EUROSMART

The Voice of the Smart Security Industry

Position Paper
European Citizen Card: One Pillar of Interoperable eID Success

October 2008

Index

1. Purpose of the Position Paper

This Eurosmart document reflects Eurosmart members resolution, and in particular the position of members that are smart card manufacturers, to promote the use of the ECC standardization works made at CEN.

The Eurosmart members that are smart card developers and manufacturers state that they will provide implementation of ECC card software:

- Compliant with published functional specifications;
- With their commitment to be compliant and interoperable, through suites of tests.

Their commitment is the guarantee of multisourcing and durability of ECC, that then may be the reference for a pan European interoperability of e-government and e-services cards that will provide benefits on identified use cases.

The current news about French and German national e-ID programs is a real opportunity for the concretization of ECC that will take full consideration of needed interoperability with already rolled out national ID cards.

"ANTS[1] is in charge of the project of the French National e-Identity cards. It wants the card to be used for both Citizen Identification and access to e-services, in particular with the aim to contribute to the modernization of the administration services. Having studied the existing projects and the state of the art of the industry, ANTS is aiming to refer to ICAO EAC e-travel specification for the Citizen Identification and to the IAS ECC[2] specification published by Gixel[3]. The specification itself that complies with the CEN standard, the works on interoperability test suites, testing results with the test suite and with the middleware that is selected by French Government showed real interoperability between 3 different suppliers and have convinced ANTS to select IAS ECC for e-services. "

Gérard Bonningue
ANTS

Contacts :
Raphaël Bartolt, Préfet et Directeur de l'ANTS – raphael.bartolt@interieur.gouv.fr
Gérard Bonningue, Chef du Département Titres et Identité - gerard.bonningue@interieur.gouv.fr
Agence Nationale des Titres Sécurisés – French Secure Documents Agency
106-116 rue Victor Hugo - F-92 300 Levallois-Perret

2. Introduction: eID in Europe

National ID cards are issued by National government bodies or agencies for citizens of the respective country. Personal identity documents confirm the identity of individual citizens, thus proving their legitimate residency within their homeland.
An e-ID in this context is a National ID card with visible and invisible security features and a secured microprocessor. These cards have the so called ID-1 format which is well known from credit cards.

Traditionally an ID card serves as personal document for visual identification.

