Open Smart Card Infrastructure for Europe

v2

Volume 6: **Contactless Technology**

Part 3: **White paper on the Certification of Contactless Cards**

Authors: **eESC TB6 Contactless Smart Cards**

NOTICE

This eESC Common Specification document supersedes all previous versions.

Neither eEurope Smart Cards nor any of its participants accept any responsibility whatsoever for damages or liability, direct or consequential, which may result from use of this document.

Latest version of OSCIE and any additions are available via www.eeurope-smartcards.org and www.eurosmart.com. For more information contact info@eeurope-smartcards.org.

Table of CONTENTS

1 INTRODUCTION

The document is part of eEurope TB6 Contactless Technology trailblazer / 'SINCE' IST project, which has three mains goals:

- ⇒ Promote the proliferation of contactless technology
- ⇒ Harmonise the contactless infrastructure and ensure the interoperability of systems
- ⇒ Stimulate the use of contactless technology through education

The interoperability of contactless products and systems is essential if the market for this technology is to be expended. The technology is still in its infancy in terms of standardisation and industrialisation. Very recently, the ISO/IEC 14443 series of standards has become available. The challenge to ensure that different products and cards from different manufacturers with different applications on systems from different manufacturers are compatible is subject of Interoperability (SINCE WP1 D1.1). In the present study the possibilities to certify products and cards according to defined standards is analysed.

It is essential for the development of contactless technology that the necessary laboratories are developed. In this way the interoperability of the systems may be ensured and the end-user's and operators confidence in the technology is enhanced. In this area, the first task is to evaluate the current market available for certifying conformity of products and security relevant to existing contactless technology.

The first step in this process is the development of links with evaluation laboratories to aid in the development of contactless specific evaluation tools and methods. The first part of this document gives a general overview on current procedures and practices for certification. Starting with common certification procedures on smart cards with contact interface (ISO 7816) the feasibility of applying similar techniques to contactless technology environment is studied. From this starting point, collaboration with the laboratories and industrials to create a minimum "common specifications" validation procedure is established. The conclusion leads into recommendations to standardisation bodies for improvement of standards building the basis for certification.

1.1 PRODUCT CERTIFICATION

Today, there are more products and services available than ever before. This means the need for consumer protection has never been greater. Consumers can be protected by certification, inspection and testing of products and by manufacturing under certified quality systems.

Product certification can be based on the verification of certain characteristics specified by a company or according to an international standard for a specific product.

As consumers need confidence in the certification, inspection and testing work carried out on their behalf, but which they cannot check for themselves. This checking is the job of accreditation bodies. Certifiers of systems and products as well as testing and calibration laboratories need to demonstrate their competence. They do this by being accredited by a nationally recognised accreditation body.

1.2 ACCREDITATION OF CERTIFIERS

Accreditation delivers confidence in certificates and reports by implementing widely accepted criteria set by the European (CEN) or international (ISO) standardisation bodies. The standards address issues such as impartiality, competence and reliability; leading to confidence in the comparability of certificates and reports across national borders. Governments have confidence in testing and certification in support of regulatory functions.

The scope of accreditation of a testing laboratory is the formal and precise statement of the activities which the laboratory is accredited for. It is as such the result of a combination of information (scope parameters) concerning the testing field, the type of test (describing the measurement principle), the product/object tested and the methods and procedures used for the test.

The assessment of the scope of accreditation represents the core of the accreditation process and may be defined as the set of operations carried out by the Accreditation Body in order to ensure, with an adequate degree of confidence, that the laboratory has the competence to provide reliable test services within the defined scope.

Accredited laboratories may be allowed to modify their own laboratory-developed methods or to use up-dated versions of standard methods and standards they are accredited for and to introduce similar new methods without having to report to the Accreditation Body in advance, provided that these modifications and up-dated versions or new methods do not incorporate new measurement principles that are not covered by the original description of the scope.

The laboratory must inform the Accreditation Body about modifications in an agreed time interval.

1.3 REFERENCES

ISO/IEC 17025: General requirements for the competence of testing and calibration laboratories

EN 45 011: General requirements for bodies operating product certification systems

2 CURRENT STATUS OF CERTIFICATION FOR CONTACTLESS SMART CARDS

2.1 CERTIFICATION OF CONFORMANCE

This kind of product certification is based on the verification of certain characteristics specified by a company or according to an international standard for a specific product. In this context certification should aim on interoperability, as this is the most stringent characteristic for the deployment of contactless card technology, besides, of course, security, which will be dealt with in a specific chapter later in this document.

The prerequisite for certification is the existence of a widely accepted international standard. For contactless technology several sets of international standards exist.

2.1.1 International Standards for contactless smart cards

Basically there are three sets of international standards for contactless smart cards:

2.1.1.1 ISO/IEC 10536: Identification Cards - Contactless integrated circuit(s) cards Close-coupled cards

This set standardises a "close-coupled" type of inductive and capacitive coupled contactless cards with an operating range of few millimetres. This standard is no more relevant to the market due to technical advantage of inductive coupled cards described in ISO/IEC-Standards 14443 and 15693.

