FPEG Subgroup of Security Evaluation and Certification

A Survey on the Security Evaluation Procedures for the Certification of Payment Products in the European Union

---

1 The secretariat of the FPEG Subgroup on security evaluation and certification is provided by DG Internal Market and Services within the European Commission. However, the views expressed in this report are purely those of the writers and may not in any circumstances be regarded as stating an official position of the European Commission.
TABLE OF CONTENTS ........................................................................................................................................... 2

EXECUTIVE SUMMARY ............................................................................................................................................ 4

1. INTRODUCTION .................................................................................................................................................... 5

2. THE EU POLICY FRAMEWORK UNDERPINNING THE CREATION OF SEPA ................................................. 6
   2.1. The creation of SEPA and the security of payments .................................................................................. 6
   2.2. The new payments services directive: no provision on security evaluation ................................................ 7
   2.3. Existing recommendations on the harmonisation of evaluation procedures ............................................. 7

3. OVERVIEW OF THE ACTORS INVOLVED IN SECURITY EVALUATION AND CLARIFICATION ON THEIR ROLE AND RESPONSIBILITY .............................................................. 8
   3.1. The targets of the evaluation procedures: products, processes and services ............................................. 8
   3.2. The oversight policy and the European system of central banks ............................................................... 9
   3.3. The card industry: the European payment council and the payment schemes .......................................... 9
   3.4. Global payment schemes .......................................................................................................................... 9
   3.5. European and national payment schemes ................................................................................................ 10
   3.5.1. Internal approval scheme ..................................................................................................................... 11
   3.5.2. Outsourcing some roles in the approval scheme .................................................................................... 12
   3.6. The national public certification authorities ............................................................................................ 13
   3.6.1. The certification authorities ................................................................................................................ 13
   3.6.2. Country examples .................................................................................................................................. 14
   3.6.3. European recognition agreement ......................................................................................................... 15
   3.6.4. Actors involved in the CC evaluation ................................................................................................... 16
   3.7. Other parties: evaluation laboratories ....................................................................................................... 16
   3.7.1. Evaluation laboratories: role and responsibilities ................................................................................ 16
   3.7.2. Independence of the laboratory ........................................................................................................... 17
   3.7.3. Security & Confidentiality .................................................................................................................... 17
   3.7.4. ISO/CEI 17025 compliance .................................................................................................................. 17
   3.7.5. Means and competences ....................................................................................................................... 18
   3.7.6. Knowledge of the state of the art of attacks, Internal R&D on attacks ................................................. 18
   3.7.7. Scheme licensing .................................................................................................................................. 18

4. SECURITY EVALUATION PROCEDURES ............................................................................................................. 19
   4.1. List and overview of the security evaluation procedures implemented ...................................................... 19
       4.1.1. The survey on manufacturers ............................................................................................................ 19
       4.1.2. The survey on the banking & payment industry ................................................................................ 19
       4.1.3. Certification of production sites ......................................................................................................... 20
   4.2. Comparison regarding the coverage of security criteria ............................................................................ 21
   4.3. Ongoing initiatives to harmonise or align evaluation procedures or requirements .................................... 24
       4.3.1. Introduction ....................................................................................................................................... 24
       4.3.2. The CAS initiative ............................................................................................................................. 24
       4.3.3. Harmonisation features of PCI ......................................................................................................... 26
       4.3.4. Harmonisation features of EMVCo ................................................................................................. 27
       4.3.5. Harmonisation of site certification requirements ............................................................................. 28

5. VIEWS OF THE STAKEHOLDERS .......................................................................................................................... 28
   5.1. Views of administrations ........................................................................................................................... 28
   5.2. Card and terminal manufacturers ............................................................................................................ 29
   5.3. Banking sector .......................................................................................................................................... 29
   5.4. Views of merchants .................................................................................................................................... 30

6. CONCLUSIONS – THE WAY FORWARD ............................................................................................................... 30

LIST OF ANNEXES .................................................................................................................................................... 31
EXECUTIVE SUMMARY

The Fraud Prevention Expert Group has undertaken an overview of the methodologies currently used for the security evaluation of card payment products (cards, terminals etc), processes (software, etc.) and production sites, in the context of the creation of the Single Euro Payments Area.

There are several actors involved in security evaluation, each of them with its own role and responsibility. While there are global “proprietary” card schemes which issue proprietary standards that apply to components used in those schemes, there are also public security evaluation schemes, such as Common Criteria when used by national issuers are under the responsibility of Public Certification Authorities or bodies. For all payment schemes, the evaluation process approval is outsourced to independent security laboratories which perform the technical tasks following standardized rules determined by “public” or “proprietary” schemes.

The security evaluation procedures implemented are diverse. There are currently different initiatives to harmonise or align evaluation procedures and/or requirements. This relates in particular to the CAS initiative (which has started to align the security requirements of European and national players and to consolidate their positions with respect to the security standards issued by worldwide card schemes), to harmonisation features of proprietary schemes such as PCI and EMV (CAS has initiated talks with PCI and EMVCo to avoid redundant evaluation work) and to initiatives in relation to the harmonisation of site certification requirements.

FPEG experts are of the view that, as a matter of priority, security evaluation procedures should be aligned and mutual recognition achieved throughout the EU.
A SURVEY ON THE SECURITY EVALUATION PROCEDURES FOR THE CERTIFICATION OF PAYMENT PRODUCTS IN THE EUROPEAN UNION

1. INTRODUCTION

In October 2004 the Commission issued an Action Plan 2004-2007 of non-legislative measures to prevent fraud and counterfeiting of non-cash means of payment, with a view to foster a more coherent approach to fraud prevention. This Action Plan builds on a previous one covering the period 2001-2003.2

A Fraud Prevention Expert Group (FPEG) was established under those Action Plans. This experts’ group at EU level includes representatives of different parties involved in fraud prevention (national and international payment schemes, banks, law enforcement, Central Banks, other national authorities, retailers, consumer groups, manufacturers of cards and terminals, network operators etc.). It aims at promoting the exchange of information and best practices and at fostering cross-border cooperation, notably between different sectors, in order to prevent payment fraud.

The FPEG decided to create a Sub-group on Security Evaluation and Certification (hereafter the Subgroup) with the objective of, inter alia, issue a report on the current situation of security evaluation and certification in the area of on payment systems, identifying future needs and proposing recommendations.

The work of the sub-group is reflected in this report, which provides an overview of the methodologies currently used for the security evaluation of card payment products (cards, terminals etc), processes (software, etc.) and production sites. The structure of the report is as follows:

- Section 2 presents an overview of the EU policy framework underpinning the creation of Single Euro Payments Area;
- Section 3 presents an overview of the actors involved in security evaluation, with a clarification of their roles and responsibilities;
- Section 4 presents an overview of the security evaluation procedures implemented, a comparison of the coverage of security criteria and a description of the ongoing initiatives to harmonise or align evaluation procedures and/or requirements;
- Section 5 presents the views of the stakeholders;
- Section 6 presents some conclusions for the way forward.

2 For further information, see http://europa.eu.int/comm/internal_market/payments/fraud/index_en.htm.
2. THE EU POLICY FRAMEWORK UNDERPINNING THE CREATION OF SEPA

2.1. The creation of SEPA and the security of payments

In recent years, a wide debate on how to achieve a Single Euro Payment Area (SEPA) took place between the European Commission, the European Central Bank, the banking community (in particular through the European Payment Council - EPC) and other payment providers. The goal is to achieve an integrated market for payment services which is subject to effective competition and where there is no distinction between cross-border and national payments within the euro area. This objective calls for the removal of all technical, legal and commercial barriers between the current national payment markets3.

The EPC has started to work with a view to deliver true pan-European payment instruments, and, as regards payment cards, has already adopted a SEPA Cards Framework. The European Central Bank indicated 2008 as the date when banks should begin harmonising credit transfers, direct debits and card payments, and 2010 as the date for the completion of this process.

The creation of SEPA should result not only in greater economies for consumers and businesses, but also on increased security. In the area of the security of card payments the obstacles to be overcome are well known. Removing the differences in standards, regulations and practices would favour interoperability and help preventing payment fraud. The ultimate objective is that cardholders and payment systems users are able to enjoy the same high level of security throughout SEPA when using their payment instruments.

Concerning the security evaluation of card payment products, components and processes, stakeholders (notably the European regulators, the banking sector and the manufacturers of chips, cards and terminals) agree on their importance. The Eurosystem (ECB) recently issued its view on a "SEPA for cards", where it also provides its ideas with regard to standardisation and fraud prevention (selected extracts of this document are provided in annex 3 to this FPEG paper). The Eurosystem underlines the need that standards cover "the security evaluation and the certification of devices"4. The industry is also actively working on improving existing and internationally recognised methods of evaluation5.

---


For a simple description of SEPA, see the brochure prepared by the ECB in October 2006, available at the ECB website at: http://www.ecb.int/paym/pol/sepa/html/index_en.html, or generally the website of the EPC: http://www.europeanpaymentscouncil.eu/


See also generally http://www.europeanpaymentscouncil.eu/content.cfm?page=sepa_vision.
2.2. The new payments services directive: no provision on security evaluation

The Commission felt it necessary to underpin SEPA with a new EU legal framework on payments. In December 2005, it presented a proposal for a Directive on Payment Services\(^6\). However, despite the expectations in earlier preparatory work undertaken by the Commission, this Commission proposal does not include any provision on security evaluation.

Indeed, annex 7 of an earlier Commission Communication of 2003\(^7\) described the existence of different security evaluation procedures in the EU and the difficulties in having comparability between evaluations. It also pointed out the lack of mutual recognition between certifications carried out in different Member States and highlighted the times and costs associated with the need of multiple certifications in different countries.

Therefore, the question remains as to whether the European legislator should enact, in addition to the self-regulatory work undertaken by industry, mandatory card standards for the entire market covering every phase of the transaction chain (cardholder-to-terminal, terminal-to-acquirer and acquirer-to-issuer as well as processing), the security evaluation and certification of devices.