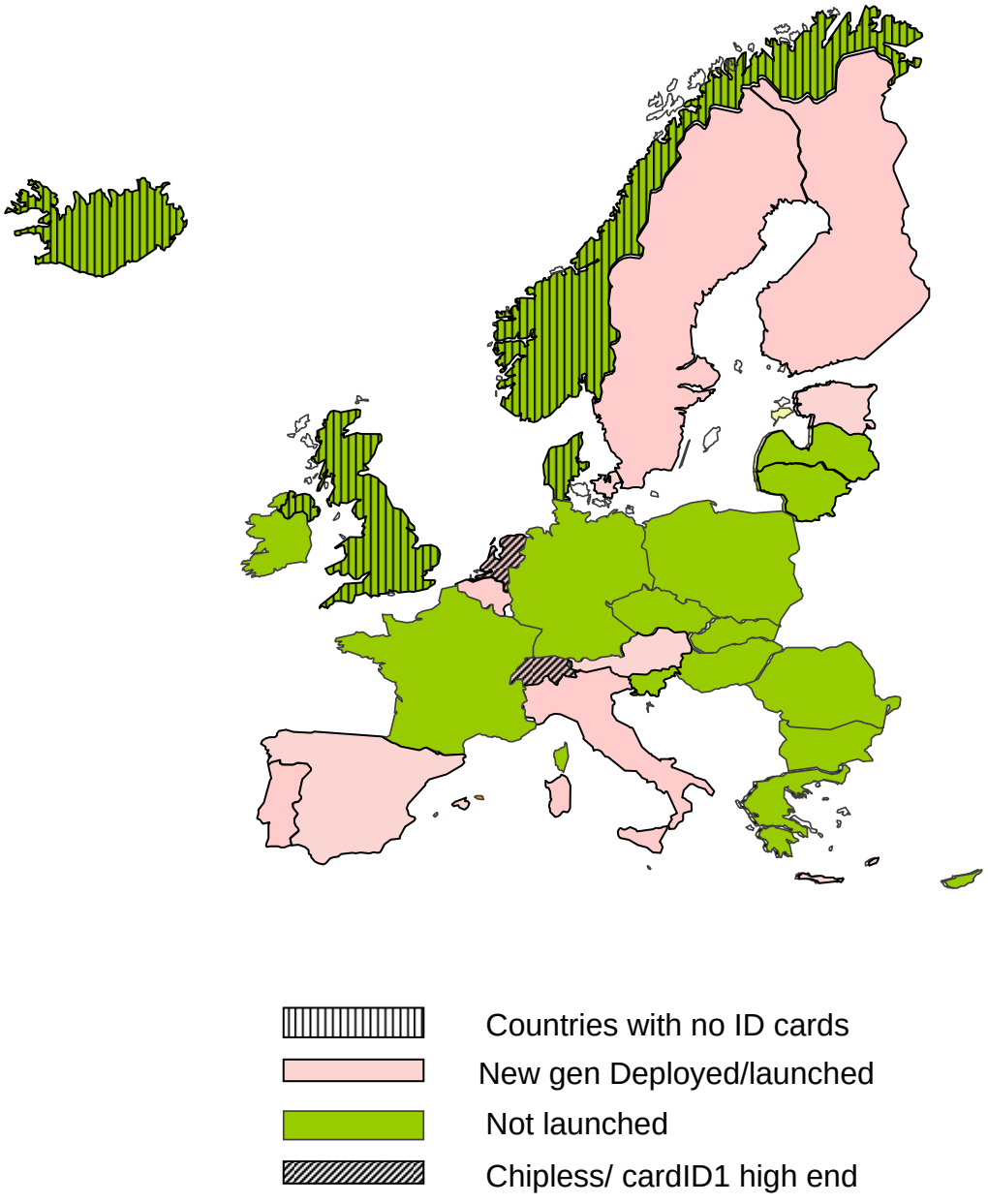
[1] ANTS stands for Agence Nationale des Titres Sécurisés. It is the French government agency in charge of the issuance of all ID secure documents.
[2] IAS ECC is the specification of e-services access application defined by Gixel in full compliance with the European Citizen Card CEN standard
[3] Gixel is a professional association of industries working in electronics. Its Smart Card Group is working on solutions for e-government. Members are Gemalto, Imprimerie Nationale, Oberthur Technologies, Sagem Orga and Thales.

By including a chip the security will be increased because smart card microprocessors are virtually impossible to be counterfeited. This chip could carry the biographic data of the citizen.
Additional storage of biometric features in the chip could create a liaison between the document and the card holder as successfully realized in e-Passports.

The e-ID is supposed to carry credentials in order to provide all or part of the following services:

- Act as an Inter-European Union travel document;
- Facilitate logical access to e-government or local administration services.

The trend is set in Europe: Electronic Passports have been deployed successfully; most European countries have a National ID card and several (Belgium, Estonia, Finland, France, Germany, Italy…) have adopted or are adopting an electronic National ID card.



3. What does smart card bring to national e-ID?

Advantages of the smart card technology are multiples, especially for eID:

- e-ID smart chip technology protects the individual's privacy while securely assuring their identity by using PIN codes or biometrics;
- e-ID's proven security increases confidence in a national credentialing system;
- Using e-IDs does not require on-line access to central databases as citizen verification and identity authentication is performed off-line;
- Virtually impossible to counterfeit, the e-ID provides a strong countermeasure against Identity theft;
- e-ID's digital signatures contribute to the accountability of government officials and employees;
- e-ID's enable citizen's authentication and accountability;
- An e-ID reduces government expenses by eliminating multi-claim benefit fraud.

4. Motivation for a European Citizen Card definition

European governments are motivated for moving from the existing situation to a new one in order to reinforce security after the 11th September 2001. This is true for border control, this is also true for simple control in the street done by the police. In the same time, e-Services are motivated by the societal move from a paper world to a paperless one, and by the necessity for governments to reduce their budget, i.e. reduce the cost for some applications as citizens services offers and Government to Government exchanges.

The requirements for a more secure ID document and for electronic services offered to the citizen were the two pillars which motivated the definition of the European Citizen Card definition at CEN.

With the European Citizen Card standard, the European Union can take the leadership into eID as it did in the past with the GSM standard for mobile communication.