ISO/IEC 10536-1:	Physical characteristics
ISO/IEC 10536-2:	Dimensions and location of coupling areas
ISO/IEC 10536-3:	Electronic signals and reset procedures

2.1.1.2 ISO/IEC 14443: Identification Cards - Contactless integrated circuit(s) cards Proximity Cards

ISO/IEC 14443 is currently the most widely used standard for contactless smart cards. The standard defines two types of cards with different data transmission and protocols. For interoperability a card reader has to support both types.

The standard comprises following parts:

ISO/IEC 14443-1: Physical characteristics

Refers to ISO/IEC 7810 for dimensions and introduces specific terms, like PICC (Proximity Integrated Circuit(s) card) and PCD (Proximity coupling device). Also definitions are made for behaviour of the card exposed to static and alternating electric and magnetic fields.

ISO/IEC 14443-2: Radio frequency power and signal interface

This part of ISO/IEC 14443 describes characteristics of power-transfer and communication between PICC and PCD. Two different types of communication signal interfaces are specified, Type A and Type B.

ISO/IEC 14443-3: Initialisation and anticollision

This part of ISO/IEC 14443 describes:
- polling for PICCs entering the field of a PCD
- byte format, frames and timings
- Request (REQ) and Answer to request (ATQ) commands
- Anticollision methods to detect and communicate with one card among several cards

Polling methods:
- Terminal talks first
- PICC must be able to accept a request within 5 ms after exposure to the operating field.

Anticollision methods:
- Type A: Binary search method referring to the Unique Identifier (UID) of the card
- Type B: Slotted Aloha method

ISO/IEC 14443-4: Transmission protocol

This standard specifies:
- Protocol activation for type A
- A half duplex block transmission protocol (T=CL).
- Protocol deactivation of the card

The evolution of this standard is still ongoing; several proposals for extensions as well as for improvement of the test methods are under consideration by the responsible working groups.

2.1.1.3 ISO/IEC 15693: Identification Cards - Contactless integrated circuit(s) cards Vicinity Cards

ISO/IEC 15693 defines several different data transmission modes and protocols. Contrary to ISO/IEC 14443 the card has to support all for interoperability. The card reader selects the mode which will be used for operation.

The standard comprises following parts:

ISO/IEC 15693-1: Physical characteristics

Refers to ISO/IEC 7810 for dimensions and introduces specific terms:
Vicinity Integrated Circuit(s) card (VICC) and (VCD) Vicinity coupling device
Also definitions are made for behaviour of the card exposed to static and alternating electric and magnetic fields.

ISO/IEC 15693-2: Air interface and initialisation

This part of ISO/IEC 15693 describes characteristics of power-transfer and communication between VICC and VCD. Several different types of modulation and data coding must be supported by the VICC.

ISO/IEC 15693-3: Anticollision and transmission protocol

This part of ISO/IEC 15693 describes:
- protocol and commands
- other parameters required to initialise communication between a VICC and a VCD
- methods to detect and communicate with one card among several cards (anticollision)
- Data elements like Unique Identifier (UID) and Application Family Identifier (AFI)
- Memory organisation
- Behaviour of VICCs described in state machine diagrams
- Set of commands (mandatory, optional, custom and proprietary)

2.1.1.4 Standardised Test Methods

For each set of the standards there is a corresponding standard describing test methods for the specific card type:

ISO/IEC 10373-6: For proximity cards according to ISO/IEC 14443
ISO/IEC 10373-7: For vicinity cards according to ISO/IEC 15693

Both standards describe the measurement methods for the physical interface for energy transfer and data exchange between cards and terminals.

2.1.2 Proprietary certification models for contactless smart cards and systems

Some companies have introduced their own certification schemes for contactless smart cards and systems to insure interoperability.

2.1.2.1 Calypso

Calypso is an open technology standard for contactless ticketing, designed and promoted by public transport operators. It is maintained by the Calypso Networks Association.

Calypso includes a lot of elements, not only technical, which are available to any transport operator to allow an easier implementation of a contactless ticketing system open to multi-modality and multi-application.

The development of the Calypso ticketing application is based on the international standards as far as possible and covers the following areas:

- Contactless communication ISO/IEC 14443, type B.
- Card OS and file architecture: ISO/IEC 7816-4.
- Card data structure: CEN ENV1545.
- Card and SAM Security Mechanisms Data Model
- Terminal Application Software
- Security Management and Architecture.

Testing and certification of products is available from laboratories which are member of the Calypso Networks Association (see www.calypsonet-asso.org).

2.1.2.2 MIFARE®

The MIFARE® Interface Platform is an industry standard for contactless smart cards introduced and maintained by Philips Electronics N.V. with contactless communication according to ISO/IEC 14443, type A.

The key application for the MIFARE® Interface Platform is electronic ticketing in public transport. It contains a wide range of product families, ranging from hardwired ICs using the MIFARE® classic protocol to dual interface controllers which feature an open protocol on both contact and contactless interfaces, delivering the flexibility and security to support multiple applications on a single card IC.