2.3. Existing recommendations on the harmonisation of evaluation procedures

The harmonisation of security evaluation procedures of payment products would be fully in line with to the EU policies in other areas of Information Technology in the financial sector, such as for example:

- Creation of ENISA in November 2003 aiming at ensuring particularly high levels of network and information security. ENISA is operational since September 2005;
- Implementation of stronger risk management liability and rules for the financial sector (implementation of Basel II and the approach of operational risk to reduce card fraud);
- Combating of identity fraud, organised crime and terrorism by securing and organising the interoperability of electronic identity documents (passports, driver licenses as well as vehicle identification documents)

---


This communication followed a wide public consultation.
There are indeed some recommendations related to this issue.

**Council Recommendation on IT products (2002)**

A Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security stated that: “The security of transactions and data has become essential for the supply of electronic services, including e-commerce and online public services, and low confidence in security could slow down the widespread introduction of such services”. The Resolution asks the Member States to launch or strengthen information and education campaigns to increase awareness of network and information security; to specifically target such actions at business, private users and public administrations; to develop such awareness raising actions closely with the private sector, including inter alia internet service providers, and to encourage private sector-led initiatives.

**ECB report on E-money Security Objectives**

The European Central Bank released in May 2003 the Electronic Money Security Objectives (EMSSO), which promote the reference to Common Criteria methodology for all IT products, including smart cards. The EMSSO report is a follow-up to the ECB's 1998 “Report on Electronic Money” which defined a common policy with regard to electronic money and established a set of general requirements that electronic money schemes should fulfill. The EMSSO report contains a general description of e-money schemes, a comprehensive risk/threat analysis and a list of security objectives that should be met by e-money schemes in order to cover these risks/threats.

### 3. OVERVIEW OF THE ACTORS INVOLVED IN SECURITY EVALUATION AND CLARIFICATION ON THEIR ROLE AND RESPONSIBILITY

Security evaluation process is a basis for risk management, a rating for resistance against the “state-of the art” of attacks. It can target products processes and services (see subsection 3.1). “Proprietary” and “public” security evaluation schemes co-exist and involve different actors. Central banks (see subsection 3.2) have an oversight policy in this area.

Global “proprietary” card schemes (see subsection 3.4) issue standards that apply to components used in those schemes, inside or outside EU. Several of them do so through PCI SSC and EMVCo. Many payment products issued in the EU bear the logos of two main card schemes, one active solely in SEPA and the other active worldwide. Issuers (see subsection 3.3) naturally ask for the greatest possible similarity between SEPA standards and the standards of worldwide card schemes. CAS has started to align the security requirements of European and national players (see subsection 3.5) and to consolidate their positions with respect to the security standards issued by worldwide card schemes.

“Public” security evaluation schemes such as Common Criteria when used by national issuers are under the responsibility of Public Certification Authorities or bodies (see subsection 3.6). For all payment schemes, the evaluation process approval is outsourced to independent security laboratories (see subsection 3.7) which perform the technical tasks following standardized rules determined by “public” or “proprietary” schemes.

#### 3.1. The targets of the evaluation procedures: products, processes and services.

The production of security requirements is only part of the process set up to provide assurances. A set of security requirements is usually linked to an assurance programme that, under certain conditions, determines how well the relevant requirements are met. A
set of security requirements and associated assurance programme applies to any relevant target of evaluation affected by the said requirements and programme.

A target of evaluation (object to which the security requirements and assurance programme are relevant) may be a product, a process or a service.

3.2. The oversight policy and the European System of Central Banks

A large majority of European central banks has an oversight policy for card payment schemes. Almost all central banks regard themselves as directly overseeing card payment schemes for security issues, with the objective of maintaining public confidence in means of payment.

3.3. The Card Industry: the European Payment Council and the payment schemes

The EPC groups banks and national payment schemes in Europe. The EPC has started to work with a view to deliver true pan-European payment instruments. In March 2006, the EPC has issued a SEPA card framework calling in particular for the payments schemes to engage in mutual recognition of security evaluations for cards and terminals.

The payment schemes are divided, for the purposes of this report into: global payment schemes and European/national payment schemes.

3.4. Global payment schemes

The global schemes:

- have several tens of thousands of member banks;
- have more than two billion (thousand million) cards between them;
- process more than six trillion (million million) euros.

A significant proportion of this business involves European issuers and acquirers interacting with the rest of the global market, enabled by the infrastructure provided by the global schemes.

Payment schemes such as Visa and MasterCard operate as a “four-party” model. Within this model, there is an issuing function (issues payment instrument - usually cards), an acquiring function, cardholders (associated with Issuers) and merchants (associated with Acquirers). Payment schemes manage, in various ways, the relationships between issuing and acquiring functions. MasterCard and Visa do not, for example, issue or acquire directly, but enable, in various ways, their member banks that do so, making them four-party systems. Other global schemes (such as American Express, Discover Financial Services and Diner’s Club) have a different business model where they also issue and acquire directly as well as enable third party entities to issue and acquire. This is more akin to a “three-party model” but the principles would be similar.

---

8 Visa (Visa Europe is currently a group member and co-owner of Visa International), MasterCard Worldwide, American Express, JCB, Discover Financial Services, and Diner’s Club are examples of global card payment schemes.
One of the main attributes of a global scheme is the global interoperability of products where payment instruments (mostly, but not exclusively, cards) can be accepted at participating merchants globally. Global interoperability does not happen by accident – to ensure that such happens, certain functions, such as interoperability principles and security, are managed on a global level. For security in particular, this ensures that there is a global minimum standard that all relevant payment devices and associated processes adhere to. This provides assurances to both Issuers, and their cardholders, and Acquirers, and their merchants, wherever they may come from and wherever they may be, that those minimum standards are upheld and universal acceptance is ensured.

For example, Visa International introduced a set of security requirements for terminal components handling Personal Identification Numbers in 1997. The requirements were based on available international standards. After a few years of acclimatization, the original self-certification form method evolved to a terminal testing process using third party laboratories. MasterCard had a similar process.

A parallel risk evaluation process established for payment instruments (Integrated Circuit Cards) was established in the late 1990’s – this involved testing the cards at approved laboratories from its inception. For example, Visa uses a methodology called Card Risk Testing programme for testing VSDC (Visa Smart Debit & Credit) products. MasterCard uses a methodology called CAST to test products issued under, for example, its MChip programme. A different process, managed under the auspices of EMVCo, applies to those Visa and MasterCard products that use the CPA (Common Payment Application) applet instead of scheme specific applets.

For further information about EMV, see below chapter 4.3.3.

### 3.5. European and national payment schemes

Approval is the process by which a payment scheme component (a product or a service) is authorised for use in that payment schemes. Approval is an essential part of a payment scheme’s governance. Therefore a payment scheme formalises a number of roles and tasks to be performed by them in the approval process. This constitutes an approval scheme.

The approval process includes functional testing and, when relevant, a security evaluation.

We first describe (3.5.1) an approval scheme where all the roles are internal to the payment scheme (with the possible exception of the role of Evaluator). We then describe (3.5.2) the outsourcing of some roles. Those descriptions are generic.

---

9 For the purposes of this report, European or national payment schemes are the European based payment schemes that are normally active in their country of location only, or in a few European countries.
3.5.1. Internal approval scheme

a) Approval Council

The Approval Council defines and maintains the approval scheme.

The Approval Council is responsible to ensure that approval requirements (e.g. functional requirements, security requirements, migration dates) and any other information relevant for the Approval Scheme are available to the Approval Applicants.

The Approval Council delegates tasks to the Security Committee and to the Technical Committee for component approval as well as for approval scheme maintenance.

Based on the recommendations of the Security Committee and of the Technical Committee, the Approval Council decides on the approval of a component, especially if deviations from the requirements have been detected. This means that the Approval Council performs some risk management.

b) Security Committee

The Security Committee is informed of modifications in the security requirements by other parts of the payment scheme’s governance. It updates accordingly the approval requirements and the evaluation process.

The Security Committee assesses on the basis of an evaluation report (and of further explanations when necessary) whether a component complies with the requirements.

The Security Committee also assesses whether the evaluation process and the evaluation report comply with scheme rules.

c) Technical Committee

The Technical Committee is informed of modifications in functional specifications by other parts of the payment scheme’s governance. It updates accordingly the approval requirements and the functional testing process.

The Technical Committee performs the same tasks in the functional domain as the Security Committee in the security domain.

d) Approval Office

The Approval Office is in charge of administration. It communicates changes in the approval process to laboratories. It registers applications and checks eligibility of components for approval. It delivers approval letters and publishes approvals. It archives all the documents used in the process of approving a given component.

e) Evaluators

Testing and evaluation tasks are performed by laboratories / evaluators whose expertise and professionalism have been assessed by the Technical Committee or the Security Committee.

Evaluators may be internal to the payment scheme or third parties licensed by the payment scheme.
3.5.2. **Outsourcing some roles in the approval scheme**

A payment scheme may choose to outsource some tasks to a third-party evaluation and certification scheme composed of a Certification Body and of laboratories. These tasks are typically:

- laboratory licensing by the Certification Body,
- evaluation by the laboratory
- and evaluation supervision by the Certification Body.

The payment scheme requires enough visibility to warrant confidence in the certification scheme’s internal processes.

At the end of an evaluation, the applicant receives an evaluation report and, if the evaluation is successful, a certificate.

The payment scheme requires access to the evaluation report (or an extract thereof) for risk management purposes.

---

**Approval in Cartes Bancaires (a payment scheme operating mostly in France)**

Cartes Bancaires has an approval scheme for cards, terminals, cryptographic enclosures (i.e. containers for secret keys), card manufacturing sites, card personalisation sites, card personalization processes, protection of personal data, etc.

