24 The Organisational Security Policies (Section 2.3) cover the monitoring of all relevant events taking place between sub-systems.

Attackers fall into four classes, according to their objectives:

- swindlers who attempt to penetrate the system or to misuse some of its functions for financial profit;
- vandals, saboteurs or, in an extreme case, terrorists who attempt to destroy all or part of the system;
- hackers who attempt to demonstrate their know-how with regard to the security of the system;
- those who misuse the system in order to facilitate the commission of illegal acts;

The e-money system must also protect itself against inadvertent malfunctioning as a result of carelessness.

2.2.2 Threats list

Creation of fake EV

This category covers all circumstances in which it might be possible for an attacker to obtain CP in exchange for fake EV, i.e. EV that does not represent an EV Issuer debt.

Attacks in this category resort to classical methods such as forgery (fake amounts of EV), illicit repudiation (illicit denial of a transaction, or part of a transaction, with the intention of being improperly credited with EV as a result).
These threats directly affect the financial equilibrium of the EV Issuer.

Creation of fake EV can result from the following:

- unauthorised third parties gaining knowledge of secrets of the sub-system; [T.Disclosure_Creat]
- modification of transaction attributes, AD and data related to EV creation and extinguishment, or secrets; [T.Modification_Creat]
- the usurpation of another's privileges through the misuse of secrets; [T.Usurpation_Creat]
- the creation of fake transactions by duplication of authentic attributes or authentic AD, duplication of parameters of a sub-system, or duplication of data relating to EV creation or extinguishment extracted from an authentic transaction. Similarly, the creation of fake transactions with false attributes, false AD, or false data relating to EV creation or extinguishment; [T.Counterfeiting_Creat]
- a player's illicit denial of his participation in all or part of a transaction, if accepted (e.g. A quasi-actor's illicit denial of initiation of the transaction). [T.Repudiation_Extin]

Illicit extinguishment of EV

This category covers all attacks or incidents that lead to an abnormal[25] and irrevocable EV loss.

These attacks benefit the EV Issuer by reducing his debt, but constitute a major threat to the credibility of the system and can lead to numerous disputes.
Attacks perpetrated by criminals rely on logical destruction (erasure of programs, viruses, scrambling), forgery (creation of fake amounts of EV).

Illicit extinguishment of EV can result from the following:

- unauthorised third parties gaining knowledge of sub-system secrets; [T.Disclosure_Extin]
- the modification of transaction attributes, AD, data related to EV creation and extinguishment, or secrets; [T.Modification_Extin]
- the usurpation of another's privileges through the misuse of secrets; [T.Usurpation_Extin]
- the creation of fake transactions by duplication of authentic attributes or authentic AD, duplication of parameters of

25 *As opposed to natural EV losses, which would result from the accidental loss or destruction of cards.*

a sub-system, or duplication of data relating to EV creation or extinguishment extracted from an authentic transaction. Similarly, the creation of fake transactions with false attributes, false AD, or false data relating to EV creation or extinguishment. [T.Counterfeiting_Extin]

Embezzlement of EV

This category covers all attacks in which one actor embezzles EV from its legitimate owner.

These attacks do not affect the financial equilibrium of the EV Issuer.
Actors perpetrate attacks in the system with malicious intent to defraud. They resort to substitution, diversion, or the use of covert communication channels in the system.

Embezzlement of EV can result from the following:

– transferring, during a transaction with CP, an EV amount differing from the amount agreed in the contractual commitment; [T.Modification_Embez]
– repeating an authentic transaction without any contractual commitment other than that of the original transaction. [T.Replay_Embez]

EV theft

This category covers all opportunities for an attacker to steal EV.[26]

These attacks do not affect the EV Issuer's financial equilibrium.
Attacks result in transactions in which the contractual commitment with regard to CP is not honoured. They resort to swindling when the transaction is being carried out.

EV theft can result from the following:

– the illicit modification of transaction attributes, AD, data related to EV creation and extinguishment or secrets; [T.Modification_Theft]
– the usurpation of another's privileges through the misuse of secrets. [T.Usurpation_Theft]

Abuse of the e-money system

This category arises from the use of the e-money system for the purposes of infringing regulations unrelated to the system.

These attacks do not affect the EV Issuer's financial equilibrium or the EV/CP equilibrium of transactions.
Examples of such threats are money laundering, the withdrawal of capital and breaches of privacy.

Abuse of the e-money system can result from the following:

– the use of RD or System Supervisor information for purposes other than monitoring the e-money system, or unauthorised third parties gaining knowledge of sub-system secrets; [T.Disclosure_Abuse]
– the illicit modification of sub-systems parameters, System Supervisor information or a secret; [T.Modification_Abuse]
– the usurpation of another's privileges through the misuse of secrets. [T.Usurpation_Abuse]

26 *Theft of EV indicates that, during a communication, the EV is routed to a place unknown to the User. Theft could be compared with EV embezzlement, but in the latter event the EV is routed to a place known to the User, e.g. an internet site which does not deliver the goods/services required.*

Interference with the operation of the e-money system

This category covers accidental or intentional malfunction that may result in the system being totally or partly unavailable.

Such malfunction may result from an actor unwittingly failing to comply with e-money system regulations, or from a terrorist attempting to harm the system.
Terrorists could resort to logical or physical destruction, to espionage and to disclosure of confidential data.

