EUROSMART THE VOICE OF THE SMART CARD INDUSTRY

Eurosmart contribution to Europe New Legal Framework for Payments in the Internal Market
(Consultative Document proposed by the European Commission in December 2003)

Smart cards for Payment – A secure tool in need of harmonised rules

---

The smart card has become the major tool in Europe's means of payment. In order to complete the legal framework for payment, the EU Commission is considering the evaluation of the security of payment instruments and components (annex 7). Eurosmart, smart card and secure solutions industry association, wants to bring its expertise to this debate.

As stated in the consultation document of the Commission, security evaluation procedures are not yet harmonised in Europe. The industry is in favour of promoting a high level of security based on common rules and references. Of course, a common reference, will play its role only if accepted and implemented in the same way by all actors.

CONTEXT

Different methodologies exist for security evaluations. Some are operated upon private schemes, other refer to national or international models. However only Common Criteria are acknowledged as a fully international standard and used at a worldwide level. European industries initiated 5 years ago migration towards this ISO standard and have developed their own know-how about CC standard implementation, gaining a great deal of experience. However in the payment area, the situation is still not clarified, knowledge sharing needs to be maintained and can be improved for the benefit of all.

Position of the market actors

In the electronic payment chain, a secure reliable infrastructure associates many actors: Banks, payment organisations at national and international level, chip/IC manufacturers, terminal providers, system integrators and smart card manufacturers. They all have a specific role regarding security issues.

There is no direct link between the manufacturers and the final card holder. Requirements, particularly on security, are established by the payment organisations acquiring the cards. This particular situation becomes more complex when referring to responsibility: research on security is being supported by the industry but the main responsibility of fraud or malfunction falls on the acquirer. This has an impact on the development of security schemes. Each payment provider wishes to develop internally, its "own-better performing" system meaning a proliferation of schemes, while industrial actors favour the convergence towards a unique certification process.

Regulation regarding security evaluation are not sufficient

Recommendations for the promotion of a common reference and method exists: EC Council resolution of 28 January 2002 and European Central Bank document EMSSO released in May 2003 are promoting the reference to Common Criteria methodology for all IT products including smart cards. **Such recommendations are not sufficient.**

The real picture of security evaluation/certification of products and production

Multiplication of Security schemes in the payment sector.

For site security requirements

ORGANISATION	STANDARDS/SCHEMES	AREA
APACS	Apacs*	**Banking**
AMEX	Amex*	**Banking**
CARTES BANCAIRES	CB*	**Banking**
DINERS	Diners*	**Banking**
GSM Association	SAS*	**Telecom**
DIN/ISO	DIN/ISO 17799	**Global**
JCB	JCB*	**Banking**
BSI	Common Criteria	**Global**
	Grundschutzhandbuch	**Global**
MASTERCARD	Security Standards for Vendors*	**Banking**
	Logical Security Standards*	**Banking**
MONDEX	Reference to MASTERCARD	**Banking**
VISA	Security Standards for Vendors*	**Banking**
	Key Management*	**Banking**
German TELECOM	TU4*	**Telecom**
	SiCaS*	**Telecom**

**proprietary Standards*

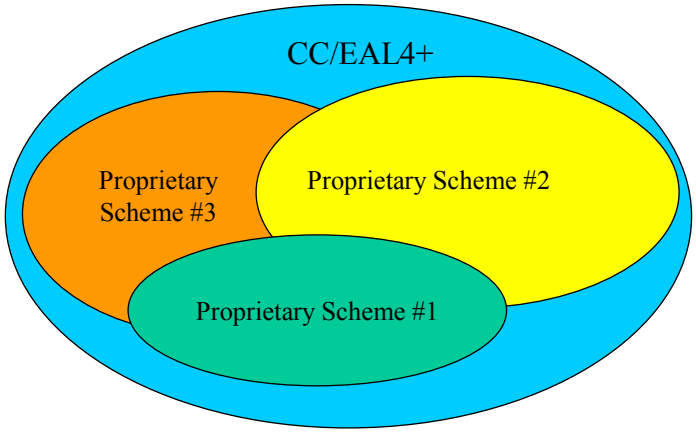
Security certifications come in two flavours: products security certifications (hardware and software) and production sites certification.