Upon initiating the use of smart cards for payments and cash withdrawals, Cartes Bancaires joined efforts with card vendors and with the European CC certification scheme to optimise the use of the Common Criteria (ISO 15408) for smart cards. This has been greatly facilitated by Eurosmart, an association representing card manufacturers, as well as by the responsiveness of National Certification Authorities.

Cartes Bancaires has benefited by leveraging expertise and quality processes that would have been too expensive in-house. Card manufacturers have benefited from improved development methodologies by integrating in them the requirements of the CC methodology.

Cartes Bancaires relies sometimes on its own resources for tests, audits and evaluations, and sometimes on third-parties. Cartes Bancaires is at present analysing modifications of its approval schemes in the light of the Directive on Payment Services. Cartes Bancaires preferred strategy in doing so is to contribute to the emergence of European-wide competence centers.

**Dutch evaluation scheme for PIN**

Due to PIN online, there has always been a strong tradition in security evaluations of PIN terminals in the Netherlands. The certification scheme for terminals has always been run by the banking community. Today the certification scheme is run by Currence, the Dutch payment scheme provider for PIN. Expect for the independent test labs which act as the Security Evaluator there are no external certification roles for PIN.

Besides the hardware evaluation done by the accredited test labs an important point in the security evaluation of the terminals is the mandatory code review of all security related software of the terminal. Further, certified software must be brought under control of Currence, and a PIN acquirer must verify the authenticity of the security software before a terminal can be deployed in the field. A certified terminal gets an approval period of 3 years for deployment, after these 3 years re-certification of the terminal is necessary. At the end of the approval period, installed terminals in the field can still be used for another 5 years.
Throughout the years, the certification scheme of PIN has been perceived as playing a significant role in preventing fraud.

3.6. The national Public Certification Authorities

The national Public Certification Authorities are responsible for public security evaluation schemes. These public schemes are used in particular by the payment schemes (except when dealing with proprietary security evaluation schemes).

3.6.1. The Certification Authorities

National Certification Authorities became established in the EU at first for certification of products and systems based on ITSEC\textsuperscript{10} in 1991 or later and to this day more focused on the certification based on the Common Criteria.

The Certification Authorities are either established under the provisions of a law, subsidiary legislation or other official administrative procedure valid in the country concerned or accredited by an appropriate Accreditation Body. In both cases, it is to meet either the requirements of EN 45011 or ISO GUIDE 65.

The Certification Authorities or Certification Bodies (CBs) as usually referenced, are not only responsible for the certification of products and systems but also for other functions listed below - e.g.:

- to authorise the participation of Evaluation Facilities in the Evaluation and Certification Scheme
- to ensure the equivalence of all certification results
- to monitor the performance of participating Evaluation Facilities and their adherence to the agreed evaluation criteria and evaluation methods
- to issue additional guidance to Evaluation Facilities as required
- to monitor every evaluation in progress within the Scheme
- to review all evaluation reports to ensure that the conclusions are consistent with the evidence adduced and that the agreed evaluation criteria and evaluation methods have been correctly applied
- to produce a Certification Report in respect of each evaluation completed under the auspices of the Scheme
- to issue and publish certificates and also publish their associated Certification Reports
- to ensure that the rules of the Scheme are followed.

3.6.2. Country examples

The national CB in Germany

As one of its many activities aimed at increasing IT security, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI), established by law in 1991, provides a certification service whereby IT products and IT systems are evaluated in respect to their security capabilities.

The technical evaluations of a product aimed at certification are generally performed by one of the 13 Evaluation Facilities which have been accredited and licensed by the BSI.

The issue of these security certificates for IT systems and components (41 CC certificates have been issued by the BSI in 2005) is governed by the “Act of the establishment of the BSI”\(^\text{11}\) (BSI-Errichtungsgesetz) and a Certification Ordinance (BSI-Zertifizierungsverordnung-BSIZertV).

Demand for CC certification has been increasing steadily within the past years and concerns a wide range of products implemented in either hardware or software or a combination of both. One important area is the certification of smartcards or smartcard components. A complete list of certified products is available at [www.bsi.bund.de/zertifiz](http://www.bsi.bund.de/zertifiz).

The national CB in UK

The UK IT Security Evaluation and Certification Scheme was established in December 1989 to evaluate and certify the trustworthiness of security features in Information Technology (IT) products and systems. The scheme Certification Body is part of CESG, a government organisation, which is the UK’s national technical authority for information assurance. The Common Criteria scheme uses four commercial laboratories (which are licensed by CESG and also independently assessed for ISO purposes). Demand for certification has been increasing recently from an annual level of around 12 certificates. Published certificates can be found on the CESG website at [www.cesg.gov.uk](http://www.cesg.gov.uk). (NB where the sponsor only requires confidence for internal reasons the certificate may not be published)

The national CB in France

Information Technology Security Evaluation (with ITSEC) began in France under the aegis of Ministry of Defence in 1991. Central Directorate for Information System Security (Direction Centrale de la Sécu-rité des Systèmes d’Information (DCSSI, previously SCSSI)), organisation which depend on Prime Minister, was designed by law in 1995, then by decree in 2002 as the authority in charge of the management of the French evaluation and certification scheme in the area of IT Security.

The decree allows DCSSI to use any criteria. For the time being criteria used are essentially CC and ITSEC.

The technical evaluations of a product aimed at certification are performed by one of the five Evaluation Facilities. A specificity can be highlighted: The French scheme considers

\(^{11}\) Act of the establishment of the BSI of 17 December 1990, Bundesgesetzblatt I p. 2834.
two domains for licensing ITSEF\textsuperscript{12}: "hardware product and embedded software" and "software and network product".

Due to the French market, certified products are mainly in the area of electronic components and smart cards. The level reached is generally EAL4\textsuperscript{13} or EAL5+ (VLA.4). Nevertheless, since few years, software certified products are increasing. In 2005, DCSSI issued 52 certificates. The list of “public” certificates can be found at the following URL: http://www.ssi.gouv.fr/en/confidence/certificats.html (some sponsors don’t want to have their certificates published. They generally use it as an input for their own internal approval process e.g. banking cards and others organisation).

3.6.3.  European Recognition Agreement

To avoid multiple certification of the same product (and the same protection Profiles\textsuperscript{14}) in different countries, the IT security certificates issued are mutually recognised under certain conditions, provided that they are based on the ITSEC or the Common Criteria (CC – see annex 5). Certificates issued in one signatory state are therefore mutually recognised in the other signatory states.

In March 1998, an agreement on the mutual recognition of ITSEC certificates came into force (SOGIS-MRA), which defines the conditions under which ITSEC certificates of IT products are recognised. It was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, and the United Kingdom.

This agreement replaces previously existing bilateral agreements between BSI, the UK ITSEC Scheme and the French certification body SCSSI. The agreement on the mutual recognition of IT security certificates based on the CC was extended up to and including the evaluation level \textbf{EAL7}.

The signatories of the SOGIS-MRA are separated in "Certificate Producing" members who are authorised to issue certificates and "Certificate Consuming" members who recognise these certificates.

<table>
<thead>
<tr>
<th>Certificate Consuming</th>
<th>Certificate Producing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portugal</td>
<td>France</td>
</tr>
<tr>
<td>Switzerland</td>
<td>Germany</td>
</tr>
<tr>
<td>Sweden</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Finland</td>
<td></td>
</tr>
<tr>
<td>Greece</td>
<td></td>
</tr>
<tr>
<td>Italy</td>
<td></td>
</tr>
<tr>
<td>The Netherlands*</td>
<td></td>
</tr>
<tr>
<td>Norway*</td>
<td></td>
</tr>
<tr>
<td>Spain*</td>
<td></td>
</tr>
</tbody>
</table>

\textsuperscript{12} Information Technology Security Evaluation Facility.

\textsuperscript{13} Evaluation Assurance Level, please refer to Annex 5 on Common Criteria.

\textsuperscript{14} Please refer to Annex 5 on Common Criteria.
3.6.4. **Actors involved in the CC evaluation**

Usually, three parties are involved in the certification and evaluation process: The applicant, the licensed evaluation facility selected by the applicant and the certification body. The Evaluation Facility must fulfil two conditions:

- it must be accredited by an Accreditation Body officially recognised in the country concerned
- it must be licensed by the Certification Body responsible for the management of the Scheme.

Accreditation entails the Evaluation Facility's demonstrating its impartiality and its general technical, methodological and procedural competence and in particular that it meets the requirements of EN 45001 or ISO Guide 17025 in so far as these requirements are consistent with the peculiarities of the domain of IT security.

3.7. **Other parties: Evaluation laboratories**

3.7.1. **Evaluation laboratories: Role and Responsibilities**

Evaluation laboratories, also called ITSEF (Information Technology Security Evaluation Facilities) are actors of the evaluation/certification schemes.

The overwhelming majority of evaluations are conducted using the Common Criteria methodology. As a highly methodical approach Common Criteria is in a good position to provide a standardised basis for the evaluation work. But Common Criteria is a methodology aiming at covering the complete IT product range. Products summarised under the term “IT” are very diverse and therefore any evaluation methodology must be defined in a generic way. For use with specific product ranges it is essential that adequate interpretations are defined that translate the generic rules into the actual situation of these products.

For smartcard products, the European certification bodies BSI, CESG, DCSSI, CCN and NSCIB which cooperate in JIL (Joint Interpretation Library) put supported by the industry a high effort into interpreting the CC methodology for the use in smartcard security evaluations. This effort is rewarded by an ever increasing acceptance of the Common Criteria by manufacturers as well as users.

Basically, all the technical tasks of an evaluation are performed in the ITSEF. The ITSEF proposes to its Certification body a report describing all the work performed associated with a verdict. The Certification Body analyses the report, validates the work and emits the Certificate.