Interference with the operation of the e-money system can result from the following:

- unauthorised third parties gaining knowledge of secrets of the sub-system; [T.Disclosure_Malfunc]
- the modification of all or part of the system (especially of an asset), of a sub-system's parameters, of RD or System Supervisor information or of a secret; [T.Modification_Malfunc]
- the usurpation of another's privileges through the misuse of secrets; [T.Usurpation_Malfunc]
- late arrival of RD. [T.TimeLimits_Malfunc]

2.3 Organisational security policies (OSPs)

Organisational security policies (OSPs) are described in the cc framework as security rules, procedures, practices and guidelines with that the TOE must comply:

- Supervision of the security of the TOE detects attempts and occurrences of malfunction in the TOE, whether or not these are intentional. [OSP.Detection]
- Supervision of the security of the TOE is used to define actions to limit or suppress the effects of a detected or suspected malfunction (intentional or not). [OSP.Reaction]
- The e-money system security events listed hereunder are recorded in order that they can be traced to their source [OSP.Log]:
  - generation of secrets;
  - revocation of secrets;
  - renewal of secrets;
  - initialisation of sub-system parameters;
  - modification of sub-system parameters;
  - initialisation and modification of the parameters related to EV creation and extinguishment.
- The security architecture of the TOE is based on standardised, publicly known and extensively reviewed, state-of-the-art cryptographic algorithms and cryptographic key management. The TOE does not use cryptographic algorithms that must remain confidential for security reasons. The Strength of Function (SOF[27]) for the use of cryptography must be high. [OSP.Crypto]
- The communication architecture of the TOE is based on standardised protocols and security procedures. [OSP.Protocol]
- Hardware devices, software and organisational procedures have passed functional qualification tests and hardware security tests. [OSP.Qualification]
- For every transaction with CP, a commitment relates the CP to the EV amount exchanged. The terms of this commitment are known to both parties before the initialisation of the transaction. [OSP.Commitment]
- Every transaction with CP is validated by both parties. The validation procedure complies with the terms of the commitment and both parties take note of the commitment prior to initialisation of any transaction. [OSP.Validation]
- Every transaction with CP can be recorded so that each of the parties can check all relevant details a posteriori. Both parties are aware of how to check a transaction. [OSP.Verification]
- In the course of a transaction, EV debit always precedes EV credit. When the actor

27 *The SOF qualification of a TOE expresses the minimum efforts assumed necessary to defeat a system's expected security behaviour by directly attacking its underlying security mechanisms. In the Common Criteria framework, the SOF and its level (high, medium and low) are not part of the security objectives.*

from whom EV is debited enjoys a lower trust level than the actor to whom EV is credited (e.g. in the case of a refund of EV), EV is transferred before the CP that fulfils the obligation of the actor to whom EV is credited. When the actor to whom EV is credited enjoys a lower trust level than the actor from whom EV is debited (e.g. in the case of loading of EV), EV is transferred after the CP that fulfils the obligation of the actor to whom EV is credited. [OSP.Sequence]

- All of the secrets used in the TOE have a limited life span in accordance with their usage and are renewed when required. [OSP.SecretLifespan]
- The security level is maintained during the life cycle of the devices through security updates. This includes the maintenance of hardware and software necessary for the functioning of the e-money system. [OSP.Maintenance]
- All of the secrets can be replaced. Sub-systems can be replaced either in whole or in part. Replacement must be performed in such a way as to minimise the impact on service availability. [OSP.Evolution]
- There is a technical and organisational end-of-life procedure for every device containing EV. This procedure includes[OSP.EVPresentation]:
  - presentation and extinguishment of EV;
  - communication of RD to the System Supervisor;
  - communication of AD to the EV Issuer.
- Authorised and identified personnel perform the installation, initialisation, administration and operation of all sub-systems. The TOE enforces organisational and technical procedures that restrict access to assets to authorised personnel. [OSP.Access]
- Every sub-system preserves the integrity of the stored amount of EV. The maximum EV amount that can be debited from a sub-system must not exceed the EV amount with which it has been credited. [OSP.Equilibrium]

3 Security objectives

This section defines the security objectives for the TOE and its environment. The security objectives aim at countering the identified threats and at addressing identified organisational security policies and assumptions (see Annex F for a cross-reference table).

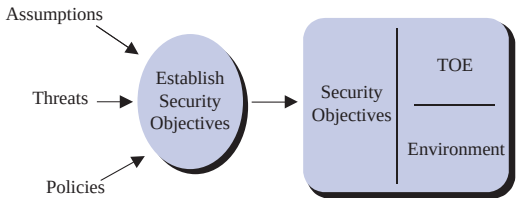
3.1 Classification of security objectives

3.1.1 Security objectives for the TOE or the environment

The purpose of determining security objectives is to address all of the security concerns and to declare which security aspects are addressed either directly by the TOE or by its environment. Thus, the security objectives are of two types:

- security objectives for the TOE, traced back to aspects of identified threats to be countered by the TOE and/or organisational security policies to be met by the TOE;
- security objectives for the environment, traced back to aspects of identified threats not completely countered by the TOE and/or organisational security policies or assumptions not completely met by the TOE.

Figure 9
Security objectives derivation



3.1.2 Application domains

The scope of the security objectives is specified on the basis of domains. The following domains are defined:

- E-money System (SYS): These objectives concern the whole e-money system.
- Secrets (SEC): These objectives concern keys, passwords and authentication data, as well as their management: generation, deletion, revocation, distribution, storage and use.
- Transactions (TRANS): These objectives concern the transaction domain, i.e. basic operations, the devices of the sub-systems inside or between which EV circulates, the actors in charge of those sub-systems and the following assets:
  - transaction attributes, especially the EV exchanged between two sub-systems and stored in a sub-system;
  - the functional parameters of sub-systems;
  - RD generated for a transaction and communicated to the System Supervisor.[28]
- EV creation and extinguishment (CREXT): These objectives concern the elements dedicated to EV creation and extinguishment, i.e. basic operations dedicated to EV creation or extinguishment, related sub-systems, actors in charge of those sub-systems and the following assets:
  - the data which result in EV creation and the data which result from its extinguishment;
  - the parameters related to EV creation or extinguishment;
  - AD generated for a transaction and communicated to the EV Issuer.
- Monitoring (MON): These objectives concern the RD and the System Supervisor information.[29]

28 *The transaction domain focuses on the dynamic aspect of the RD, i.e. sending of the RD to the System Supervisor. The monitoring domain (see below) focuses more on the non-dynamic aspect, i.e. on use by the System Supervisor of the RD and the System Supervisor information.*

29 *Monitoring is related to the operation and handling of RD and System Supervisor information by the System Supervisor. The dynamic side is covered in other domains.*

3.1.3 Naming convention

The security objectives below are named as follows:

OT|OE.<domain_code>.<general_objective> [.<specific_objective>],
where :
- OT|OE indicates whether the objective concerns the TOE (OT) or the environment (OE).
- <domain_code> is one of SYS, SEC, TRANS, CREXT and MON.
- <general_objective> indicates the general objective under which this objective is classified.
- <specific_objective> is an optional refinement for this objective

3.2 Security objectives list

A list of 24 Security objectives in presented below.