Even if harmonization at European level needs to base on agreed legal, semantic and technical requirements, this Eurosmart position paper focuses on technical concerns only. The expected results are to:

- Improve security of ID documents security by adding security features and the usage of secure electronic components;
- Reduce costs for businesses and administration activities by simplifying procedures and optimizing resources;
- Improve the quality and accessibility of public services. That means make public sector more open and transparent, and facilitate transactions between administrations & citizens;
- Pick out services with clear added-values to citizens & governments; i.e. increase the quality and accessibility of public services and offer accessibility for all users and not only for some experts;
- Harmonize data and security architecture in the EU-area for a complete intra-European interoperability motivated by European citizens' mobility.

The main requirements for eID are travel functionalities and e-Services which are based on 3 key functions: Identification, Authentication, and Digital Signature. As travel functionalities are well covered by the ICAO standard for ePassport, this position paper focuses mainly on the requirement connected with e-Services aspects.

Identification, Authentication, and Digital Signature could be used in relation to a host of diverse technologies, applications and projects. There is an important need for interoperability between national systems in order to allow mobility and facility of use by European citizens everywhere in Europe. An interoperable solution across all European nations is crucial; however there are obstacles which include: relatively centralized and often proprietary architectures; fragmented responsibilities and difficult collaboration, nationally developed digital modernization programs and a wide range of ID and exchange security methods.

Therefore, e-Services interoperability must be based on a general framework agreed upon by all Members states and the protection of the fundamental freedom of citizens and their personal data. It covers the legal, organizational and semantic aspects, as well as trust, security and technical framework.

This leads Eurosmart to focus on 2 major concerns:

- Interoperability of e-services: Interoperability starts with the compliance to specifications, but is proven by the results to test suites that check both compatibility to the specifications and interoperability, as tested cards show how they respond to external solicitations. Such test suites exist for e-travel applications and others will exist for ECC. Eurosmart members will apply them on their cards.

- Security: Security shall be evaluated, comparable within Europe and certified. Common Criteria scheme is already in place and in wide use in smart card industry. The Common Criteria define the methodology of evaluation and European Member States have agreed on mutual recognition of certificates delivered by their certification bodies. Evaluation of a smart card refers to Protection Profile (PPs) documents that explicitly guide the process of evaluation taking into consideration the security needs for the use cases of the card. Eurosmart has contributed to the writing of several PPs. Security evaluation of e-travel application refers to ICAO and EAC PPs. Security evaluation of e-passports is already made according to them. For e-services, several PPs are already a good base, for Authentication and digital Signature features in contact mode of communication.

The European standard ECC allows connecting the smart token directly to the server where e-Services must be used; this reduces risk management (security, privacy) and avoids legacy difficulties. Identity cards have been in common use throughout numerous countries around the world for a while now. They have been established for several reasons: as proof of identity, to prove the age, to vote, etc. Building upon the technologies introduced for the implementation of ePassports, eID cards own microprocessor technology to store personal information, enable the electronic identification and/or authentication of the holder, and allow secure digital signatures. The cards become an efficient and secure platform and interface for the receipt of government services. This is the first relevant advantage from Eurosmart's point of view.

Nevertheless, 7 European Member States have already started their national eID project by using smart card not based on ECC standard, while 14 others have been analysing this

smart card technology for their coming national eID project. Interoperability has always been important for the smart card industry. For any smart card program to be effective, the card must work seamlessly with readers, and the readers with PCs or networks. This is perhaps even more important when the cards and readers are supplied by different vendors or are used in multiple environments or geographical area. The European Citizen Card standard (part 3; see below) gives technical answers regarding the requirement for interoperability. This is the second relevant advantage from Eurosmart's point of view. By using the ECC standard, that means we are able to promote national eID projects with a complete interoperability management between already deployed ones and coming ECC based eID programs.

5. European Citizen Card description

- ***What does ECC bring?***

ECC is an open application standard, defining logical data structure, security and privacy mechanisms of the data and interface and communication protocols. It is open, because it allows the governments to select options. For instance, both contacts and contacless smart card interfaces are defined, biometrics and/or PIN for a 2-factor authentication. The complete framework for an electronic signature is specified. There is no limitation on this standard in the project quantity scale and/or in the type or number of online services.

ECC is a key pillar for an interoperable and cross border e-services solution.

ECC is open for various services, like eGovernment, eBusiness, eVoting, eDemocracy, eBanking and others.