Because evaluations are standardized (The Common Criteria or ISO 15408 norm) and because Certificates are recognized internationally through the CCRA (Common Criteria Recognition Arrangement)
Recognition Arrangements), evaluation results must be equivalent independently of the laboratory performing the work. To ensure this equivalence (or at least comparable results) a laboratory has to follow some rules, to justify of an internal methodology guarantying a constant quality level and to be aware of the state of the art of the attacks on the evaluated products.

Rules depend on the scheme, but a strong common kernel exists:

- Independence of the laboratory
- Security & Confidentiality
- ISO/CEI 17025 compliance
- Means and competences
- Knowledge of the state of the art of attacks, Internal R&D on attacks

3.7.2. Independence of the laboratory

The laboratory must show that it is independent of any developer and that there is no possible conflict of interest during the evaluations.

3.7.3. Security & Confidentiality

Because of the sensitivity of the information managed by the laboratory:

- Critical know how of the developers
- Potential vulnerability of products on the market
- “Teaching” of hackers

Laboratories must set up a policy of managing the confidentiality (physical security, personnel security, dedicated and protected areas, etc).

3.7.4. ISO/CEI 17025 compliance

To guarantee stability in the results and to avoid as much as possible variability in the evaluation, the laboratories must define and apply a Quality System compliant to the ISO/CEI 17025 norm.

This compliance guarantees that the evaluation process is managed in an adequate way (internal methodology, management of the competence of the personnel, management of the equipments and tools involved in an evaluation).

The compliance is checked periodically by an independent institution (COFRAC in France) and is formalized by the accreditation of the laboratory.

Depending on the national policies, this norm could be adapted by defining local interpretation, detailing the technical areas covered by the accreditation. For example, in France, the program 141 of COFRAC covers all the evaluation tasks and competences by level (in accordance with the evaluation levels of the Common Criteria, the EALs) but
excludes the management of the competences and the tools related to attacks on the evaluated products (these elements are checked directly by the Certification Body).

3.7.5. **Means and competences**

Because testing, in the sense of vulnerability analysis and attacks, is very specific and different of the developers point of view of functionally testing the product, a specific competence has to be developed in the laboratory.

Various approaches are used over Europe. Some Schemes request the laboratory to own themselves all the equipments, some to have an access independent of the involved developer and some accept for the lab to use the developers’ equipments. In all the cases, a specific competence of using the equipments for attacks is necessary.

3.7.6. **Knowledge of the state of the art of attacks, Internal R&D on attacks**

At the heart of every security evaluation is the vulnerability analysis, penetration testing and assessment. Any security evaluation methodology can only be as good as the underlying security test methods. For example the attack methods for the smart card product range cover diverse fields of expertise such as e.g. physics, informatics and cryptography. The use of these different types of expertises for attacks is very complex.

Potential attackers have no rules, and the area of attacks is evolving extremely quickly. During the last ten years at least 3 or 4 generations of products were developed, and attacks have done tremendous progress. The basic idea of the evaluation/certification scheme is that the evaluators, having high competences, having access to top level equipments, and seeing all the evolution of the products, are in advance of the hackers. This can only be maintained by internal R&D.

Nonetheless the evaluation scheme must ensure that a homogeneous understanding of “state-of-the-art” attack methods exists across the participating evaluation labs and is applied accordingly. To promote this task for the field of ICs and smart cards, JIL has a working group “JHAS” (JIL Hardware-related Attacks Subgroup)\(^\text{15}\) where all the major players in the smart card field work together in order to constantly update and adjust countermeasures: Representatives of IC-vendors, card vendors, evaluation labs, certification bodies and service providers come together and pool their expertise to assess the “state-of-the-art” and “best practice” for security evaluations of smart cards. As a result of this wide ranging expertise a comprehensive picture of “state-of-the-art” attack methods was compiled and is summarised in the document “Application of Attack Potential to Smartcards” which is now a compulsory CC document.

3.7.7. **Scheme licensing**

Due to the specific knowledge requested to evaluate a specific product and to the differences between the products (vulnerabilities of an internet server are certainly not the same than those of a smartcard), some Schemes license the laboratory for a specific area. For example, in addition to a Common Criteria level (EAL), France licenses laboratories for either hardware products or software products.

\(^{15}\) This initiative first started in 2000 as ISCI, International Security and Certification Initiative. This group managed to finalise a Catalogue of relevant attacks methods on ICs and smart cards, with description of key factors and harmonised security ratings based on these attacks.
4. SECURITY EVALUATION PROCEDURES

Section 4 presents in the first place (see subsection 4.1) an overview of the security evaluation procedures implemented in Europe, following a survey conducted by the FPEG subgroup. Secondly (see subsection 4.2), it presents a comparison of the coverage of security criteria as regards cards on the basis of a survey done by Eurosmart. Finally (see subsection 4.3), it provides a description of the ongoing initiatives to harmonise or align evaluation procedures and/or requirements. This relates in particular to the CAS initiative, to harmonisation features of proprietary systems such as PCI and EMV and to initiatives in relation to the harmonisation of site certification requirements.

4.1. List and overview of the security evaluation procedures implemented

The Subgroup conducted a survey in order to identify which security evaluation procedures are used at present in the different EU Member States and for which products and components.

4.1.1. The survey on manufacturers

The questionnaire to the manufacturers was addressed to the Members of Eurosmart, Smart Card, chip and terminals manufacturers. The replies received from the members can be considered as representative of the payment cards and systems manufacturers (3 parts – card and chip products, terminal and site).

The main conclusions that can be drawn from the manufacturers’ replies are the following:

• The hardware part of the smart Card that is developed by Semiconductors industries is preferably (systematically) evaluated using Common Criteria as most of markets accept and recognize Common Criteria security evaluation.

• The Software part of the smart Card is evaluated according also to Common Criteria but also as required by the market FIPS and other schemes (VISA, ZKA, ….)

• The smart card industry wishes that all evaluation schemes converge into one single scheme.

Looking at the terminal products security evaluation scheme, PCI is widely used but national processes are still present in many countries.

4.1.2. The survey on the banking & payment industry

The questionnaire to the banking sector was addressed to the European Payment Council Security of Payments Task Force (EPC SPTF). Although replies were received only from some countries, they can be considered as representative as they include most of the countries where security evaluation of chips, terminals and software is carried out on a large scale and where the laboratories specialised in testing IT products are located. The main conclusions that can be drawn from the banks' replies are the following:

Conclusions from the SPTF questionnaire

16 See Annex 5 on Common Criteria.
The questionnaire to EPC OITS SPTF has resulted in 7 national responses and a submission on behalf of CAS, the European Common Approval Scheme. The following assessment is on the supplied responses and some general knowledge of the changing situation in Europe resulting from new initiatives and threats.

In general, security evaluation of products and processes is widespread, and has largely been based on national banking approaches addressing specific topics, such as the processes and procedures in place to ensure the security of the processes, procedures and products relating to a national cheque guarantee card scheme. In many cases these national evaluation schemes have been formalised by regulation and sometimes by legislation.

The pressures to change have arisen from the use of new technologies such as those associated with PKI and chip cards. In some cases this calls for new evaluation methods, and in others - more difficult - the revision of existing schemes to take account of the new technologies. Other pressures have arisen from the realisation that evaluation needs to address pan-European and international recognition, since systems and products are increasingly required to handle overseas cardholders, international payments and multinational product suppliers. There is also pressure from suppliers of products and services to minimise the number of different schemes which audit them and evaluate their products.

These pressures have given rise to increased recognition of international / mutually recognised accreditation and certification schemes such as ISO 27001 (known previously as BS 7799), Common Criteria\(^{17}\), FIPS 140-2, the European Common Approval Scheme. There is not unanimous support for these, and these schemes are themselves are adjusting to address new requirements. For example, ISO is standardising FIPS 140-2, and there are initiatives to ensure that Common Criteria laboratories will have a shared knowledge of the latest threats on cards and terminals. The international payment schemes (MasterCard, Visa, American Express and others) are also extending their Payment Card Industry (PCI) initiatives on products and processes, and have formalised their management into the PCI Security Standards Council. It is expected that the adoption of international and pan-European evaluation schemes will grow as new systems are introduced, and as the schemes become established.

Because existing evaluation methods have become established in the laws and procedures of many countries they tend to change only when forced to do so by external pressures and new circumstances. This ensures a degree of stability and allows time to assess the various new schemes and ensure that they are fit for purpose. Many of the remarks in the questionnaire responses indicate the tension between stability and recognition of new and potentially more interoperable schemes.

4.1.3. Certification of production sites

The risk evaluation of the product might affect the production risks and have an influence on the production environment. The security evaluation procedures do not only cover products and components, but also the certification of their production sites. Analysing the answers to the questionnaire from the physical security of manufacturing and personalisation sites, the picture is the same, each issuers has its own set of

\(^{17}\) See Annex 5 on Common Criteria.
requirements, its own certification procedure, its own accreditation scheme for auditors (VISA, GIE CB, MasterCard, APACS as well as organisation outside the banking sector such as GSMA). The industry suffers today of a lot of audits dealing with the same topics. Nearly 80% of the standards are equal, but there is a big space for interpretation by the auditors which gives too much room for subjectivity. Furthermore there seems to be a lack of risk orientation in the standards which might not bring more security, but costs for the industry and sometimes even security gaps on other fields.

4.2. **Comparison regarding the coverage of security criteria**

A survey on the coverage of security criteria for cards (but not terminals) was undertaken by Eurosmart Security Working Group in October 2004 for 6 private/national/international Schemes (A to E) + Common Criteria (CC)\(^{18}\).

The various schemes have been compared bearing-in-mind a common understanding of what would be an efficient evaluation: a well-defined, stable and common methodology, a sizeable correctness effort, at optimised costs and duration. In addition repeatable tests with a common scale, consistent with risk analysis and clearly defined security objectives would be part of a good evaluation.

Security evaluation schemes have been compared against the following seven aspects: coverage, depth of tests, product design and source code analysis, design assurance evaluation, environment development and production. Attack sharing is concerned with laboratories sharing knowledge on attacks.