Each security objective is first introduced in a general manner, then broken down into specific objectives for the various domains.

3.2.1 Integrity [INT]

The integrity of the assets is preserved, in particular EV amounts.

- Every sub-system preserves the integrity of the stored EV amounts. [OT.SYS. INT.EVSTORAGE]
- Only authorised transactions can modify the EV amount stored in a sub-system. [OT.SYS. INT.EVTRANSAC]
- For every transaction the EV amount debited from one sub-system equals the EV amount credited to the other. [OT.TRANS. INT.EQUALITY]
- The EV amount created or extinguished equals the EV amount exchanged in the related transaction. [OE.CREXT. INT.EQUALITY]

3.2.2 Confidentiality [CONF]

The assets that must remain confidential are preserved accordingly.

- The TOE preserves the confidentiality of all secrets. [OT.SEC.CONF.SEC]
- The TOE preserves the confidentiality of the System Supervisor information. [OT.MON.CONF.SSI]
- RD and the System Supervisor information are known solely by those with a need to know. [OE.MON.CONF.NEEDTOKNOW]

3.2.3 Identification [ID]

An unambiguous identification is required for some components of the e-money system

Each of the following elements of the TOE is unambiguously defined by a unique identifier [OT.SYS.ID].:

- the System Supervisor;
- the EV Issuer;
- the sub-systems and, through them, the actors in charge of each sub-system;
- the transactions;
- the transaction types;
- the secrets;
- the quasi-actors (if applicable).

3.2.4 Authentication [AUTH]

EV transactions and monitoring data exchanges are authenticated.

- For each transaction the sub-system debited with EV and the sub-system credited with EV authenticate each other. [OT.TRANS.AUTH.SUBSYS]
- For each transaction, the sub-system credited with EV authenticates the EV stemming from the debited sub-system. [OT.TRANS.AUTH.EV]
- For each transaction, the sub-system debited with EV delivers proof of its participation in the transaction to the sub-

system credited with EV and vice versa. [OT.TRANS.AUTH.PROOF]
- The sub-system sending RD to the System Supervisor authenticates the System Supervisor when sending the RD.
- The System Supervisor authenticates the RD that he receives. [OT.TRANS.AUTH.RD]
- The TOE provides means to communicate AD to the EV issuer in an authenticated manner and to verify that they have been received.
- The EV Issuer authenticates the AD that he receives. [OE.CREXT. AUTH.AD]

3.2.5 Access control [ACC]

Unauthorised access to all assets is prevented, even in the case of a malfunction in monitoring or in secrets management. Every identified actor has a clear set of access rights.

- The TOE implements security functions that prevent illicit access to secrets in the event of a malfunction in secrets management. [OT.SEC.ACC.SEC]
- In the event of a monitoring malfunction, the TOE implements security functions that prevent illicit access to the System Supervisor information. [OT.MON.ACC.SSI]
- Every identified actor within the system has a clear set of access rights. [OE.SYS.ACC.PRIVILEGES]

3.2.6 Commitment and validation [COMM]

Transactions are conducted and validated under the terms of a commitment between the parties.

- Transaction initialisation is possible only after the actors in charge of the sub-systems to be credited and debited with EV have validated a commitment. This commitment fixes the EV amount to be exchanged. [OE.TRANS.COMM.COMMITMENT]
- For each commitment there is only one transaction. The EV amount exchanged in this transaction is equal to the EV amount defined in the commitment. [OE.TRANS.COMM.AMOUNT]
- Every transaction must be validated by the two parties. The validation procedure complies with the commitment terms. Both parties are aware of the commitment prior to any transaction. [OE.TRANS.COMM.VALIDATION]

3.2.7 Atomicity [ATOMICITY]

Transactions are either completed or undone.

- The TOE enforces security functions that allow a transaction to either be completed or undone as long as the closure operation has not been performed. [OT.TRANS.ATOMICITY]

3.2.8 Transaction order [ORD]

Every transaction consists of a set of basic operations executed in a predefined order.

- Every transaction contains only one single occurrence of every basic operation that it consists of. [OT.TRANS.ORD.OCCURRENCE]
- For every transaction, basic operations are executed in the following order:
  - initialisation;
  - EV debiting precedes EV crediting;
  - closure.

  [OT.TRANS.ORD.ORDER]

- For every transaction involving EV creation or extinguishment, basic operations are executed in the following order:
  - EV creation or extinguishment precedes closure;
  - AD transmission to the EV Issuer takes place after EV creation or extinguishment;
  - AD can be processed only if and when the transaction has been completed. [OT.CREXT.ORD.ORDER]

3.2.9 Non-evaporation [EVAP]

Only authorised sub-systems can perform extinguishment transactions.

– The TOE restricts EV extinguishment to transactions between two authorised sub-systems of the TOE. [OT.CREXT.EVAP]

3.2.10 Limitations [LIM]

EV amounts are limited during the EV life cycle.

For each sub-system, parameters set are:
– the maximum EV amount which the sub-system can store;
– the maximum EV amount which can be exchanged in a transaction;
– the maximum EV amount which can be created in a transaction. (This relates only to the issuing sub-system.)

[OT.SYS.LIM.EVLIMITS]

3.2.11 Traceability [TRAC]

The System Supervisor is able to trace and audit all strategic events. Sub-systems record and keep the data required by the System Supervisor for as long as required. Traceable data accurately reflects recorded events.

– The generation, deletion, revocation and replacement of secrets are strategic events: these events are recorded in order that they can be audited by the System Supervisor. [OT.SEC.TRAC.AUDIT]
– The initialisation and the modification of the sub-systems' functional parameters are strategic events. These events are recorded so that they can be audited by the System Supervisor. [OT.TRANS.TRAC.AUDIT]
– Initialisation and modification of the parameters relating to EV creation and extinguishment are strategic events. These events are recorded in order that they can be audited by the System Supervisor. [OT.CREXT.TRAC.AUDIT]
– The TOE provides means, when required, to communicate RD to the System Supervisor in a timely manner.[30] [OT.TRANS.TRAC. TIMELY]
– Every sub-system that produces RD for the System Supervisor keeps, for as long as required, a record of the transactions that it has performed and a record of the RD to be communicated to the System Supervisor. [OT.TRANS.TRAC.RECORD]
– RD accurately reflect transactions. [OT.TRANS.TRAC.TRUE]
– Every sub-system that produces AD keeps, for as long as required, a record of the AD communicated to the EV Issuer. [OT.CREXT.TRAC.RECORD]
– AD accurately reflect transactions involving EV creation or extinguishment. [OE.CREXT.TRAC. TRUE]

3.2.12 Detection [DETECTION]

The system has the capability to:

– detect abnormal events, including actual or attempted modification of assets and counterfeiting of transaction attributes;
– communicate to the Systems Supervisor all information which traces these abnormal events.