Conformance to the interface specifications, which are based on ISO/IEC 14443, type A, can be certified by an independent test laboratory.

2.1.3 Conformance testing

2.1.3.1 Conformance to ISO/IEC 10536

The technology described ISO/IEC 10536 can be regarded as outdated now, as it is replaced by the higher performance standards ISO/IEC 14443 and ISO/IEC 15693. The corresponding test methods standard has not yet been published under it's designated number ISO/IEC 10373-4 and work on this publication is stopped now.

2.1.3.2 Conformance to ISO/IEC 14443

Since ISO/IEC 14443 is the most widely used international standard for contactless smart cards, the following analysis will be based on that standard. The structure of ISO/IEC 15693 is very similar to ISO/IEC 14443, so that conformance testing will be similar.

ISO/IEC 14443-1 describes physical characteristics and tests relating to environmental characteristics:

- Dimensions compliant to ID-1 ISO/IEC 7810
- Bending and other stress defined in ISO/IEC 10373
- Alternating magnetic and electric fields
- Static magnetic and electric fields
- Operating temperature (0 to 50 degree Celsius)
- Surface quality printing
- Restrictions may apply to embossing of the PICC

The main parts for interoperability testing of the physical layer are the modulation, data coding and initialisation characteristics written in parts 2 and 3 of ISO/IEC 14443 as well as the corresponding test methods of ISO/IEC 10373-6.

The standard for test methods is currently under amendment procedure for improvement of RF related test methods and to include protocol tests for both types A and B. The following amendments deal with protocol tests:

ISO/IEC 10373-6 / Amendment 1: Identification cards – Test methods – Part 6: Proximity Cards – Amendment 1: Additional PICC test methods

ISO/IEC 10373-6 / Amendment 3: Identification cards – Test methods – Part 6: Proximity Cards – Amendment 3: Additional PCD test methods

The RF test methods (physical layer) are amended by:

ISO/IEC 10373-6 / Amendment 2: Identification cards – Test methods – Part 6: Proximity Cards – Amendment 2: Improved RF test methods

The following table show a summary of conformance tests derived from ISO/IEC 14443 for cards (PICC).

Test / Measurement	ISO/IEC 14443 Base Standard Reference	ISO/IEC 10373-6 Test Methods Reference	Test limits	Magnetic field strength
for Type A cards:				
Operating frequency	-2, clause 6.1		(13560 ± 7) kHz	
Operating field	-2, clause 6.2	clause 6.2 [1]	functional	H = 1.5 / 4.5 / 7.5A/m
Acceptance of PCD modulation	-2, clause 8.1.2	clause 6.2 [1], see AMD2 clause 5.2.1 (draft)	functional	H = 1.5 / 4.5 / 7.5 A/m
Frame delay time PCD to PICC	-3, clause 6.1 -2, clause 8.1.2	clause 6.2 [1]	see ISO/IEC 14443-3, clause 6.1.2	H = 1.5 / 4.5 / 7.5 A/m
Load modulation	-2, clause 8.2.2	clause 6.2 [1], see AMD2 clause 5.1 (draft)	see ISO/IEC 14443-2, clause 8.2.2	H = 1.5 / 4.5 / 7.5 A/m
Initialisation and anticollision	-3, clause 6	see Amendment 1 (draft)	command set: REQA, WUPA, ANTICOLLISION, SELECT, HLTA	
Transmission protocol	-4, clauses 5,7,8	see Amendment 1 (draft)		
for Type B cards:				
Operating frequency	-2, clause 6.1		(13560 ± 7) kHz	
Operating field	-2, clause 6.2	clause 6.2 [1]	functional	H = 1.5 / 4.5 / 7.5A/m
Acceptance of PCD modulation	-2, clause 9.1.2	clause 6.2 [1], see Amd.2 clause 5.2.2 (draft)	functional	H = 1.5 / 4.5 / 7.5 A/m
Load modulation	-2, clause 8.2.2	clause 6.2 [1], see AMD2 clause 5.1 (draft)	see ISO/IEC 14443-2, clause 8.2.2	H = 1.5 / 4.5 / 7.5 A/m
Frame format and timing	-3, clause 7.1		see ISO/IEC 14443-3, clause 6.1.2	H = 1.5 / 4.5 / 7.5 A/m
Initialisation and anticollision	-3, clause 7.3	see Amendment 1 (draft)	command set: REQB, WUPB, Slot-MARKER, ATTRIB, HLTB	
Transmission protocol	-4, clauses 6,7,8	see Amendment 1 (draft)		

[1] Test PCD Assembly

Table 3.1: Summary of conformance tests for proximity cards (PICC) according to ISO/IEC 14443

Testing can be performed on the physical layer as described in ISO/IEC 10373-6 using standard laboratory equipment. For anticollision sequence and protocol testing a suitable reader can be used, where the necessary commands that can be programmed and the card's response can be analysed.