**Coverage (Threats covered by security functions)**

Coverage is related to the scope of the evaluation. It provides an indication of which security functions related to threats and policies will be considered. Also included here is to which extent all feasible and known attacks are part of the evaluation. In other words, coverage defines the comprehensiveness of the security evaluation.

In some schemes the evaluation comprises only some cryptographic functions, assuming that security is only based on Cryptographic functions.

The CC scheme has been rated ‘10’ as it assures by definition (since compliance to well-accepted Protection Profiles is mandated) application oriented security functions and a high resistance against state of the art attacks (Assurance Level EAL 4+ with AVA_VLA.4 highly-resistant assumed).

**Depth of tests: Penetration Testing / Depth of security tests**

Depth of tests is related to security functions & penetration testing and to which extent these tests are performed. Therefore the rating is based on whether both aspects are covered and how rigorous the tests are.

Some schemes just require a list of attacks to be performed, where this list slightly differs from scheme to scheme. Sometimes security function testing is included.

\(^{18}\) See Annex 5 on Common Criteria.
Within a CC evaluation comprehensive security functions and penetration testing is mandatory. The ATE class (testing) forces the developer and evaluator to strive for maximum test coverage. The need to be highly resistant (AVA_VLA.4) forces the evaluator to perform highly sophisticated penetration tests using sophisticated or bespoke equipment.

**White Box Testing**

White Box testing is related to product design information and source code analysis. When conducting White Box testing in contrast to Black Box testing product design information and source code analysis is mandatory. The assessment by the evaluator of the resistance to attacks is based on detailed knowledge of the product and the implementation of the security functionality. A penetration test is therefore better targeted and more effective. This 'White Box Testing' is therefore rated ‘10’.

Just doing the tests without knowledge about implementation details is considered to be 'Black Box Testing’ and rated '0'. In the case where some implementation details are considered it is defined as the "grey box area" and rated accordingly.

The source code analysis permits the exploitation of potential weaknesses in the implementation. It therefore allows the evaluator to derive and refine penetration testing and to develop the most appropriate attacks. Product Design Analysis also covers design information on the hardware.

**Design Assurance Evaluation. (Design Ass. Eval.)**

From security requirements to implementation, the developer has to prove to the evaluator that the security functionality is consistent and covers all the threats appropriately and that all the security functions are correctly implemented in the product.

Only 2 schemes (CC is one of them) require product design evaluation. In these 2 schemes the developer has to prove that each defined security requirement is well specified, methodically designed and tested. This design assurance evaluation provides the foundation for the “White Box evaluation” described above.

**Environment (Development and Production)**

Evaluating a product and its related environment provides confidence in its security level (functional analysis and testing; development and production environments; delivery and deployment; application of defined counter measures in the environment of use).

If the entire environment of the development/production is well audited we rate it as ‘10’, if no audit is made, the value is ‘0’. In some cases, this environment is ignored, in some others it just involves a visit to development or production sites.

In the case of CC, the developer has to prove that the security measures are sufficient to maintain the security of the entire product under development. Security of the production environment may be included as well if within the scope of evaluation of the product. CC can therefore cover the complete development and production life cycle phases.

**Attack Sharing**
This concerns whether laboratories are (or not) sharing knowledge of the existence, the importance and the required skills for attacks.

In contrast sharing of attack information is an inherent part of the CC scheme. The certification bodies ensure that labs operating under the scheme have the capability to perform “state-of-the-art” security testing. The definition of “state-of-the-art” is derived and updated from a wide basis to which all labs have to contribute.

The certification body under the CC scheme requires that the evaluator performs an adequate and complete execution of all relevant “state-of-the-art” security tests.

**Mapping Robustness and Correctness**

As an illustration of the previous section, the Figure below compares assurances of correctness and robustness resulting from the chosen evaluation schemes.

![Mapping Robustness and Correctness](image)

Note: Rating (average) is based on industry’s knowledge and experience of the compared schemes at the time they evaluated their products

Only schemes D and CC reach a high level of assurance of correctness. Only schemes B and CC reach a high level of assurance of robustness.

The Common Criteria scheme is the only methodology allowing attainment of the highest level of assurance of both robustness and correctness, due to the comprehensive white box analysis and the required expertise performing robustness analysis. This includes strong product design information and source code analysis, the mandatory definition and analysis of function strength, and the significant spent time performing penetration testing based on vulnerability analysis. One of the major advantages of Common Criteria is the comparability of the results.

All relevant evaluation schemes, private, national and international, have been considered equally, keeping in mind, the objective of answering the market need for security assurances.

This survey confirms the growing need for product security. It also demonstrates that the Common Criteria is the only methodology which attainment of a high level of assurance of both robustness and correctness, therefore providing the highest level of confidence for critical applications.
4.3. Ongoing initiatives to harmonise or align evaluation procedures or requirements

4.3.1. Introduction

The survey conducted shows that security evaluation procedures are not yet harmonised in Europe, even if in many countries the same procedures are used for the same products and components.

The practical consequences of this situation may be the following:

- Heterogeneous testing procedures do not ensure full comparability between similar items (e.g. two different software modules, cards or terminals) tested in different Member States. Moreover, information is generally not entirely provided about the tests performed and on the detailed criteria for approval or non-approval. It may therefore be difficult for service providers, merchants and consumers to know to what extent a product offered by a manufacturer is more secure than another one. This situation may have an impact on strategic security decisions and on users’ confidence.

- Product certification delivered in one Member State may not be recognised in other countries (or even by other schemes in the same country), if they implement different and/or additional security requirements for evaluation.

- Certification procedures are requiring rather long evaluation efforts and represent a substantial cost for the manufacturers, especially if they need to be undertaken in many countries.

In recent years, work has been undertaken towards establishment of standardised security requirements, which would facilitate an objective evaluation of the security level of products and systems. These initiatives cover different issues.

In this context, the EPC has defined in September 2006 a process for standardisation in SEPA card schemes. It establishes priorities and capitalises on existing initiatives. One of those priorities is security evaluations and the corresponding initiative is CAS. The work of EMVCo in card security evaluations and the security requirements issued by PCI for terminals are also mentioned. The process ensures a free access to standards. The EPC and each initiative will agree on business requirements and on work to be completed, in terms of deadlines and deliverables. The EPC will decide whether the implementation of a standard is recommended or mandatory. If it is mandatory, the EPC will also determine the implementation date.

4.3.2. The CAS initiative

Security experts of European card schemes have been meeting regularly since 3Q 2004. Their aims are to (1) define common security requirements for card scheme components (products, services, processes), (2) define common methodologies for security evaluations, (3) establish and operate a scheme enabling mutual recognition of security certificates between card schemes.

EPC has requested CAS to include functional certificates as well in the mutual recognition scheme. Other standardization groups provide the functional testing requirements and the methodology.
CAS agrees business requirements with the EPC.

CAS does not expect any commitment from payment schemes and payment institutions to adopt its standards and processes. This kind of governance is left to payment schemes and to the EPC, within the guidelines defined by overseers (the European Commission, Central Banks).

CAS consults with all interested parties. Especially, it consults with manufacturers / service providers and evaluators about the feasibility of components compliant with the requirements and about the adequacy of the evaluation methodologies. Professional associations such as Eurosmart greatly facilitate this.

CAS takes into account the requirements of the overseers as follows.

CAS defines security requirements on the basis of Risk analyses that can be presented to central banks. CAS selects evaluation methodologies that provide sufficient evidence to meet the overseers’ expectations.

Financial institutions can include CAS risk analyses and evaluation processes in their Basel II advanced risk measurement.

Many cards issued in SEPA bear two brands. The domestic brand provides acceptance locally and the worldwide brand provides acceptance in the rest of the world.

Similarly, many SEPA terminals accept also cards issued outside SEPA and bearing a worldwide brand.

Therefore, in the interest of SEPA card schemes, CAS maximizes commonalities with the standards defined by worldwide schemes, as long as they suit the European environment.

Aversion to risk is a characteristic of the European environment, as demonstrated by the early adoption of smart cards and the preponderance of debit cards.

CAS has initiated talks with PCI and EMVCo to avoid redundant evaluation work.

In view of the ECB’s desire to see emerge at least one more European bank-owned card scheme next to Visa and MasterCard (“The Eurosystem’s view of a SEPA for cards“, November 2006), CAS adopts an independent stance with respect to PCI and EMVCo, so as to be able to serve equally all SEPA card schemes.

CAS first priorities are cards and terminals.

For smart cards, CAS has issued security requirements and has elected the Common Criteria evaluation methodology. CAS has established a dialog with the European CC schemes, which it will trust with smart card evaluations. CAS is therefore ready for smart card evaluations.

For terminals, security requirements will be released in March 2007. The evaluation methodology will be defined by mid 2007, making evaluations possible in 3Q 2007.

Work is in progress on a scheme enabling mutual recognition of certificates between card schemes, with the aim to have it operational at the end of 2007.
CAS main targets are

- Benefit from existing industry or official ISO/CEN standards like Common Criteria, PCI PED and advanced regional markets within SEPA.
- Build a future oriented security and certification standard compliant to the SEPA Cards Framework
  - To benefit from nowaday’s investments in advanced IC technology within SEPA,
  - By enhancing PCI PED by requirements to protect banking assets beyond the cardholder PIN to be protected by the whole terminal according to European state of the art technologies
  - By taking into account the ECB’s requirements on transparency and
  - By harmonizing certification over all types of POS or ATM devices.

4.3.3. Harmonisation features of PCI

In recent times the major global card schemes established Payment Card Industry (PCI) with the aim to cooperate in the harmonization of non-competitive issues such as security requirements and associated processes. The main reason for this was to avoid the danger of having conflicting and/or redundant security requirements and evaluation processes that would potentially increase confusion and costs. PCI participants were originally MasterCard and Visa. JCB, American Express and Discover Financial Services have since joined them and cooperate in some (not all) of the PCI initiatives.