In particular:

– The TOE provides means to detect attempted or actual occurrences of illicit access to secrets, modification or illicit use of secrets. [OT.SEC.DETECTION]
– The TOE provides means:
  – to detect attempted or actual occurrences of modification of the transaction's domain assets;
  – to detect attempted or actual occurrences of transaction attribute counterfeiting;
  – to provide RD to the System Supervisor to enable these abnormal events to be traced to their source;

30 *"In a timely manner" refers to the time needed to allow processing of data to meet all deadlines relevant to the process goal.*

– to detect attempts to replay authentic transactions (or a part thereof). [OT.TRANS.DETECTION]
– The TOE provides means to detect attempted or actual occurrences of modification or counterfeiting of the creation and extinguishment domain assets. [OT.CREXT.DETECTION]
– The TOE provides means to detect attempted or actual occurrences of illicit access and modification of the monitoring domain assets. [OT.MON.DETECTION]

3.2.13 Reaction [REACTION]

The system provides means to limit or undo the consequences of an abnormal or illicit action.

– The TOE provides means to ensure service continuity by limiting the consequences of illicit access to secrets, modification or illicit use of secrets. [OT.SEC.REACTION]
– The TOE provides means to implement the reactions ordered by the System Supervisor to limit or suppress the effects of a detected or suspected malfunction in relation to the assets. [OT.TRANS.REACTION]
– The TOE cancels every transaction involving a malfunction. [OT.TRANS.REACTION.UNDO]
– The TOE provides means to implement the reactions ordered by the System Supervisor to limit or suppress the effects of a detected or suspected malfunction. [OT.CREXT.REACTION]
– The TOE provides means to react against attempted or actual occurrences of modification or counterfeiting of the monitoring domain assets. [OT.MON.REACTION]

3.2.14 Cryptography and protocols [CRYP]

State-of-the-art cryptography, protocols and security procedures are required.

– The security architecture of the TOE is based on standardised, publicly and extensively reviewed, state-of-the-art cryptographic algorithms and cryptographic key management. The TOE does not use cryptographic algorithms, which must remain confidential for security reasons. [OT.SYS.CRYP.CRYPTO]
– The SOF[31] for the use of cryptography and probabilistic mechanisms must be high. [OT.SYS.CRYP.SOF]
– The communication architecture of the TOE is based on standardised protocols and security procedures. [OT.SYS.CRYP.PROTOCOL]

3.2.15 Secret management [MNG]

The confidentiality and integrity of secrets is preserved by correct generation and distribution, physical storage protection, limited life span and renewal.

– The TOE generates and distributes secrets in accordance with standardised procedures. [OT.SEC.MNG.INITIALISATION]
– Secrets are generated in such a way that their value cannot be predicted. [OT.SEC.MNG.PREDICTABILITY]
– Every secret has a limited life span according to its usage. [OT.SEC.MNG.LIFESPAN]
– The TOE provides means to generate new values to replace secrets at any time. [OT.SEC.MNG.REPLACEMENT]
– Every secret dedicated to one security function must only be used for that function. [OE.SEC.MNG.SEPARATION]
– Relevant secrets are transported and stored in devices that resist physical tampering and interference. Relevant secrets must never be found in clear text outside such devices. Private and secret cryptographic keys to be used outside of

31 The SOF qualification of a TOE expresses the minimum efforts assumed necessary to defeat a system's expected security behaviour by directly attacking its underlying security mechanisms. In the Common Criteria framework, the SOF and its level (high, medium and low) are not part of the security objectives.

such devices must be reduced to a strict minimum and must not be essential to security. Private (asymmetrical) cryptographic keys and symmetrical Master or Root Keys in a hierarchical key structure are essential to security. [OT.SEC.MNG.TAMPER]
– All procedures and associated elements used for generating secrets are known only by those with a need to know. Secrets are distributed only to those who need them. [OE.SEC.MNG.NEEDTOKNOW]

3.2.16 Trusted path [TRUSTED_PATH]

Interaction with the system is achieved through protected communication means.

– The TOE provides a "trusted path" between authorised quasi-actors and sub-systems in order to protect exchanged assets (transaction data, access data, etc.) from modification by, or disclosure to, untrusted applications. The trusted path is capable of ensuring that a quasi-actor is communicating with the correct sub-system, and vice versa. [OT.SYS.TRUSTED_PATH]

3.2.17 Trusted location [TRUSTED_LOCATION]

A physically protected environment is required for sensitive security devices.

– Security devices, when under the responsibility of an Administrator or Operator, are located in a physically protected (or trusted) environment. [OE.SYS.TRUSTED_LOCATION]

3.2.18 Competence and responsibility [RESP]

People involved in the system know and follow their own contractual obligations, and have sufficient means, training and information to perform their role.

– The actors and quasi-actors know and follow their contractual obligations as well as their reciprocal obligations with regard to regulations, finances and security. [OE.SYS.RESP.RESPONSIBILITY]
– Those in charge of the following functions have the necessary competence and expertise in the relevant field:
  – management of secrets;
  – installation, administration and operation of sub-systems.

  They have sufficient means, training and information to perform their role. [OE.SYS.RESP.COMPETENCE]
– A state-of-the-art hiring policy, control of access to company premises and a security awareness programme apply to the personnel of all companies dealing in the production and the distribution of devices or software used by the TOE. [OE.SYS.RESP.PERSONNEL]

3.2.19 Qualification and tests [QUAL]

System components are tested, before and/or during operation.