The various test parameters are well defined in the standards together with specific test methods. Some important test methods, like protocol tests, are still drafts in the amendment stage.

Nevertheless ISO/IEC 14443 does not specify exactly what a compliant cards must implement mandatory. Following areas were identified, that raise problems for interoperability of cards:

⇒ Proprietary anticollision and protocols are allowed by the standard
⇒ Cards need not implement the ISO/IEC 14443-4 protocol

The situation is even more difficult on the compliance for readers (PCD), as summarised in the following table.

Test / Measurement	ISO/IEC 14443 Base Standard Reference	ISO/IEC 10373-6 Test Methods Reference	Test limits	Test equipment
Carrier frequency	-2, clause 6.1		(13560 ± 7) kHz	Spectrum analyser
PCD operating field strength	-2, clause 6.2	clause 8.1	1.5 A/m .... 7.5 A/m	Reference PICC (ISO/IEC 10373-6)
Power transfer PCD to PICC	-2, clause 6	clause 8.2	5 mW	Reference PICC (ISO/IEC 10373-6)
Modulation index and waveform, type A	-2, clause 8.1.2		ISO/IEC 14443-2, fig. 2	DSO
Modulation index and waveform, type B	-2, clause 9.1.2		ISO/IEC 14443-2, fig. 4	DSO
Bit rate and coding, type A	-2, clauses 8.1.1, 8.1.3			DSO
Bit rate and coding, type B	-2, clauses 9.1.1, 9.1.3			DSO
Load modulation reception, type A	-2, clause 8.2	clause 8.4	ISO/IEC 14443-2, clause 8.2.2	Load modulation PICC (ISO/IEC 10373-6)
Load modulation reception, type B	-2, clause 9.2	clause 8.4	ISO/IEC 14443-2, clause 8.2.2	Load modulation PICC (ISO/IEC 10373-6)
Functional tests and anticollision, type A	-3, clause 6	see Amendment 3 (draft)		Type A card emulator
Functional tests and anticollision, type B	-3, clause 7	see Amendment 3 (draft)		Type B card emulator
Transmission Protocol	-4, clauses 5-8	see Amendment 3 (draft)		Type A/B card emulator

Table 3.2: Summary of conformance tests for proximity card readers (PCD) according to ISO/IEC 14443

2.1.3.3 Conformance to ISO/IEC 15693

ISO/IEC 15693-1 describes physical characteristics and tests relating to environmental characteristics similar to ISO/IEC 14443-1:

- Dimensions compliant to ID-1 ISO/IEC 7810
- Bending and other stress defined in ISO/IEC 10373
- Alternating magnetic and electric fields

- Static magnetic and electric fields
- Operating temperature (0 to 50 degree Celsius)
- Surface quality printing
- Restrictions may apply to embossing of the PICC

The main parts for interoperability testing of the physical layer are the modulation, data coding and initialisation characteristics written in parts 2 and 3 of ISO/IEC 15693. Part 3 also describes the basic transmission protocol from reader to card and vice versa. The corresponding test methods are in ISO/IEC 10373-7.

The test methods are not as complete as for ISO/IEC 14443 and will be needed to be amended as the evolution of the ISO/IEC 10373-6 proceeds.

Another obstacle may be the admission of optional and manufacturer proprietary commands for cards in ISO/IEC 15693-3, which may make interoperability difficult to achieve and certification less useful.

In relation to conformance testing the structure of ISO/IEC 15693 is different to that of ISO/IEC 14443 by the fact that there is one type of card which must be able to understand and support many kinds of modulation types and coding. The choice of modulation and behaviour of the card is totally under the control of the reader. Therefore a lot various parameter combinations have to be considered for compliance testing, which are shown in the following table.

Test / Measurement	ISO/IEC 15693 Base Standard Reference	ISO/IEC 10373-7 Test Methods Reference	Test limits	Data coding	Data rate	Sub-carrier	Magnetic field strength
Operating frequency	-2, clause 6.1		(13560 ± 7) kHz	1/256 1/4	low, high	single, dual	
Operating field	-2, clause 6.2	clause 6.2 [1)]	functional	1/256 1/4	low, high	single, dual	0.15 – 5 A/m
Modulation envelope	-2, clause 7.1	clause 6.2 [1)]	see ISO/IEC 15693-2, clause 7	1/256 1/4	low, high	single, dual	0.15 – 5 A/m
Load modulation	-2, clause 8.1	clause 6.2 [1)]	see ISO/IEC 15693-2, clause 8.1	1/256 1/4	low, high	single, dual	0.15 – 5 A/m
VICC timing	-3, clause 9.1	clause 6.2 [1)]		1/256 1/4	low, high	single, dual	0.15 – 5 A/m
VICC states and anticollision	-3, clauses 7,8			1/256 1/4	low, high	single, dual	0.15 – 5 A/m
VICC commands	-3, clause 10			1/256 1/4	low, high	single, dual	0.15 – 5 A/m

[1)] Test PCD Assembly

Table 3.3: Summary of conformance tests for vicinity cards (VICC) according to ISO/IEC 15693