With the decision to take this application standard into a national government and/or industry program, the decision maker reduces development time, decreases technical risks as well as the needed budget for the period of definition, specification and tendering.

- ***ECC implementation***

The standards define the services and mechanisms to be adopted for the provision of features in products that need to comply with functional requirements, user capability to use the product, integration in the environment. The standards provide a certain level of interoperability. However the high level of definition introduces different interpretations and the options that can be part of a standard may introduce interoperability difficulties. The specifications contain an implementation view that determines choices left open by standards and thus lead to a high level of interoperability. In addition, the level of definition made in specifications allows producing test suites that will be used for interoperability evidence.

In France the Gixel association has published the IAS ECC specification that fully complies with the ECC standard while providing a high level of interoperability with an IAS former specification used for the new generation of healthcare card (Vitale 2).This ECC standard is a central element for an interoperable e-ID management system. It is a key enabler for the achievement of the i2010 objectives proposed by the European Commission and it is already used by some Members States as France and very soon as Germany which is looking for a compliance with ECC for its future National e-ID card.

- ***ECC parts 1,2,3,4***

The European standardization body CEN has published the technical specification 15480, (CEN TS 15480) the European Citizen Card (ECC) as an offer to be used for governmental purpose. The European Citizen Card is neither a physical card nor a specific card application or set of applications by itself, but a definition of logical data groups and services that can be provided by any governmental card issued for their own application context, e.g. ID cards or health cards.

The specification of the European Citizen Card envelopes four parts, so far: part 1 and 2 have been published in 2007, part 3 and 4 are currently under development in CEN TC 224 WG 15:

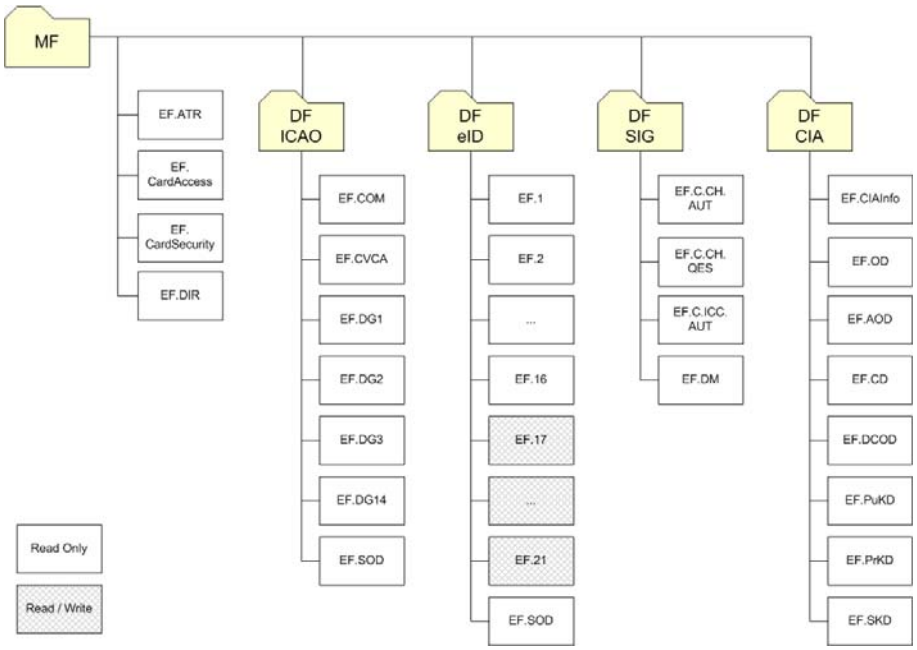
- Part 1: Physical, electrical properties and transport protocols (Physical Card Interface);
- Part 2: Logical data structures and card services (Logical Card Interface);
- Part 3 (preliminary): Interoperability using and application interface (Middleware);
- Part 4 (preliminary): Recommendations for issuance, operation and use (Card Profiles)