– Hardware devices, software and organisational procedures have passed functional qualification tests. Hardware devices have also passed physical resistance tests. [OE.SYS.QUAL.QUALIFICATION]
– During its operation phase, every device can undergo functional testing without this affecting the availability of the e-money system. [OE.SYS.QUAL.OPERTEST]
– Before it is put into operation, every device is tested, first in isolation and then following integration into the TOE. [OE.SYS.QUAL.DEVELTEST]
– Every sub-system is subject to a qualification procedure which verifies the reliability of the following functions whenever they are supported:
  – amounts of EV received are aggregated into a single amount, the value of which equals the sum of the amounts received;
  – the stored EV amount is broken into smaller amounts, the sum of which

equals the stored EV amount. [OE.SYS.QUAL.RELIABLE]

3.2.20 Assessment [ASSESSMENT]

Important players are subject to assessment.

– The Administrator and the Operator are reviewed to provide assurance that practices properly reflect the security policy. [OE.SYS.ASSESSMENT]

3.2.21 Security update

A periodic security update is required for all sensitive parts of the system.

– In order to maintain a constant security level, a periodic security update for hardware and software is necessary. [OE.SYS.MAINTENANCE]

3.2.22 Availability [AVAIL]

The system ensures service availability, even during maintenance of a part of the system.

– The TOE ensures small service discontinuity when one or more (or even all) secrets of the TOE are replaced. [OT.SEC.AVAIL.AVAILABILITY]
– The TOE provides means to create and extinguish EV continuously, in particular while some or all of the devices which store and process AD are being replaced. [OT.CREXT.AVAIL.AVAILABILITY]
– A business continuity plan limits the impact of any malfunction of the e-money system, or any part thereof, on service availability. [OE.SYS.AVAIL.AVAILABILITY]
– The TOE provides means for continuous monitoring, particularly while some or all of the devices which store and process RD are being replaced. [OT.MON.AVAIL.AVAILABILITY]
– Assets and data are stored in devices which prevent their deterioration over time. [OT.SYS.AVAIL.PERENNIALITY]

3.2.23 Life cycle [LIFE]

State-of-the-art security procedures are used during the life cycle of the EV and sub-systems.

– State-of-the-art physical and logical protection applies to all premises upon which devices and software used by the TOE are initialised. [OE.SYS.LIFE.INITIALISED]
– Sub-systems are initialised in compliance with stateof-the-art security procedures. [OE.SYS.LIFE.INITIALISATION]
– State-of-the-art security applies to the packaging, distribution and installation of all devices and software used by the TOE. [OE.SYS.LIFE.DISTRIBUTION]
– Circulation of EV in a sub-system is restricted in accordance with well-defined criteria. [OT.TRANS.LIFE.CIRCULATION]
– The TOE enforces a technical and organisational end-of-life procedure for every device which contains EV. This procedure includes:
  – presentation and extinguishment of EV;
  – communication of RD to the System Supervisor;
  – communication of AD to the EV Issuer. [OT.SYS.LIFE.TERMINATION]

3.2.24 Partition [PARTITION]

When a sub-system uses applications other than the e-money application, separation is enforced between the applications.

– When an e-money system shares one or more devices with other applications, these devices must isolate the e-money system from those other applications. Only processes internal to the e-money system can modify data belonging to the e-money system. [OE.SYS.PARTITION]

Annexes

A Sources

This report is based on the following sources:

- [CC-1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model Version 2.1 ISO/IEC 15408-1;
- [CC-2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements Version 2.1 ISO/IEC 15408-2;
- [CC-3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements Version 2.1 ISO/IEC 15408-3;
- Information Technology – Security Techniques – Guide for the Production of Protection Profiles and Security Targets, Draft, ISO/IEC PDTR 15446;
- CEM 97/017 Common Methodology for Information Technology Security Evaluation, Part 1: Introduction and General Model;
- CEM 99/045 Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology;
- Report on Electronic Money, ECB, 1998;
- Security of Electronic Money, Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries, 1996;
- Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of e-money institutions.

B Application notes

A number of aspects of the EMSSO are described below, including the general model of an e-money system and the general threats to the system.

B.1 Link with the CC methodology

In defining security objectives, the report uses the framework and terminology of the CC standard. It broadly follows the outline defined in the CC. However, this does not imply that the CC standard should be used in defining concrete security functions and in the evaluation/assessment phase.

Several steps may be followed under the CC methodology in order to compile a comprehensive list of security objectives (for the system that is subject to evaluation, or TOE). Figure 10 below illustrates these different steps.

Firstly, the "security environment" – the context in which it is intended to use the subject or TOE – should be defined including all of the organisational issues, expertise and knowledge deemed relevant.

In particular, the TOE physical environment, assets and TOE purpose have to be taken into account:

- TOE physical environment: identifies all aspects of the TOE's operating environment relevant to TOE security, including known physical and personnel security arrangements;
- assets requiring protection: includes assets that are directly referred to, such as files and databases, and assets that are indirectly related, such as authorisation credentials and the IT implementation itself.
- TOE purpose: may relate to the product type and intended usage of the TOE[32].

Thereafter, investigations into the threats, risks and security policies provide a more specific representation of the:

- Assumptions: The assumptions must be met by the TOE environment in order for the TOE to be considered secure. This statement can be accepted as axiomatic for the TOE evaluation.
- Threats: this includes all threats perceived by the security analysis as relevant to the TOE. The CC characterises the threat in terms of a threat agent, a presumed attack method, any vulnerabilities forming the foundation for the attack, and identification of the asset under attack.
- Organisational security policy: this includes all relevant policies and rules. For a system, such policies may be explicitly identified.

The results of the analysis of the security environment could then be used to state the security objectives designed to counter the identified threats and to address the organisational security policies and assumptions identified.