Test / Measurement	ISO/IEC 15693 Base Standard Reference	ISO/IEC 10373-7 Test Methods Reference	Test limits	Test equipment
Carrier frequency	-2, clause 6.1		(13560 ± 7) kHz	Spectrum analyser
VCD Operating field an power	-2, clause 6.2	clause 8.1	0.15 – 5 A/m	Reference PICC (ISO/IEC 10373-7)
Modulation index and waveform	-2, clause 7.1	clause 8.2	see ISO/IEC 15693-2, clause 7.1	DSO
VCD Bit rate and coding	-2, clause 7.2		see ISO/IEC 15693-2, clause 7.2	DSO
Load modulation reception	-2, clause 8	clause 8.3	see ISO/IEC 15693-2, clause 8	Load modulation PICC (ISO/IEC 10373-6)
Functional tests and anticollision	-3, clauses 7,8,9			Card emulator

Table 3.4: Summary of conformance tests for vicinity card readers (VCD) according to ISO/IEC 15693

Although the framework of ISO/IEC-Standards already cover a lot of technical issues to ensure interoperability of cards and readers from different manufacturers, in the view of certification there are still some areas, where test methods or specifications are not completely covering all necessary aspects to assure interoperability. Among these are:

⇒ A test method for load modulation reception is not standardised, it is only "informative" in both ISO/IEC 10373-6 and ISO/IEC 10373-7. While load modulation values for cards are well defined with a standardised test method, there is no such method for readers.

⇒ For vicinity cards only two elementary commands are mandatory according to ISO/IEC 15693 (Inventory, Stay Quiet), all other commands are optional. Which means that any card manufacturer can implement his own commands as custom type commands.

2.1.4 Survey of Test Labs and Test Equipment

2.1.4.1 Test Labs

It is essential for the development of contactless technology that the necessary laboratories are developed. In this way the interoperability of the systems may be ensured and the end-user's/operators confidence in the technology enhanced.

At present, the possibilities for having a system or product certified are extremely limited. In this chapter we will mainly deal with conformance testing and not certification of security levels, which will be considered later in this document.

A number of test labs were questioned about their activities in the field of testing smart cards with emphasis on contactless technology.

The summary in the following table shows an overview of test labs working on contactless smart cards. It must be noticed that conformance, performance and interoperability are generally not tested and certified.

	Physical Parameters	Conformance ISO/IEC 14443	Conformance ISO/IEC 15693	Interoperability	Security (ITSEC/CC)	Other (EMV, etc.)	Test equipment	Comment
Exponent	X				X			
Integri		X		X	X	X	X	
T-Systems ISS					X			
CEA-LETI (CESTI)				X	X			
Collis				X		X	X	
FIME						X		
Arsenal research		X		X			X	
Micropross							X	

Table 3.5: Summary of test labs and suppliers for contactless

2.1.4.2 Test Equipment

The basic test equipment for measurement on the RF-interface is described in the test methods standards ISO/IEC 10373-6 and -7. It is a general principle to use standard laboratory test equipment, which can be traceably calibrated, for measurement. The special test set-ups and coils for measurement can be well and easily reproduced from the data specified in the standards.

For protocol testing on the card a suitable reader can be utilised, for which data transfer can be programmed and retrieved on a low level software basis. This is far more complicated for testing the correct behaviour of a reader. In that case a card emulator is necessary, which simulates a contactless card fully and allows to modify card-specific parameters to test the ability of the reader to communicate as demanded from the standard.

Generally the availability of test equipment for contactless card or reader evaluation is still very limited. The printed circuit boards and test set-up as described in ISO/IEC 10373-6 and -7 are available from Micropross and Arsenal Research.

For ISO/IEC 14443 Micropross is offering also a "Contactless Customisable Reader CLASS 185" and "Contactless Analyser CLASS 3150", which can simulate a contactless card and analyse data transferred over the RF-interface.

2.1.5 Contactless System Interoperability certification procedures

(to be completed)

2.2 CERTIFICATION OF SECURITY LEVELS

Essential part is the technical evaluation of the product according to the commonly known security criteria by an approved test lab. Every evaluation is accompanied by staff of the certification body to ensure a common method and procedure. The test reports of the labs have to be accepted by the certification body. This procedure assures a uniform assessment in comparison to various certification activities. The result is written down in a certification report which contains the relevant details of the product rating and information for the user. The certificates are made public if the applicant agrees to a publication.

2.2.1 Security criteria

Several security criteria which provide the basis for the evaluation of smart cards are available. The "Information Technology Security Evaluation Criteria" (ITSEC) is the outcome of several precursor documents issued in the United Kingdom, France and Germany. The German contribution to ITSEC was the "IT Security Criteria" published in 1989. ITSEC was published by the European Commission. The "IT Security Evaluation Manual" (ITSEM" was published as a supplement in 1993.

As a further development and harmonisation of the European ITSEC, the US "Federal Criteria" and the Canadian "Trusted Computer Product Evaluation Criteria" the "Common Criteria for Information Technology Security Evaluation" (CC) were established and later published as ISO Standard ISO 15408.