For most of the Eurosmart members company, an average of 70 certifications per site is the usual situation having to organise the audit of 11 different “customers” or “authorities”.

This represents a cost reaching well over 500 000 Euro for a manufacturer with 10 different production sites, amount to which all the internal cost for the preparation and administrative tasks of the audit, must be added.

For Products evaluation: Visa, MasterCard, ZKA, Proton and CC schemes are all applicable to payment smart cards. However, when analysing the various requirements, security experts come to the same conclusions: the scope of each proprietary evaluation presents nearly 90% of similarity and CC methods covers all requirements.

Security Evaluation Scope



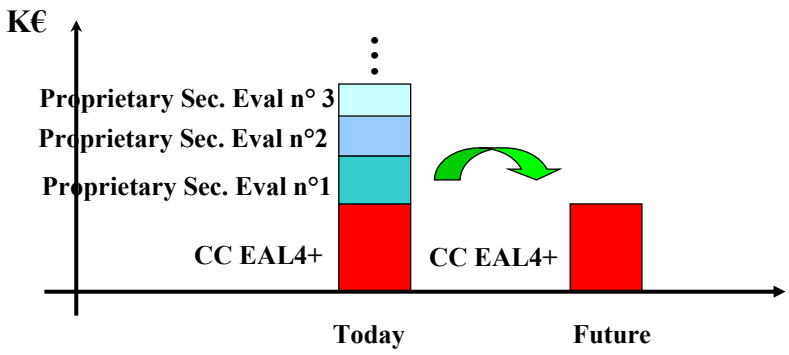
- **Hardware (H/W) and Software (S/W) evaluations**

Moreover, proprietary evaluation are based on a rigid "black box" approach, where the card is tested upon a blind process without knowledge about the product itself (source code, security architecture of the product, etc.). CC method covers all requirements (threats & security objectives). One of the specificities of the smart card industry is to enhance evaluation through a "white box" approach, where source code, security function descriptions, and security architecture are provided by the product supplier. This allows for a complete vulnerability analysis with corresponding dedicated security tests connected with the product specificities.
The difference in term of approach between "black box " and "white box" is fundamental and justifies also the CC approach for a complete security evaluation needed for European banking payment.

The situation today is described in the diagram below: It means time and cost without benefit for the end-users/consumers

Security evaluation cost H/W & S/W

- **Additive cost due to proprietary schemes in terms of evaluation for a same product**



Competition between schemes does not benefit the market and is costly and time-consuming not only for the manufacturers but also for the payment organisations.

It seems that recognition of CC ISO15408 and ISO17799 is effective for governmental applications but not for payment.

Considerable energy and efforts are deployed by market participants to certify their products and production but if it was better rationalised, such efforts could be targeted towards technology improvements and finding security solutions for the future.

Similar issues face the payment terminal manufacturers, with multiple security evaluations and approvals required. The costs of the multiple evaluations do not add to the security of the payment system, and therefore do not provide sufficient cost-benefit to EU constituents. It should be noted that the costs of security approvals are far greater than the price paid to the evaluation laboratory itself. The preparation effort, special documentation, design peculiarities to meet specific testability requirements, support of the evaluation laboratory, etc. typically costs the company seeking security approval between two and five times the laboratory evaluation cost. A typical payment terminal security approvals will cost 100,000€, with Common Criteria security approvals costing up to 150,000€.

Manufacturers of payment terminals therefore universally support a single consolidated set of security requirements with a single security approval. The exact definition of the security requirements and evaluation will need to be determined through close cooperation between all actors in the system including the payment schemes, terminal manufacturers, card issuers, transaction acquirers, and merchant associations. No assumption however should be made regarding the final outcome for the security or evaluation requirements. In particular it would be dangerous to assume that since smart card manufacturers strongly support the use of the Common Criteria for smart card evaluations, that payment terminals manufacturers – many of which are not European - would support the same. Indeed it has been argued that similar levels of assurance can be obtained through less detailed and formal evaluation processes.