PCI encompassed many different, but related areas of security in the card payment industry. The more commonly known security programmes are:

- PCI PED, related to the security requirements of PIN Entry Devices
- PCI EPP, related to the security requirements of Enciphering PIN Pads, and
- PCI DSS, related to the Data Security Standards applicable to stored and transmitted data. PCI DSS has the widest acceptance among the global schemes – all members of PCI collaborate on this programme.

The PCI PED and EPP programmes.

These programmes were initiated in 2004 with participation of MasterCard and Visa. Since then, JCB has also joined these programmes. Currently there are 8 laboratories from different world regions individually recognized by the participating global schemes to carry out the required testing for PCI PED and PCI EPP.

Before a laboratory is accepted as a recognized laboratory, there is an initial vetting process where various business and technical checks are carried out. In particular, the credentials of workers in the laboratories are checked, as are the premises and the operating procedures of the laboratory. There are also a number of tests carried out to establish the proficiency of the laboratory personnel, culminating in a test evaluation of a series of products that are crosschecked with the evaluations of other established laboratories. Great effort is expended to ensure that the different laboratories sited in various parts of the world work to the same principles and standards, and carry out comparable evaluations of all relevant devices throughout their operations.
Some documentation on PCI PED programme is publicly available at [www.visa.com/pin](http://www.visa.com/pin). There are further sets of documents available to vendors (so-called DTR – derived test requirements) and participating laboratories (e.g. the actual test procedures used by all the recognized laboratories for their testing of devices, called the DTP - Detailed Test Procedures).

Other PCI programmes are in progress\(^{19}\) or are planned for the future\(^{20}\).

On September 7, 2006, the PCI Security Standards Council was created. Initially, the remit of this Council is to manage PCI DSS. It is planned that other PCI programmes will be taken over by that Council at a near time in the future\(^{21}\).

### 4.3.4. Harmonisation features of EMVCo

EMVCo LLC was formed February 1999 by Europay International, MasterCard International and Visa International to manage, maintain and enhance the EMV™ Integrated Circuit Card Specifications for Payment Systems. With the acquisition of Europay by MasterCard in 2002 and JCB International joining the organization in 2005, EMVCo is currently operated by JCB International, MasterCard International, and Visa International.

EMVCo's primary role is to manage, maintain and enhance the EMV Integrated Circuit Card Specifications to ensure interoperability and acceptance of payment system integrated circuit cards on a worldwide basis. The work of EMVCo is currently divided into eight areas, each supported by a dedicated Working Group. One of these areas\(^{22}\) is Security Evaluation: i.e. development and management of the security evaluations for hardware chip security, as well as Common Core Definitions and Common Payment Application compliant card security.

#### EMVCo - Security Evaluation

The process is based on the established processes already used, for example in IC manufacturer Certification. The EMVCo Security Evaluation Working Group (SEWG) manages and oversees this process. This Working Group consists of a restricted number of participants from each EMVCo Member. The SEWG reviews recommendations on Certification from the Secretariat, and issues Certificates based on this. The Secretariat Function is delegated to the MasterCard CAST Team.

---

\(^{19}\) PCI PIN (establishes common PIN security requirements and management process for Acquirers and/or associated processors), PCI Vendor Security Requirements (covers both Logical and Physical security requirements for all vendors who are involved in card data preparation, management, initialization, personalization or processing).

\(^{20}\) PCI UPT (for Unattended Payment Terminals) and PCI ATM.

\(^{21}\) The current PCI POS PED and PCI EPP security requirements are in the process of being formally adopted by the relevant bodies within the PCI SSD. Such process is expected to be completed by Q2/Q3 2007.

\(^{22}\) The other 7 areas are: Card and Terminal (Management and enhancement of EMV Specifications); Security (definition of security aspects of the specifications and key length review); Terminal Type Approval (Development and management of the test requirements and device approval processes); Interoperability (Management of interoperability problems reported in the field); Common Core Requirements (Management and enhancement of Common Core Definitions (CCD) and Common Payment Application (CPA) Specifications); Card Approval (Development and management of the card approval process for CCD compliant card applications and CPA); and Contactless (Development of the common contactless application kernel and related type approval process for card and terminal).
4.3.5. Harmonisation of site certification requirements

The Security Standard Harmonisation Working Group was launched in April 2006 under the initiative of the Security Manager of smart card manufacturers companies. The group gathers Security Managers of production and personalisation sites in charge of logical and physical security certification, the responsible manager of evaluation and certification/agreements of Visa Europe, MasterCard, GIE Cartes Bancaires, APACS, ZKA as well as GSMA (global GSM operators’ organisations).

Smart Card manufacturers, in 2004, realised a survey on the various existing schemes and came to the conclusions that all schemes have a similar objective, secure site, therefore, 80% of their content is similar. However, all banking organisations still have their own way to implement it, meaning for the industry, more than 400 certifications to take care of on 80 production sites, expenses increasing continuously without any impact on security. The conclusions were presented to the Scheme operators who decided to work around the same table.

The common WG is now meeting every 2 months to agree on a common set of security requirements in a first step and to work on the possibility to adopt a common audit procedure (if validated by all).

5. Views of the Stakeholders

5.1. Views of Administrations

National central banks, as supervisors, are pushing for harmonised solutions concerning standards and evaluation procedures and call the European Payment Council to investigate this area (see annex 3).

Concerning the question of whether this harmonisation should be made mandatory by legislation, some authorities take a clear position on this issue.

The Observatory for Payment Cards Security—a French public body meant to promote dialogue and exchange of information between all parties (banks, merchants, consumers, public authorities) interested in the smooth functioning of card payment systems—strongly believes that user confidence is a key factor of success for the development of pan-European payment services. Indeed, the increased interoperability of upcoming pan-European payment instruments will make them more visible and as such more vulnerable to fraud.

The Observatory welcomes the choice of EMV chip cards as the supporting technology for card payments in Europe, but fears that construction of the European card payments systems leads to a harmonisation to the lowest common security denominator. Experience shows that all cards are not equal from a security point of view; the Observatory therefore promotes the definition by the industry of harmonized high-level security requirements for cards and card accepting devices.

The Observatory believes that the situation in Europe is currently unsatisfactory on that matter because of a double heterogeneity: first, card payment systems do not have the same levels of security requirements;
second, public security evaluation schemes based on recognized international standards coexist with private (and closed) evaluation schemes. Several nearly equivalent evaluations have to be conducted for a same product, which results in longer times-to-market and higher cost for new card technologies.

On that basis, the Observatory promotes the inclusion in the SEPA Card Framework of security requirements for both cards and terminals, on particular based on the works by the Common Approval Scheme (CAS). Then, because harmonisation of security evaluations is needed, the Observatory supports the inclusion in the upcoming Directive on Payment Services of a framework for mutual recognition of security certification of cards and accepting devices.

5.2. Card and terminal manufacturers

Cards and terminal manufacturers are in favour of promoting a high level of security based on common rules and references.

In the process of creating SEPA, efforts should be intensified towards aligning security evaluation procedures and reach a full mutual recognition situation, with a view to achieve interoperability within the European Union and beyond.

Harmonised evaluation criteria and procedures would allow certification performed into one country to be de facto recognised in other EU countries. The overall certification duration and costs would then be substantially reduced and significant savings would be made by the products and systems manufacturers. This could have a critical impact on the time to market of these products, with positive consequences on their price rate.

It is therefore essential to define common ways and means for evaluating and certifying security, possibly at international level, with a view to ensure the transparency of procedures, the comparability of security evaluations and the quality insurance of implemented processes.

For sites certification, a Global Security Standard which is accepted by all Payment Schemes might be of great benefit. It could reduce audits, bring more risk orientation in the process, and help to get more objectivity in the audits.

5.3. Banking sector

The EPC is of the view that further standardisation is needed and is currently working on this issue. EPC has set up a dedicated Standardisation Task Force which works in close liaison with already existing initiatives for standardisation across SEPA. Standards specifications are being developed for cards, terminals and networks, which include minimum requirements, recommended specifications and/or best practice guidelines and a framework for certification.

This work is focusing on 4 domains leading to 5 main initiatives/standards. Among these five initiatives, the Common Approval Scheme (CAS) project, an initiative of several European payment schemes which aims at proposals for:

- minimum security requirements for cards & terminals (‘point of interaction’),
- a Common and Neutral security evaluation methodology (should be the Common Criteria),
- a framework for mutual recognition and type approval across SEPA.
This process however raises the following problems of deciding who will be the EU body/authority for (i) the accreditation/monitoring of the laboratories in charge of evaluations; (ii) endorsement of ‘CAS’ proposals and setting up the security rules for SEPA (CAS is proposing a certain level of security, which is high for cards and is yet to be finalized for points of interaction); (iii) definition of an adequate minimum security level for all payment Schemes across SEPA; and (iv) enforcement of this minimum security level for mutual recognition across the EU?

5.4. Views of merchants

The concerns of the merchants are more on the standard themselves than on the security evaluation procedure. They are in favour of simple standards applying to all machines everywhere: e.g. European and international standards should be as close as possible. In any event, the understanding is that the final level of security should not be for merchants' decision but for the banking sector.

A French national association of merchants, Mercatel, points out that, on the occasion of the issuance of a Data Security Standard by PCI, the following lessons were learnt.

- Security standards for SEPA should reflect a risk analysis specific to the SEPA environment. SEPA specificities are not limited to chip and PIN. For example visual cryptograms are used to secure card-not-present transactions.

- Security standards for SEPA should, to the greatest extent possible, stay at the level of objectives and let merchants propose the solutions best suited for their systems and processes.

- The organisation of security audits of IT systems should include considerations about commercial secret and economic intelligence.

6. CONCLUSIONS – THE WAY FORWARD

Stakeholders are generally of the view that security evaluation procedures should be aligned and mutual recognition achieved throughout the EU.