2.2.2 Targets of Evaluation (TOE)

The testing and assessment of product and systems against the Common Criteria (CC) is referred to as an "evaluation". A product or system undergoing evaluation is known as "Target of Evaluation" (TOE). Products and systems of quite different kinds can be evaluated on the basis of the above sets and baseline criteria. However, an important requirement is that the certificate issued at the end of the procedure states the security features regarding confidentiality, availability and integrity which the product is confirmed as possessing.

Products can be

⇒ Software components
⇒ Hardware components
⇒ Combinations of software and hardware (e.g. smart card combined with an operating system)

2.2.3 Organisational requirements for Certification

Usually three partners are involved:

⇒ The applicant (manufacturer, distributor, etc.)
⇒ The licensed evolution facility selected by the applicant
⇒ The Certification Body

The applicant concludes an evaluation agreement with the evaluation facility and applies to the Certification Body to have his product certified. Then the applicant provides all information necessary and the target of evaluation itself.

Evaluations aimed at certification have to be performed by evaluation facilities licensed by the Certification Body and is specific to a particular set of security criteria, i.e. ITSEC or CC. By the licensing process it is established whether the evaluators of the evaluation facility to be licensed possess the necessary qualification required under the security criteria concerned. Before an evaluation facility can be granted a license, it must be accredited under the European standard EN 45001. This standard contains general criteria regarding test laboratory operations and is therefore independent of any specific test domain. Accreditation of evaluation facilities under the EN 45001 is performed by the national accreditation authority, which is member in the international organisational network of accreditation authorities.

These organisations have joined to form European Accreditation (EA) which now covers all European conformity assessment activities:

- ⇒ testing and calibration
- ⇒ inspection
- ⇒ certification of management systems
- ⇒ certification of products
- ⇒ certification of personnel
- ⇒ Environmental verification under the European Eco-Management and Audit Scheme (EMAS) regulation

The evaluation facility is responsible for the correctness of its test results and documents and justifies these results in evaluation reports. The applicant receives the evaluation reports following acceptance of the evaluation facility by the certification body.

2.2.4 Duties of the certification body

It is the task of the certification body to ensure the equivalence of all certification results. For this purpose, the certification body monitors every evaluation. Such monitoring ensures that a uniform procedure and methodology are employed on every certification and with that ensuring that evaluations are comparable. Specific tasks of the certification body in this context are acceptance of the target of evaluation, checking and acceptance of the evaluation reports, participation n evaluation sessions and formal interpretation of the base security criteria.

The requirements contained in the base criteria are formulated in generic terms in order to be applied to a wide spectrum of possible products. This means that requirements contained within the criteria always need to be interpreted in specific, individual cases. To ensure that evaluation results produced by different evaluation facilities are comparable, the certification body prepares mandatory interpretations in such cases, in consolation with the evaluation facility. The certification body then draws up generalised interpretations on the basis of these decisions on individual cases. These are in turn submitted by the certification body to international working parties for the creation of internationally harmonised interpretations of criteria.

2.2.5 "ITSEC" Evaluation

During the 1980s, the United Kingdom, Germany, France and the Netherlands produced versions of their own national criteria. These were harmonised and published as the Information Technology Security Evaluation Criteria (ITSEC). The current issue, Version 1.2, was published by the European Commission in June 1991. In September 1993, it was followed by the IT Security Evaluation Manual (ITSEM) which specifies the methodology to be followed when carrying out ITSEC evaluations. The "Information Technology Security Evaluation Criteria" (ITSEC) consists of four parts, with the following structure of the documents:

Chapters 1 and 2: Explanation and definition of the used terms and explanation of the "security target" document.

Chapter 3: Requirements for testing and assessment from the point of view of effectiveness.

Chapter 4: Evaluation levels for the assessment of correctness

The central document for the specification of the security features of a product or system is the security target. The security target serves as a specification for the evaluation. It contains both the security enforcing functions to be tested and assessed and the evaluation requirements through the statement of evaluation level. The security target must therefore be subject to a thorough examination prior to commencing with the evaluation, since changes at a later stage can result in considerable time delay and additional cost. The product or system to be evaluated is referred to as the "Target of Evaluation" (TOE).

2.2.6 "Common Criteria" Evaluation

The Common Criteria represents the outcome of international efforts to align and develop the existing European and North American criteria. The Common Criteria project harmonises ITSEC, CTCPEC (Canadian Criteria) and US Federal Criteria (FC) into the Common Criteria for Information Technology Security Evaluation (CC) for use in evaluating products and systems and for stating security requirements in a standardised way. Increasingly it is replacing national and regional criteria with a world-wide set accepted by the International Standards Organisation (ISO15408). The "Common Criteria" (CC) can be divided into three parts:

Part 1: Introduction and general model – This part explains the underlying rationale of the CC and requirements regarding Security Target (ST) and Protection Profiles (PP).

Part 2: Security functional requirements – This part contains a catalogue of generic functional components for the specification of the security functional requirements in a hierarchical classification.