The EMSSO report is structured as follows:

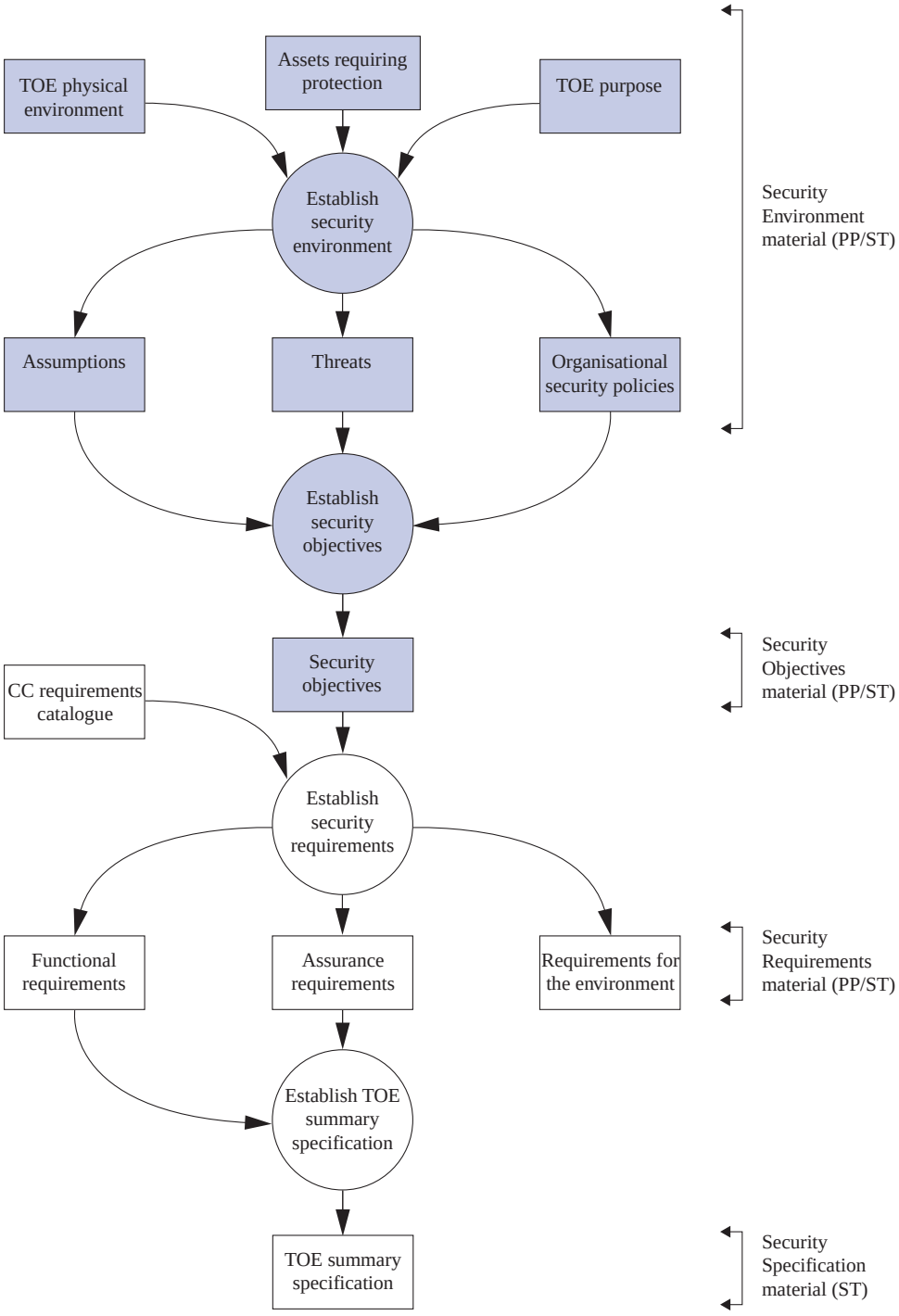
- the Target Of Evaluation (TOE);
- the security environment of the TOE, including the assets to be protected and the potential threats to the TOE or its environment, the assumptions made and the organisational policies used;
- the security objectives for the TOE and its environment.

The following figure gives an overview of the Common Criteria process for deriving requirements and specifications and the parts (shown in darker shading) which are covered by this document.

32 *Source: Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model (1998).*

Figure 10

Parts of the CC framework covered in this document [33]



33 *Source: Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model (1998).*

B.2 Rationale for the model

Many factors should be taken into account when formulating the security objectives, e.g. the players in the system, the organisational procedures, etc. A model of a typical e-money system could enhance the reader's understanding of the subject by illustrating all the relevant information in a manner that is easy to understand. The model presented in Section 1.1 ("E-money system: model") describes an e-money system as an IT system designed to allow the transfer of EV in a transaction between electronic devices (sub-systems).

The general model is in principle applicable to any type of e-money system, whether a card-based or software-based e-money system (including server-based/network-based types). The "System Supervisor" is a special player who is responsible for the proper functioning of the system as a whole. He is in charge of EV security management and checks that no more EV is extinguished than is created. Indeed, in an e-money system conforming to the model, the EV amount created is equal to the sum of the extinguished EV amount and the EV amount in circulation. If more EV is extinguished that the amount that was created, then false EV has been introduced into the system.

As explained in Section 2.1.3 ("Additional concepts: compensation, transactions, EV life cycle, roles, actors"), two types of transaction can be identified: transactions with compensation and transactions without compensation. In general, a payment is always defined as a "transaction with compensation", because each payment normally corresponds to a delivery of goods or services (a compensation). However, in some specific cases e-money systems could also define some payment transactions as "transactions without compensation". An e-money system could, for example, decide (for commercial reasons) to define the person-to-person payments as transactions without compensation, which do not therefore have to report to the System Supervisor. However, it is possible to impose restrictions on person-to-person payments, such as confining them to members of the same family.

B.3 Strength of function

Reference has been made in the present paper to the SOF in order to point out that, for some areas, the SOF must in any case be high. This must be considered when a complete PP is to be produced. Following the CC approach and document structure, the SOF should be specified within later chapters of a PP (security requirements, etc.) and not in security needs or security objectives.

For the CC approach, a SOF is typically an assurance requirement for a probabilistic or permutational mechanism (for example a PIN, password or the generation of keys).

In addition, the security objectives do not include any assurance requirement. As with the SOF, it is necessary to specify when a complete PP will be produced in specific chapters of such a document. The level of assurance requirements for an e-money system is not under discussion at the present time.

B.4 Roles

Roles – and trust levels – deeply impact on the system assessment, which should take into account product evaluation and process evaluation. These two evaluation types raise different issues, depending on the roles involved.

As regards Administrators, security in their area of competence area stems largely from an effective security system definition and management. Products must be used in a protected and trusted environment with a direct and controlled management.