A formal/neutral method to provide a sound evaluation assurance and to promote the exchange of information on attacks on payment systems to improve vulnerability analysis and penetration testing is needed. It is noted that Common Criteria provides a sound foundation on which to build security assurance, though it needs to be completed by practical implementation details for specific product ranges.

Indeed, cooperation of the concerned stakeholders is key. Security evaluation is based on communication. Open and detailed discussion of attack methods fosters trusts and promotes awareness. Information exchange helps to harmonise vulnerability analysis and penetration testing.

The alignment of security evaluation procedures should result in significant cost reduction while guaranteeing a consistent high security level in the payment area. This should also facilitate meeting the SEPA objectives.

*  *  *

30
List of Annexes

(1) Terms of Reference of the FPEG Sub-group on Security Evaluation and Certification

(2) Glossary of terms

(3) The Eurosystem's view on a "SEPA for cards" – November 2006 (extracts)


(5) Common Criteria

(6) Security evaluation standards for processes: ISO 2700X Series of Standards

(7) Links to relevant websites
Annex 1 – Terms of Reference of the FPEG Sub-group on Security Evaluation and Certification

Scope:

The FPEG Security Evaluation & Certification Sub-group remit covers payment products/components and services used by credit institutions or other assimilated entities that serve to withdraw or transfer funds. It does not cover the single-purpose cards that benefit from an exemption to banking monopoly, according to the European regulations.

Mission:

The FPEG S&C sub-group monitors the implementation of methods adopted by Payment Industry and products vendors for the evaluation and the certification of their products and services in order to strengthen payment systems security. It keeps abreast of the principles adopted with regard to security evaluation and certification methods standardization as well as of the main developments in this area.

In addition, the Fraud Prevention Expert Group may request the FPEG S&C Subgroup an opinion on security issues, setting a time limit for its response. The opinions are communicated to the Steering Committee with recommendations on how to use them.

More specifically, the group will link with existing initiatives such as CAS and ISCI and provide recommendations on the best available methodology.

---

23 ISCI (International Security Certification Initiative) was launched by Eurosmart

The goal of the ISCI initiative is to define, support and promote a universal framework for security evaluation and certification methods, tools and procedures, based on internationally accepted standards”. (http://www.eurosmart.com/isci/index.htm)
Annex 2 – Glossary of terms

**Accreditation**: The procedure for recognising both the technical competence and the impartiality of a test laboratory to carry out its associated tasks.

**Assets**: entities that the owner of the TOE (see Target Of Evaluation) presumably places value upon [CC]

**Assurance**: grounds for confidence that a TOE meets the SFRs [CC]

**Attack potential**: a measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation. [CC]

**Certification Process**: The certification process is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval, which is normally publicly available. The certification process is a means of gaining greater consistency in the application of IT security criteria. [CC]

**Certification authority (CA)**: A trusted authority to create and assign certificates.

**Certification body (CB)**: An independent and impartial national organisation that performs certification.

**Cryptography**: The science of cryptographic operations that is used to transform data in order to hide or reveal its information content.

**Development environment**: the environment in which the TOE is developed. [CC]

**Evaluation**: assessment of a PP, an ST or a TOE, against defined criteria. [CC]

**Evaluation assurance level (EAL)**: an assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale. [CC]

**Evaluation authority**: a body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community. [CC]

**Evaluation scheme**: the administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community. [CC]

**Evaluation Task Report (ETR)**: Report issued by the evaluator that contains a summary of evaluation tasks activities and results verdicts (Pass/Fail). The ETR is the conclusion of the evaluation process.

**Integrated circuit(s) (IC)**: Electronic component(s) designed to perform processing and/or memory functions contained on a single chip.

**PP evaluation**: assessment of a PP against defined criteria. [CC]

**Protection Profile (PP)**: an implementation-independent statement of security needs for a TOE type. [CC]
Security objective: Statements of intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions [CC]

Security Target (ST): an implementation-dependent statement of security needs for a specific identified TOE [CC]

ST evaluation: assessment of an ST against defined criteria. [CC]

Security Functional Requirements (SFR): translation of security objectives for the TOE into a standardized language. [CC]

Smart Card: An Integrated Circuits Card (ICC); A Card into which has been inserted one or more ICs. Smart Cards are widely used ad Banking Credit/debit Cards or electronic money purse (e-Purse).

Target of evaluation (TOE): a set of software, firmware and/or hardware possibly accompanied by guidance. [CC]

Testing -White Box testing: Penetration testing performed by the evaluator with the knowledge of the source code of the TOE and therefore the implementation of security functions.

Testing- Black box testing: Penetration testing performed by the evaluator without the knowledge of the source code of the TOE.

Abbreviations:

CC: Common Criteria

CCRA: Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security [CC]

DPA: Differential Power Analysis- Mean used by attackers to extract secret information based on the statistical analysis of the power consumption on Smart Cards and other cryptographic devices.

ECB: European Central Bank

EMSSO: Electronic Money Security Objectives

ENISA: European Network and Information Security Agency

EPC: European Payment Council

IT: Information technology

ITSEF: Information Technology Security Evaluation Facility

ISCI: International Security Certification Initiative

R&D: Research and Development

SEPA: Single European Payment Area
**SPA**: Single Power Analysis: Mean used by attackers to extract secret information based on the analysis of the power consumption of Smart Cards and other cryptographic devices.

**Standards**

CC: Common Criteria CCV3.1 – September 2006


BS7799: BS 7799-3:2005 Information security management systems. Guidelines for information security risk management.

"To ensure that cardholders can use their SEPA cards across the euro area, it is important to ensure that merchants can accept all SEPA cards as long as this makes economic sense for them of course. To secure this objective, there should be no technical barriers to competition. Standards are the basis for open and fair competition. They should cover every phase of the transaction chain (cardholder-to-terminal, terminal-to-acquirer and acquirer-to-issuer), the security evaluation and the certification of devices. Concerning terminals in particular, standardisation and the definition of an adequate and independent certification body is essential to ensure that any card can be accepted at any terminal. The EPC should investigate how the objectives of the SCF, especially interoperability, could be ensured by the card standards which are currently under development. Participation in the definition of standards should be open to all stakeholders. The outcome must be mandatory for the entire market, without any opt-out possibilities and with clear implementation deadlines.

In addition to technical standards, additional requirements in terms of business rules and practices are needed to ensure that cardholders have access to many POS terminals. This will also contribute to creating a level playing-field for inter-scheme competition."

Uniform standards will ensure a technical level playing-field for all euro area card schemes and infrastructure/service providers. Standards should cover every phase of the transaction chain (cardholder-to-terminal, terminal-to-acquirer, acquirer-to-issuer) and the security evaluation and certification of technical devices (in particular concerning terminals whereas standards and an adequate and independent certification body need to be set up in order to ensure that different payment applications coexist) and also focus on preventing fraud.

It is important that all stakeholders are free to participate in the definition of standards, which should be neutral, future-oriented and not nationally biased, with the aim of guaranteeing universal adoption and avoiding placing particular infrastructure/service providers in a better starting position. Standardisation will empower competition forces (which up to now have been limited within national borders), and will encourage efficiency, innovation, and better services and prices. The EPC is currently working on such standards, which the Eurosystem expects will be compulsory for all stakeholders."

"STANDARDISATION

24 For the full text, see http://www.ecb.int/paym/pol/sepa/html/index.en.html
To ensure cardholders can use their SEPA cards across SEPA, it is important to ensure that merchants are able and willing to accept all SEPA cards, or at least all the cards that are relevant for them. To secure this objective, work on standardisation is of the utmost importance. Technology should not be a barrier to competition. Uniform standards will entail a technical level playing-field for all euro area card schemes and infrastructure/service providers. Standards should cover every phase of the transaction chain (cardholder-to-terminal, terminal-to-acquirer, acquirer-to-issuer), as well as the security evaluation and certification of technical devices. Interoperability standards should be mandatory, and should be finalised swiftly in order to facilitate migration to SEPA.

The EPC should investigate how the objectives of the SCF, especially interoperability, could be ensured by the card standards which are currently being developed. Concerning terminals in particular, standards plus an adequate and independent certification body should be set up to ensure the coexistence of different payment applications, so that there is no technical hurdle for any card to be accepted at any terminal. Harmonised and adequate security requirements are needed for a common evaluation process. Two general problems facing a new European card scheme and the current national schemes in the SEPA environment are euro area-wide reachability and the establishment of a transactionprocessing network. The industry could also study the possibility of using the current payment infrastructures, in particular the direct debit ones for the processing of new SEPA card products/schemes.

The payment function needs to be clearly defined, and the various add-ons such as loyalty programmes should not hamper interoperability. Participation in the definition/choice of standards must be open and the outcome mandatory for all parties in order to ensure that standards, especially in the terminal-to-acquirer domain, adequately satisfy the needs of all stakeholders, particularly merchants and cardholders. There cannot be any opt-out options, and a clear implementation deadline needs to be defined. Technical standards alone cannot ensure that the aim of making it possible for every cardholder to use his or her card throughout SEPA is realised. Additional requirements might be needed, for example in the field of business rules and practices, to ensure that cardholders can use their card at every terminal. This will also contribute to creating a level playing-field for inter-scheme competition."
Annex 7: THE EVALUATION OF THE SECURITY OF PAYMENT INSTRUMENTS AND COMPONENTS

- **What is the issue/problem?**

At present, payment instruments and components (chip cards, terminals, etc) are certified by the competent authorities before being put onto EU national markets. They are tested with procedures established by the national certification bodies but which are not harmonised at EU level (methodology; type and number of attacks, etc). The result of different testing procedures is that:

- Full comparability is not achieved between similar items (e.g. two different terminals) tested in different Member States. It is thus difficult for the banks, the merchants and the consumers to know to what extent a product is more secure than another. This situation has an impact on buyers’ decisions and does not foster users’ confidence.