Part 3: Security assurance requirements – In this part requirements for the evaluation of the assurance of the security features of the Target of Evaluation (TOE) are defined in the form of hierarchically structured security assurance components. These security assurance components are summarised under the various evaluation aspects into classes and families. To provide a basis for the standardised evaluation of the assurance of a TOE and to simplify comparisons between different evaluation results, the hierarchical evaluation assurance levels EAL1 to EAL7 have bee formed from the security assurance components.

2.2.7 Specification of Security Features

2.2.7.1 Security Target

The Security Target is the central document for the specification of the security capabilities of a product or system. The Security Target serves as a specification for the evaluation as it contains both the security enforcing functions to be tested and assessed and the evaluation requirements. The evaluation requirements are generally stated by referring to one of the seven hierarchical evaluation assurance levels EAL1 to EAL7. The product or system to be evaluated is referred to as the "Target of Evaluation" (TOE).

The following table shows the definition of the seven assurance levels.

Level	Definition
EAL0	Inadequate Assurance
EAL1	Functionally Tested. Provides analysis of the security functions, using a functional and interface specification of the TOE, to understand the security behaviour. The analysis is supported by independent testing of the security functions.
EAL2	Structurally Tested. Analysis of the security functions using a functional and interface specification and the high level design of the subsystems of the TOE. Independent testing of the security functions, evidence of developer "black box" testing, and evidence of a development search for obvious vulnerabilities.
EAL3	Methodically Tested and Checked. The analysis is supported by "grey box" testing, selective independent confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. Development environment controls and TOE configuration management are also required.
EAL4	Methodically Designed, Tested and Reviewed. Analysis is supported by the low-level design of the modules of the TOE, and a subset of the implementation. Testing is supported by an independent search for obvious vulnerabilities. Development controls are supported by a life-cycle model, identification of tools, and automated configuration management.
EAL5	Semiformally Designed and Tested. Analysis includes all of the implementation. Assurance is supplemented by a formal model and a semiformal presentation of the functional specification and high level design, and a semiformal demonstration of correspondence. The search for vulnerabilities must ensure relative resistance to penetration attack. Covert channel analysis and modular design are also required.
EAL6	Semiformally Verified Design and Tested. Analysis is supported by a modular and layered approach to design, and a structured presentation of the implementation. The independent search for vulnerabilities must ensure high resistance to penetration attack. The search for covert channels must be systematic. Development environment and configuration management controls are further strengthened.
EAL7	Formally Verified Design and Tested. The formal model is supplemented by a formal presentation of the functional specification and high level design showing correspondence. Evidence of developer "white box" testing and complete independent confirmation of developer test results are required. Complexity of the design must be minimised.

Table 3.3: Assurance levels according to Common Criteria (ISO 15408)

2.2.7.2 Protection Profiles (PP)

Protection Profiles are used to specify an implementation-independent set of security features for certain classes of products, with agreed security objectives and operational environments. Protection Profiles are created either by manufacturers or by user groups for their specific application context. As the security features required are largely specified in the Protection Profiles, simply from analysing the implementation-independent PP it is possible to draw conclusions regarding certain aspects of the effectiveness of these security features. In this way, the use of Protection Profiles reduces the user's effort associated with evaluation of a product or system.

2.2.7.2.1 Common Smart Card Protection Profiles

Several Protection Profiles (PP) for smart cards have been defined and certified. Among these are the following:

2.2.7.2.1.1 Visa Smart Card Protection Profile

The TOE of the Visa Smart Card Protection Profile includes a smart card (contact type ISO 7816 or contactless type ISO/IEC 14443), an operating system and applications. The PP assumes that desired functionality may be implemented both in hardware and software. The TOE environment according to the PP is a conventional smart card operating environment including a variety of card acceptance devices like vending machines, PC smart card readers and so on.

It is remarkable that the Visa Smart Card Protection Profile requires compliance to international standards on the level of TOE security objectives. This may be quite obvious today, but it must be noted that many successful attacks on information technology products were possible due to proprietary solutions ignoring international standards.

The PP defines a comprehensive list of security functional requirements targeted at achieving the defined security objectives. The security functional requirements are drawn from the Common Criteria and include in general access control, import and export of user data, cryptographic operation and cryptographic key access, data security properties monitoring and protection, authentication services, data management, etc.

2.2.7.2.1.2 EMV ICC Credit & Debit Application Protection Profile

The EMV Integrated Circuit Card Credit & Debit Application protection profile (EMV-App PP) was published by EMVCo Company jointly owned by Europay International, Mastercard International, and Visa International. The current version 4.0 was issued in December 2001. The PP focuses on EMV credit/debit application that is compliant with EMV 2000 Integrated Circuit Card Specification.

The EMV-App PP defines the TOE as an on-card application performing EMV transactions according to the EMV specifications. The protection profile limits the TOE to mandatory EMV requirements and leaves a possibility to a developer to add optional EMV features supported by a specific product to the Security Target. The TOE does not include smart card hardware and card operating system software. The PP makes no assumptions about the smart card platform requirements. However, the authors suggest that the platform should meet the requirements defined in the SCSUG Protection Profile.