6. Current profiles and specifications

- ***Profile a) eID***

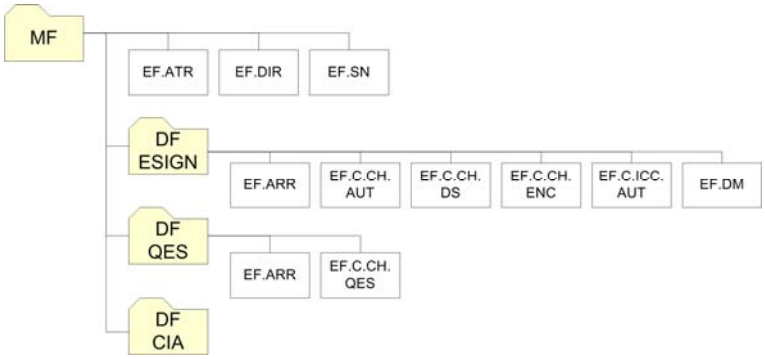
This ID scheme is presented by profile 1 of part 4 of ECC specification.
ECC Profile a) describes a card which is used as an identity document. One single mandatory contactless interface conforming to ISO/IEC 14443 is specified for all applications. The following three applications are envisioned:

- eID: This application implements electronic identity card services and data structure. The cardholder's data (corresponding to the data on conventional identity documents) are stored in distinct data groups.
- ICAO: Since ID cards are accepted as travel documents within Schengen States, this profile contains an MRTD application (Machine Readable Travel Document) in conformance to ICAO specifications, comparable to the e-passport. The mandatory card services are passive authentication, BAC, EAC chip & terminal authentication referenced by the specific OIDs, plus Secure Messaging for the ICAO application.
- SIG: The card includes a signature application in accordance with CEN prEN 14890 which contains the signature service itself on the card with the added possibility of installing the necessary certificates or keys at time of issuance or alternatively having them already installed during the personalization process.



- ***Profile b) eHealth card (ESIGN-K)***

Profile b) describes a card with an ESIGN application and the option for an additional functionality for digital signatures. It supports a contact-based interface according to ISO/IEC 7816-3 and the T=1 transport protocol. The protocols, services, and formats used in profile b) are largely based on the CEN prEN 14890 standards.