- Certification in one Member State does not mean automatically recognition in the others, as Member States may require different or additional security requirements. In this case, the country with the “strictest” requirements will not recognise a certification carried out in another. This situation is not an incentive to interoperability and is not in line with one of the basis principles of the Internal Market.

- Certification that needs to be undertaken in many countries takes longer and is substantially more expensive. If mutual recognition were to apply in full, the overall certification costs might be reduced and the savings made by the manufacturers could be reflected in the price of the components, with lower costs for banks, merchants and consumers.

Attempts to find objective ways to evaluate the security of payment instruments have been made, namely with moves towards the establishment of standardised security requirements (CC/PP methodology)44. There seems to be broad support for the introduction of this methodology, but in practice it is not being implemented expeditiously.

- **Possible ways forward**

Concerning the evaluation of the security of payment instruments and components, there is general support for the introduction of the CC/PP methodology in the EU. However, during the consultations in preparation for the present Communication a consensus was expressed against the need for legal provisions to support its introduction. According to the payment

---

44 The most relevant example are the Common Criteria/Protection Profiles (now ISO standard IS 15408). In this process, the Common Criteria (CCs) are combined with the Protection Profiles (PPs), which are security objectives related to specific categories of instruments (e.g. smart cards). In the PPs, the security features are evaluated against all the threats that a product and its environment face. Assurances about the security level are given by acknowledged certification bodies, which generally operate under the oversight of an evaluation authority. The certification bodies provide a common evaluation scheme based on common accreditation criteria and testing methodology. PPs on smart cards and other components are being developed in the European Union and in the United States under initiatives of the payment industry and government agencies.
industry, legal provisions might increase the costs of payments and jeopardise future developments and innovation. Work on standardised security requirements would better be left to market participants. On the other hand, if legislation were to prove necessary, respondents considered a Recommendation from the Council and European Parliament or from the Eurosystem as a better alternative than EU legislation. Governments and Central Banks encourage a structured and co-ordinated approach for security evaluation that might avoid high costs and time-consuming procedures. They underline that security issues may be addressed through their oversight role on payment systems and means of payments, which should cover the evaluation and certification of products and systems.

Security evaluation is essential in order to maintain confidence in payments and it is necessary to remove obstacles to the mutual recognition of security evaluations of payment instruments and components in the Internal Market. Therefore the Commission needs to examine in more detail the question of mutual recognition, also in the light of the work already undertaken in the mutual recognition of products. To achieve this objective, the Commission may act as a catalyst in order to clarify the issues at stake, and may reconsider its stance altogether if a harmonised methodology to evaluate security, reduce manufacturing costs and significantly enhance consumers’ and merchants’ confidence in payment instruments is not implemented within a reasonable timeframe by the combined efforts of market participants and other regulators.

The Commission services invite, therefore, views on the importance of this issue. Especially descriptions on any existing problems relating to the mutual recognition are welcomed.
In recent years there has been an increasing demand for certified IT security products. This resulted in an increasing demand for certificates based on the Common Criteria (CC). The Common Criteria represents the outcome of efforts to develop criteria for evaluation of IT security that are widely useful within the international community. It is an alignment and development of a number of source criteria: the existing European, US and Canadian criteria (ITSEC, TCSEC and CTCPEC respectively). The Common Criteria resolves the conceptual and technical differences between the source criteria considering the latest IT security requirements. It is a contribution to the development of an international standard and has been recognised as an international standard (ISO/IEC 15408) by the International Standard Organisation (ISO), and so opens the way to worldwide mutual recognition of evaluation results in 24 nations.

CC is an all-purpose security evaluation CC methodology that needs to be adapted to specific product types, especially the vulnerability scale.

The CC presents requirements for the IT security of a product or system under the distinct categories of functional requirements (CC Part 2) and assurance requirements (CC Part 3). The CC functional requirements define desired security behaviour. Assurance requirements are the basis for gaining confidence that the claimed security measures are effective and implemented correctly.

Evaluation Assurance Levels (EALs) define a scale for measuring assurance of a TOE. EALs are packages of security assurance components that are defined in CC Part 3. The degree of assurance is expressed in terms of increasing, hierarchical levels of rigour from the lowest EAL1 to the highest EAL7.

The CC defines a set of IT requirements of known validity which can be used in establishing security requirements for prospective products and systems. The CC also defines the Protection Profile construct (see below) which allows prospective consumers or developers to create standardised sets of security requirements which will meet their needs.

The Target of Evaluation (TOE) is that part of the product or system which is subject to evaluation. The TOE security threats, objectives, requirements, and summary specification of security functions and assurance measures together form the primary inputs to the Security Target (ST), which is used by the evaluators as the basis for evaluation.

The principal inputs to evaluation are the Security Target, the set of evidence about the TOE and the TOE itself. The expected result of the evaluation process is a confirmation that the ST is satisfied for the TOE, with one or more reports documenting the evaluation findings.

---

To complement the Common Criteria and the Common Evaluation Methodology for Information Technology Security Evaluation, Supporting Documents have been developed. These documents may be „Guidance Documents“, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or „Mandatory Technical Documents“, whose application is mandatory for evaluations whose scope is covered by that of the supporting document.

Protection Profiles

A Protection Profile (PP) defines an implementation-independent set of security requirements and objectives for a category of products or systems (e.g. smart cards) which meet similar consumer needs for IT security. A PP is intended to be reusable and to define requirements which are known to be useful and effective in meeting the identified objectives.

The PP concept has been developed to support the definition of functional standards, and as an aid to formulating procurement specifications.

A PP would be appropriate in the following cases:

• a consumer group wishes to specify security requirements for an application type
• a government wishes to specify security requirements for a class of security products
• an organisation wishes to purchase an IT system to address its security requirements.

Maintaining all laboratories at the same state-of-the-art level rests on the prerequisite that there is a commonly agreed state of the art, i.e. that there is a place for people in the know to discuss this issue confidentially.

CC schemes have made continuous and successful efforts to adapt to customer needs. Payment scheme needs:

– in addition to the certificate, extracts of evaluation technical report are made available to payment scheme for risk management,
– continuous updates of evaluation results for as long as the product is in use.

Manufacturer needs:

– product evaluation reflects the supply chain, parts of the product provided by different manufacturers may be evaluated separately and later composed together,
– a development / manufacturing process may be evaluated separately from the products developed / manufactured. Process evaluation can later be re-used in many product evaluations.
Annex 6 - Security evaluation standards for processes: 
ISO 2700X Series of Standards

This appendix addresses ISO standards in the ISO/IEC 2700x series as the main standards for process evaluation. There are others, such as ISO/IEC 21827 (systems engineering) and ISO/IEC 17025 (competence of laboratories), which address security evaluation in different ways and from specialist viewpoints: but most of these refer to the 2700x standards as their basis.

The 2700x standards refer to the establishment in an organisation of what is referred to as an Information Security Management System (ISMS). The purpose of the ISMS is to ensure that security is an integral part of the organisation's processes.

ISO/IEC 27001 Information technology - Security techniques — Information security management systems - Requirements

This is the standard which establishes the framework for an ISMS, sets the requirements, and refers across to the other standards as appropriate. The standard is the basis for an accreditation scheme similar to that established under ISO 9001 for Quality Management.

ISO/IEC 27002 - Information technology - Security techniques – Code of practice for information security management

This standard is currently known as ISO/IEC 17799, but the plan is to renumber it as 27002. It is a guideline document, but when considered in relation to 27001 the guidelines become requirements for gaining accreditation. It addresses many aspects of managing security: internal organisation; dealing with external parties; asset management; people management; physical and environmental security; communications and operations management; access control; systems acquisition, development and maintenance; incident management; business continuity; compliance with legal requirements and security policies; and audit considerations.

ISO/IEC 27003 - Information technology - Security techniques – Information security management system implementation guidance

This is a guideline document that is currently under development.

ISO/IEC 27004 - Information technology — Security techniques — Information security management metrics and measurements

This is another work-in-progress standard, which provides support for the other parts of the standard. It addresses establishing procedures and metrics for defining implementation objectives and effectiveness criteria for the ISMS, and tracking and measuring its evolution and effectiveness over time. It provides guidance on how an organization, through the use of metrics, may identify the adequacy of its security controls, policies, and procedures and develop a program to measure Information Security performance.

ISO/IEC 27005 Information security risk management
This standard will allow an organisation to assess risks, identify security requirements and help to establish and maintain the ISMS. It provides guidelines and examples on risk management but does not prescribe specific methodologies.

ISO/IEC 27006 Information technology — Security techniques — Requirements for the accreditation of bodies providing certification of information security management systems

This standard sets out criteria for bodies operating audit and certification of an organizations' management systems. If such bodies are to be accredited as complying with ISO/IEC 17021 and want to audit or certify an ISMS, some additional guidance to ISO/IEC 17021 is necessary and is provided in this standard.

One aim of this standard is to more effectively enable accreditation bodies to harmonise their application of the standards against which they are bound to assess certification bodies. Harmonisation is an important step towards mutual recognition of accreditation. This standard will also be useful to certification bodies themselves and to those whose decisions are guided by their certificates.
Annex 7 – Links to relevant websites

French Observatory: http://www.banque-france.fr/observatoire/home.htm

European Payment Council (EPC): http://www.europeanpaymentscouncil.eu/

EUROSMART: www.eurosmart.com
Common Criteria Portal site: www.commoncriteriaportal.org
Common criteria Annual Conference: http://www.iccconference.com/
Common Criteria 8th Annual Conference: http://www.8iccc.com/
Germany - BSI site: http://www.bsi.bund.de/cc/
Nederlands – TNO certification: http://www.tno-certification.nl

UK – CESG
http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=1


Italy – OCSI: http://www.oesi.gov.it


Norway – SERTIT: http://www.sertit.no/

Sweden – SWEDAC: http://www.swedac.se/sdd/System.nsf/(GUIview)/index.html


ENVCo: http://www.envco.com/