On the other hand, security in the User competence area is mainly based on products that "help" Users, who work in an untrusted

environment and with poor skills, to comply with the security system. User devices are often used in a hostile environment, where Users have no capabilities to protect them.

As a consequence:

- Evaluation in an Administrator context requires a reliable process evaluation with the aim of verifying organisational aspects of security. Products can also be evaluated at a lower assurance level, exploiting the high trust level of the Administrator's infrastructure.
- Evaluation in a User context is mainly based on product evaluation, aiming to verify the soundness of devices used in an untrusted environment. On account of the low trust level of this context, product evaluation requires higher assurance levels.
- Evaluation in the Operators context refers to a proper combination of the above-mentioned "profiles".

C Acronyms

AD	Accounting Data
CC	Common Criteria
CP	Compensation
EMI	Electronic Money Institution
EMSSO	Electronic Money System Security Objectives
EV	Electronic Value
OSP	Organisational Security Policy
PP	Protection Profile
RD	Reporting Data
SF	Security Function
SFP	Security Function Policy
SOF	Strength Of Function
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy

D Glossary [34]

Accounting Data (AD): Data sent to the EV Issuer upon EV creation and extinguishment.

Acquirer: In an e-money system, the entity or entities (typically banks) that hold deposit accounts for merchants and to which transaction data are transmitted.

Actor: See the paragraph headed "Roles, actors, quasi-actors", page 13.

Assets: Information or resources to be protected by counter-measures of a TOE.

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

Authentication data: Information used to verify the claimed identity of a User.

Availability: The ability of services and information to be accessed by Users when requested.

Common Criteria (CC): [to be added].

Compensation: See page 10.

Component: The smallest selectable set of elements that may be included in a PP, ST or a package.

Cryptography: The application of mathematical theory to develop techniques and algorithms that can be applied to data to ensure the achievement of goals such as confidentiality, data integrity and/or authentication.

Electronic Value (EV): See page 8.

Electronic Money Institution (EMI): Defined in Directive 2000/46/EC as an undertaking or legal person other than a credit institution which issues means of payments in the form of e-money.

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

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

Integrity: The quality of being protected against accidental or fraudulent alteration or of indicating whether or not alteration has occurred.

Organisational security policy (OSP): One or more security rules, procedures, practices or guidelines imposed by an organisation upon its operations.

Product: A package of IT software, firmware and/or hardware providing functionality designed for use or incorporation within a multiplicity of systems.

34 The Glossary is based on the "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model" (November 1998) and "Security of electronic money" by the CPSS and the Group of Computer Experts of the Central Banks of the Group of Ten Countries (August 1996).

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

Protocol: Procedures for the interchange of electronic messages between communicating devices.

Reporting Data (RD): Data sent to the System Supervisor by sub-systems in order to allow EV circulation monitoring.

Role: A predefined set of rules establishing the interactions allowed between a User and the TOE. See the paragraph headed "Roles, actors, quasi-actors".

Secret: Information which can only be known to authorised users and/or the TOE Security Functions (TSF; see below) in order to enforce a specific Security Function Policy (SFP; see below).

Security function (SF): A part or parts of the TOE that have to be relied upon to enforce a closely related subset of 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 organisational security policies and assumptions.

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

Server: A computer that provides services through a network to other computers.

Strength of Function (SOF): A qualification of a TOE security function which expresses the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

Sub-system: See page 8.

System: A specific IT installation with a particular purpose and operational environment.

System Supervisor: Special player in the e-money system who is responsible for the proper functioning of the system as a whole. He is in charge of EV security management and monitors EV flows.

System Supervisor information: Data obtained from RD processing and centralised by the System Supervisor.

Tamper-resistant: The capacity of devices to resist physical attack up to a certain point.

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

TOE environment: All elements which are not part of the TOE but are necessary to the TOE to satisfy its security objectives.

TOE Security environment: Security aspects of the environment in which the TOE is intended to be used and manner in which it is expected to be employed.

TOE security function (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 (see below).

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

Traceability: In e-money systems, the degree to which value transfer transactions can be traced to the originator(s) or the recipient(s) of the transfer.

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

User: Any entity (i.e. human user or external IT entity) outside of the TOE that interacts with the TOE.

User data: Data created by and for the User that does not affect the operation of the TSF.

E Minimum requirements in the "Report on Electronic Money"

Requirement 1: Prudential supervision

Issuers of electronic money must be subject to prudential supervision.

Requirement 2: Solid and transparent legal arrangements

The rights and obligations on the part of the respective participants (customers, merchants, issuers and operators) in an electronic money scheme must be clearly defined and disclosed. Such rights and obligations must be enforceable under all relevant jurisdictions.

Requirement 3: Technical security

Electronic money schemes must maintain adequate technical, organisational and procedural safeguards to prevent, contain and detect threats to the security of the scheme, particularly the threat of counterfeits.

Requirement 4: Protection against criminal abuse

Protection against criminal abuse, such as money laundering, must be taken into account when designing and implementing electronic money schemes.

Requirement 5: Monetary statistics reporting

Electronic money schemes must supply the central bank in each relevant country with whatever information may be required for the purposes of monetary policy.