EUROSMART CONTRIBUTIONS

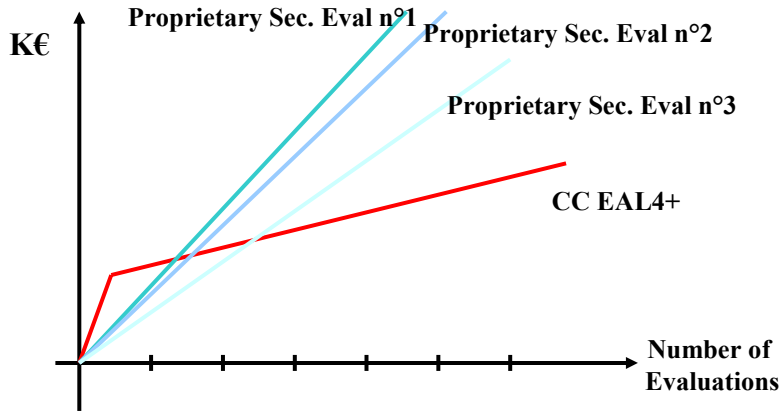
Optimisation of security is one of the main objective of the smart card sector. The history of the Association is closely linked to research in security products and pooling of know-how of the industry experts in that field. Eurosmart security working group was created in 1997 by Michel Ugon, “father” of the French banking card and of the microprocessor card we all use today. For the group, since then, Security is considered as the foundation of the smart card. Defining and promoting a measurable and easy to understand security scale was one of its first mission. It led to the ITSEC metrics adoption, and later to the internationally recognized Common Criteria, now an ISO standard.

Absolute security does not exist but it is indispensable for smart cards in a chain of trust and Eurosmart is continually making progress to secure the whole chain. Generic security requirements, Protection Profiles, have been developed by its members and evaluated by an independent authority. From the beginning, the manufacturers were in favour of the evaluation and certification of their products under a common model, an understandable language, a simple scale (from 0 to 7) global method – Common Criteria (CC) development was the assurance to work under the same procedure and obtain a product meeting the main security requirements avoiding multiple evaluations.

However, it became rapidly clear that the CC methodology was to be adapted to the smart card chain products and moreover needed to be discussed in its content between all smart card players and specially between Certification Bodies all over Europe. Eurosmart Security Working Group was the initiator of the Trailblazer 3 Certification group inside eEurope Smart Cards initiative developed in 2000 under the eEurope action lines.
The Group met and worked during more than 2 years on improving CC implementation together between, laboratories, certification bodies, banks, telecom operators and industry security experts. The achievements are enormous in terms of mutual understanding and mutual recognition in Europe. This approach respond to the Commission consideration on the reality of mutual recognition – it must

be continued. The main target is to support CC evaluation methods in a more effective way in order to re-use previous evaluation and in that way avoid a non necessary additional cost.

Re-usability



- **Reuse not possible for proprietary security evaluations**
- **CC has the advantage of re-usability**

Since 1996, Eurosmart is contributing to the overall effort to increase and improve security of smart cards and its methods of evaluation. In order to confirm the necessity to converge towards a common method, Eurosmart members are analysing and comparing the various existing schemes. A mapping of security requirements at all level of the production chain and all over Europe clearly shows the confusing situation of the market.

To extend the achievements to all actors, **International Security Certification Initiative (ISCI)** was launched to continue the work of eEurope Smart Cards (1999 – 2002) and the trailblazer 3 approach in its implementation documents for CC methods.
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. Activities of ISCI consist in:

- managing convergence of industry (supplying and issuing sides) and administration towards common references and best practices for security evaluation and certification of ICT systems
- promoting the Common Criteria (CC) Standard as the major reference for evaluation methods and tools and providing contributions for best practices in CC implementation
- supporting mutual recognition of security certificates at an international level
- networking accredited evaluation labs and harmonising protocols for their accreditation
- specifying re-usability of methods, tools and procedures defined in ISCI to any type of ICT product and extending security evaluation to a full system level
- providing the European institutions and member state governments with a framework for discussion on legal, technical and trade issues related to security certification, referring to the strategy defined by the European institutions in the eEurope 2005 initiative, and according to the existing European Council resolutions

A political and financial support will allow maintaining the participation to ISCI meetings to rapidly achieve the objectives: Harmonisation of test tools and certificates.