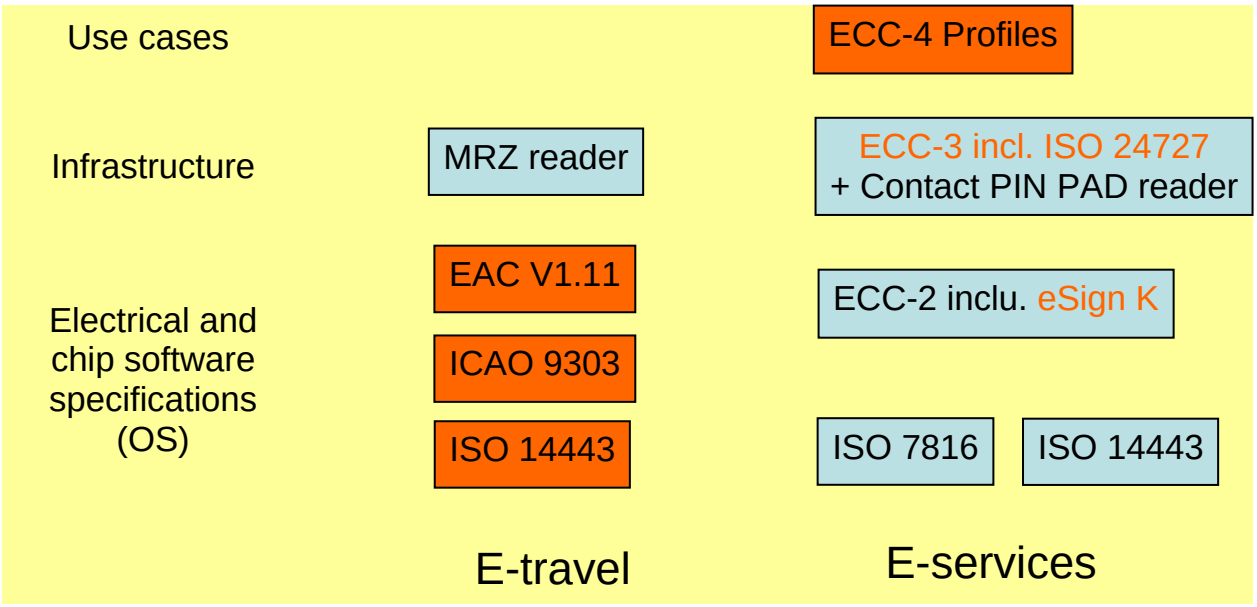


- ***Profile c) eHealth card (II)***

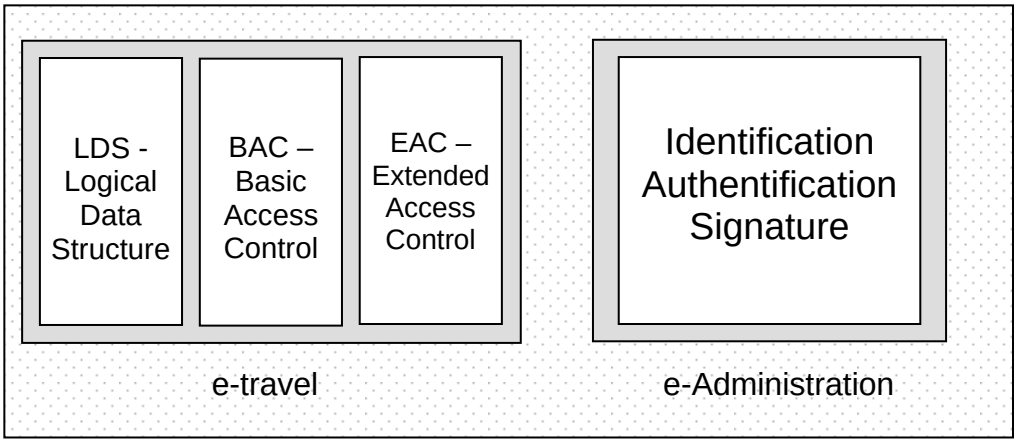
The objective of the profile is to list features for a contact-oriented smartcard supporting an eHealth application together with a legacy application. The card profile supports a RSA based digital signature functionality and symmetric device authentication using 2TDES (112 bit) with subsequent secure messaging. It can be used as an authentication token for RSA based client/server authentication. Two different card types are described for cards complying with the profile: a patient's card (health insurance card, HIC) and a health professional's card (HPC). The profile gives some simple use cases illustrating how to use the HIC/HPC cards: access of patients' insurance data by the health professional or the patient himself, creation of an electronic prescription.

- ***Profile d) eID (IAS)***

France has made the choice to be ECC compliant and selected IAS ECC as the specification for its National e-ID card. The specification is a concrete implementation of ECC and freezes some technical options proposed by the ECC. As an association of several standards (see table below), IAS ECC allows a complete interoperability between smart card manufacturers and also with previous IAS versions. The architecture is built as shown in the following figure and can be easily upgraded with new coming functionalities (ex. Biometry) or security features (ex. Elliptive Curves).



Standards used for IAS-ECC



IAS-ECC architecture

The travel functionality is contactless as for the ePassport when the e-Service is contact. This is motivated by the opportunity to reuse both existing infrastructures (ePassport & RSA PKI). Nevertheless, the e-Service side could be easily used into a contacless approach.

7. CONCLUSIONS

The pan-European emerging e-ID IT infrastructure is an opportunity for improving the life style of European citizens. But the European e-ID approach must be developed and deployed in harmony into Europe and interoperability requirements must be kept in mind.

European Members States have now the chance to benefit from the ECC solutions for the e-ID roll-out in their national solution program. There are already product offers proposed by different providers on the field that guaranty a fast deployment with cost effectiveness, and supply continuity.

It is the way to achieve the technical *rendez-vous* for the EU and to be ready for the i2010 objectives. And this proven interoperability shall be one pillar of the leading edge for e-ID for Europe.

APPENDIX

- ***ECC part 1***

Part 1 of the ECC specifications describes the physical and the electrical characteristics of the ECC. It defines the basic requirements for the format, the design, the security features, the electrical properties of the chip and the used transport protocols for the communication between the smart card and a terminal.
In doing so the specification does not introduce any new smart card definition nor limits the used chip technology of the ECC to a certain interface.
It refers to the standardized ISO specifications for smartcards such as ISO7810, ISO7816 and ISO14443. Furthermore it follows the ICAO recommendations for the MRTD in ID-1 format.
There are no restrictions related to the used interface of the smart card. In principle it is up to the issuer of the card to decide whether he wants his cards to support contact-based only, contactless only or dual interface technology. This non-constraining approach will lead to multiple, different implementations which could all be called ECC compliant.