2.2.7.2.1.3 Smart Card Security User Group’s Protection Profile

The Smart Card Security User Group's (SCSUG) Protection Profile is a is a user-oriented protection profile designed particularly but not only for the financial industry. Its creators, the members of the Smart Card Security User Group, are American Express, Europay, JCB, MasterCard, Mondex, Visa, the NIST, and the NSA. Payment organisations are planning to make a security evaluation according to the SCSUG PP a mandatory requirement for payment ICCs. The TOE comprises the integrated circuit, its operating system, and the mechanisms that allow communication with the outside world either over contacts in accordance with ISO 7816 or contactless in accordance with ISO 14443. The TOE can establish a secure channel to a trusted source for application loading or execution of privileged commands.

2.2.7.2.1.4 Eurosmart Smart Card Protection Profiles

The Eurosmart Security Working Group has published several smart card protection profiles up to now, some of them may also be applied to contactless smart cards. The protection profiles address a smart card IC and secure multi-application smart card platform applications.

Currently the following protection profiles are available and can be downloaded from the Eurosmart's website (http://www.eurosmart.com):

Smart Card Integrated Circuit Profile 3.0
Smart Card IC Platform Protection Profile 1.0
Smart Card Integrated Circuit With Embedded Software Profile 2.0
Smart Card IC with Multi-Application Secure Platform Profile 2.0
Intersector Electronic Purse and Purchase Device Profile 1.2

2.2.7.2.2 Contactless Smart Card Protection Profiles

(to be completed)

2.2.8 Contactless Cards Security certification procedures

Several Certifiers are available throughout Europe that are offering certification in the field of IT security and in particular by application of the "Common Criteria" (CC, ISO 15408) as framework for certification of security on IT hardware and software. For the actual evaluation of the target a number of evaluation test labs are operating. A list of certifiers and evaluation test labs is compiled in the appendix to this document.

All certifiers using the "Common Criteria" scheme for certifying IT products are also offering certification of smart cards. As written before in this document there are several "Protection Profiles" available for both hardware related and application related smart card evaluation.

In many application related protection profiles the actual hardware-interface is not addressed and can therefore applied to both contact and contactless smart cards. Some protection profiles explicitly states, that the interface may be either contact (ISO/IEC 7816) or contactless (ISO/IEC 14443).

(to be completed)

APPENDIX

APPENDIX A: CONTACT INFORMATION OF TEST LABS AND SUPPLIERS

Exponent Inc.
149 Commonwealth Drive
Menlo Park, CA 94025,
USA.
Phone: (650) 326-9400
Fax: (650) 326-8072
E-mail: siliconvalley-office@exponent.com
http://www.exponent.com

Integri NV
Leuvensesteenweg 325 (3rd floor)
B-1932 Zaventem
Belgium - Europe

tel : 32.(0)2.717.69.50
fax : 32.(0)2.717.69.67
http://www.integri.com

Collis BV
De Heijderweg 21
2314 XZ Leiden
The Netherlands
Phone +31 71 5813636
Fax +31 71 5813630
Email info@collis.nl
http://www.collis.nl

FIME
3, rue de Chevilly
Cerisaie 204
94262 FRESNES Cedex
France
Tél. : (33) 1 46 15 46 59
Fax : (33) 1 40 96 94 93
E-mail : p.leray@fime.com
http://www.fime.com

CEA-LETI
17 rue des Martyrs
38054 Grenoble CEDEX 9
France
Tel: +33 4 38 78 43 04
Fax: +33 4 38 78 94 14
http://www-leti.cea.fr/

MICROPROSS
33, rue Gantois
59000 Lille
FRANCE
Tel: +33 (0)320 74 66 30
Fax: +33 (0)320 74 66 37
E-mail: smartcards@micropross.com
http://www.micropross.com

T-Systems ISS GmbH
Rabinstraße 8
D - 53111 Bonn
Tel. +49 (0)228 / 98 41 – 0
Fax +49 (0)228 / 98 41 – 60
Email: info.iss@t-systems.com
http://www.t-systems-iss.com

BSI Bundesamt für Sicherheit in der Informationstechnik
Refereat II 1.1
Godesberger Alle 183
D-53133 Bonn
Tel. +49 228 9582-338
Fax. +49 228 9582-427
E-mail: bsi@bsi.bund.de
http://www.bsi.de

Entrust CygnaCom
7927 Jones Branch Dr.
Suite 100 West
McLean, VA 22102-3305
USA.
Tel: 703-848-0883
Fax: 703-848-0960
Email: corpinfo@cygnacom.com
http://www.entrust.com/entrustcygnacom/index.htm

Aspects Software Ltd,
124/125 Princes Street,
Edinburgh, EH2 4AD
United Kingdom
Tel: +44 (0)131 225 9500
Fax: +44 (0) 131 225 9555
www.aspects-sw.com