As previously stated, while CC evaluation methods are well suited to smart cards, and today almost all the manufacturers have at least one product certified using the CC methodology, they are less well applied to payment terminals. To date only one organization (APACS in the UK) has adopted the CC

as the evaluation regimen for their payment terminals, and only one payment terminal manufacturer has gone through the evaluation. The experiences of this vendor and the evaluation process should be considered as a test case and compared with the experience of the numerous other evaluation processes performed in the industry.

Security should NOT be a competitive issue. For all actors to work in a coherent and dynamic approach, the European Commission should not only act as a catalyst but as a regulator to clarify the approach.

ROLE OF THE EUROPEAN COMMISSION

Commission should act as a regulator to:

→ Adopt a regulation clearly referring to a unique method and avoid a compilation of certificates
→ Promote and negotiate at International level the same approach

Commission must be a catalyst for:

- Political support in Eurosmart approach and international discussions in particular with payment systems organisations (avoid a multiplication and/or accumulation of standards)
- Financial support for ISCI – Such a group will follow the development of new attacks, provide solutions for new products, confirm the pooling of know-how of the best experts, continue to work using the same "language" and same reference to security, promote the methods worldwide for the competitiveness of European products.

For that, Eurosmart needs support to consolidate the work infrastructure (logistics and secretariat) and confirm laboratories, universities and certification bodies involvement.

GLOSSARY

"Payment industry" – "payment system provider" – "Card companies" EU Commission document is making reference to all 3 terms to design banks or payment organisation allowed to issue payment instruments.

Payment cards (as defined by Eurosmart in its figures publication):

Financial Services Retail-Loyalty	Banking	cards issued by banks for various services (debit, credit, prepaid schemes…)
	Retailers / payment	cards issued by retailers under their own brand, bearing a domestic or international payment brand
	Private Label Card Operators	payment cards issued by a service provider on behalf of a retailer, under its own brand or on the retailer's brand.
	Retailers – Non-payments	cards issued by retailers for stand alone loyalty service
	Oil	loyalty cards issued by petrol distributors.

185 millions microprocessor cards were shipped worldwide in 2003 for financial and retail applications. A 25% growth is expected for 2004.

ISCI International Security Certification Initiative

The ISCI consortium is made of organisations providing three main categories of expertise:

- suppliers of products, systems, technologies and services which are requiring an evaluation of their inherent security level – Eurosmart members
- suppliers of expertise applying to the analysis of security threats and attacks and to the evaluation of security products, systems and services (laboratories and universities)
- organisations delivering official certificates and having in charge the implementation of the regulatory framework for security evaluation and certification: DCSSI/SGDN (F), CESG (UK) BSI (D)

ISCI community aims to become a recognised platform of knowledge and expertise enabling technical assistance and consultancy in security certification matters

---

EUROSMART is the Brussels based international association representing the Smart Card Industry for multi-sector applications. Through its activities, Eurosmart act as a catalyst and forum for the smart card stakeholders. In a global environment, Eurosmart encourages interoperability through international cooperation. It created a forum: ISCAN (International Smart Card Association Network). By a permanent relationship with the European Institutions, EUROSMART participates in various European funded projects.
Eurosmart achievements have been acknowledged by the smart card community as "the voice of the experts".

EUROSMART members are: ASK, Aspects, Atmel, Austria Card, Axalto, Emosyn, FNMT, Fujitsu, Gemplus, GIE Cartes Bancaires CB, Giesecke & Devrient, Hitachi, Infineon Technology, Ingenico, Inside Contactless, Integri, Ixla, KasYS, Laser, Mastercard UK, MCO, NEC, Oberthur Card Systems, ORGA, Philips Semiconductors, Rafsec, Sagem, Sagem Monetel, Samsung, Saqqarah Int, Setec OY, Sharp, STMicroelectronics, Thales-e-Transactions, Wave Systems, Xiring.