An elaboration on the pros and cons choosing one of the abovementioned technologies - contact-based, contactless or dual interface - can be found in the EUROSMART White Paper “Durability of Smartcards for Government ID”

- ***ECC part 2***

Part 2 of the ECC specification defines the card services that are mandatory for an European Citizen Card as well as optional extensions. It specifies the logical data structure on the card, the logical card interface itself and the security architecture/mechanism. Furthermore it defines a common set of commands for the ECC as one key part to ensure interoperability with system infrastructures.

There is a differentiation between basic and extended electronic card services. The electronic services for identification, authentication and signature creation (IAS services) purposes are mainly based on public key procedures, essentially, on RSA operations, as used by the German electronic health card eGK and the French identity card INES. However, offering equivalent security elliptic curve cryptography is gaining ground.

In general the definitions of the services and the commands are not limited to a specific chip interface technology. However, depending on the different nature of these interfaces there is the need for special treatments of particular mechanisms – for instance an additional securing of the contactless interface compared to the contact based communication. In order to reach the interoperability objective, IAS services are also compliant to prEN 14890 part 1 and part 2.

Since a card used as ECC can have many different primary applications (e.g. as an ID card or a health card), various instantiations of an ECC are imaginable. This leads to the definition of so-called card application profiles in ECC part 4.

- ***ECC part 3 middleware***

ECC part 3 will provide an interoperability model, which will enable a PC client application compliant with technical requirements, to interoperate with different implementations of the European Citizen Card.
In addition to the ECC card description in part 1, 2 and 4, this part of the ECC specification describes a generic middleware that enables the ECC to be used securely in online transactions. The middleware architecture will be based on ISO/IEC 24727 with additional technical specifics. The API provides the client-application with the abovementioned IAS services that are supported by the ECC.
The specific implementation type of the ECC card will be transparent for the ECC middleware. The ECC middleware checks the supported card functionality by reading specific card content. It is up to the ECC middleware to detect the card capabilities. As long as the services on the card are available the middleware can interoperate with the card - regardless of the nature of the card – whether it is contactless or contact-based only or whether it is a native or Open Platform implementation. Interoperability is achieved by the standardized API.

As already mentioned part 3 is not yet voted, however it is expected to be finalized by end of 2008

- ***ECC part 4***

Specific application profiles are contained in part 4, on one hand to present use cases which can act as a reference and on the other hand to exemplify use cases which are based on actual implementations. Two application profiles have been developed in the past drafts, with the expectation, that others will be added by the time, the specification is adopted.

Each of these profiles contain one or more applications which use interfaces and transport protocols described in part 1 of the specification and services described in part 2. Each profile thereby is linked to a distinct object identifier (OID) to be used as interoperable reference, e.g. to ease the discovery of the card's and/or application's capabilities. In any other case the middleware according ECC part 3 has to detect the services on the card. For this purpose one so called global profile is integrated in Part 4, to retrieve the card capabilities as well as application capabilities. This profile can be used complementary to the application profiles, in case the card/application contains additional information, which is not covered by the specific profile in use.

Profile 1 – ID Card

ECC Profile 1 describes a card which is used as an identity document.
For details see chapter 5.

Profile 2 – ESIGN-K

Profile 2 describes a card with an ESIGN application and the option for an additional functionality for digital signatures. For details see chapter 5.

Other Profiles

More profiles can be included and existing profiles are subject to further development and improvement before the specification is finally adopted. Even after it has been released, new profiles can still be added to the specification through the CEN TC224 WG 15 working group.

Therefore the standard provides a profile template to design new profiles in a comparable manner. The template contains guidelines in order to support anyone developing a profile; it clearly states which information has to be included in a profile.

In general, any country will always have the option to define and bring in its own profiles to have its country specific use cases.

Eurosmart is an international non-profit association located in Brussels and representing 25 companies of the smart security industry for multi-sectors applications. Founded in 1995, the association is committed to expanding the world's smart secure devices market, developing smart security standards and continuously improving quality and security applications.

Manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers gather and work into dedicated working groups on communication and marketing, security, electronic identity and new form factors, and prospect emerging markets. Members are largely involved in political and technical initiatives as well as research and development projects at the European and international levels

Eurosmart is acknowledged as representing "The Voice of the Smart Security Industry".

More information: www.eurosmart.com

EUROSMART
Rue du Luxembourg 19-21 – B-1000 Bruxelles
Tel. (+32) 2 506 88 38/ Fax. (+32) 2 506 88 25
Email : eurosmart@eurosmart.com