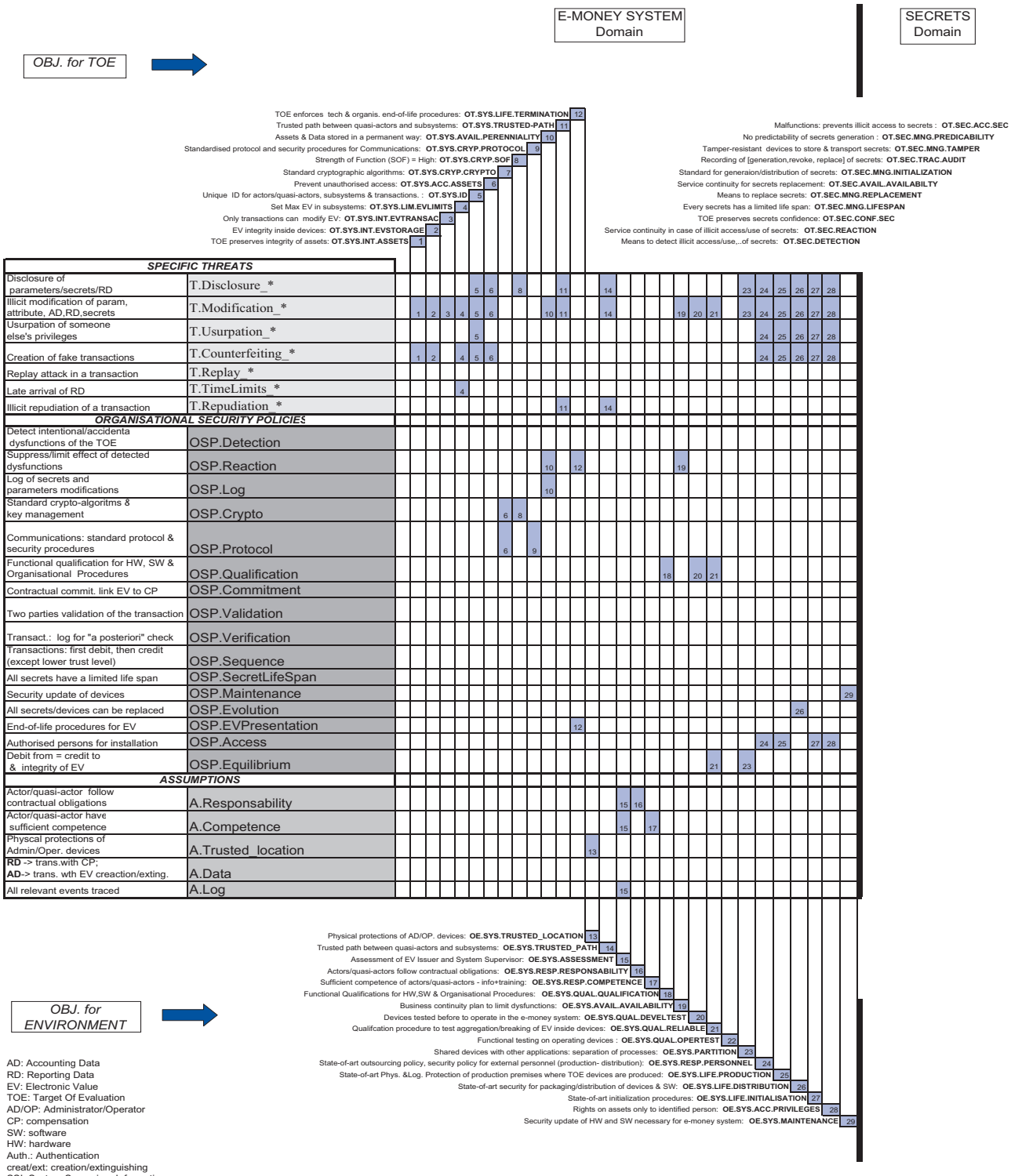
Requirement 6: Redeemability

Issuers of electronic money must be legally obliged to redeem electronic money against central bank money at par at the request of the holder of the electronic money. The details of this requirement are to be specified.

Requirement 7: Reserve requirements

The possibility must exist for central banks to impose reserve requirements on all issuers of electronic money.

F Cross-reference Table for Security Objectives



Cross reference table for Specific Security Objectives


TRANSACTIONS Domain
EV CREATION & EXTINGUIS. Domain
MONITOR Domain
Restriction of EV circulation in a subsystem: OT.TRANS.LIFE.CIRCULATION
RD represent transactions with CP: OT.TRANS.TRAC.TRUE
Initial. -> debit->credit-> close: OT.TRANS.ORD.ORDER
One occurance of basic operation per transaction: OT.TRANS.ORD.OCCURENCE
Debit = Credit (in a transaction) : OT.TRANS.INT.EQUALITY
Record/send RD to Superv.: OT.TRANS.TRAC.RECORD
Superv. authenticate RD - : OT.TRANS.AUTH.RD
RD to Supervisor on time: OT.TRANS.TRAC.TIMELY
Trace of subsys. initial. & modify: OT.TRANS.TRAC.AUDIT
Proof of partecipation in the transac.: OT.TRANS.AUTH.PROOF
Auth. of EV coming from debited subs.: OT.TRANS.AUTH.EV
Auth. among subsys: OT.TRANS.AUTH.SUBSYS
Complete or undo transac.: OT.TRANS.ATOMICITY
Reaction to abnormal events: OT.TRANS.REACTION
Undo for abnormal events: OT.TRANS.REACTION.UNDO
Detect abnorm. events on trans.: OT.TRANS.DETECTION
EV creation/extinguishing -> close -> AD to Issuer: OT.CREXT.ORD.ORDER
Record of AD communicated to EV Issuer: OT.CREXT.TRAC.RECORD
Recording of init/modify of EV creat/ext parameters: OT.CREXT.TRAC.AUDIT
Continuos extinguishing of EV: OT.CREXT.AVAIL.AVAILABILITY
Extinguishing only between authorised subsys: OT.CREXT.EVA
Reaction to dysfunctions: OT.CREXT.REACTION
Detect modification of assets involved in EV creat/ext: OT.CREXT.DETECTION
Continuos monitoring: OT.MON.AVAIL.AVAILABILITY
Malfunctions: prevent illicit access to SSI: OT.MON.ACC.SSI
Detect alteration of Superv. Info/RD: OT.MON.REACTION
Confident. of Superv. Info: OT.MON.CONF.SSI
Detect access to Superv. Info/RD: OT.MON.DETECTION
Secrets not shared among functions : OE.SEC.MNG.SEPARATION
Secrets known by who needs them : OE.SEC.MNG.NEEDTOKNOW
Commitment validation before transaction.: OE.TRANS.COMM.COMMITMENT
Exchanged EV amount = amount in contract: OE.TRANS.COMM.AMOUNT
Two parties validation of the transaction - cognisance of contract: OE.TRANS.COMM.VALIDATION
EV creat/ext=EV in transac.: OE.CREXT.INT.EQUALITY
AD represent creat/ext trans.: OE.CREXT.TRAC.TRUE
Issuer authent. received AD: OE.CREXT.AUTH.AD
RD &Superv.Info: OE.MON.CONF.NEEDTOKNOW
RD & Sup.Info known only by those who need to know