eID Interoperability for PEGS

NATIONAL PROFILE ITALY

November 2007

This report / paper was prepared for the IDABC programme by:

Author's name: Jos Dumortier - Hans Graux, time.lex

Company's name: Siemens - time.lex

Company's address (optional):

Company's logo (optional)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°3

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/6484/5938

Executive summary

The project eID Interoperability for PEGS aims to propose a solution to the legal, technical and organisational issues related to the creation of an interoperable Pan-European identity management infrastructure. The EU Member States, Candidate Countries and EEA Countries are introducing more sophisticated ways to manage identities in the eGovernment area. Different member states are implementing different structures as their identity management solution. The main challenge for the eID Interoperability for PEGS project is to propose a general architecture that, while taking into account the existence of different models, is able to cope with them by obtaining the final goal of interoperability.

The project should conclude with several different proposals how to build interoperability without affecting member states' own existing infrastructures.

This document describes the current situation regarding the use of electronic authentication means in Italian eGovernment applications.

Table of Contents

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY

1.2 Reference Documents

[RD1]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD2]	European Electronic Signatures Study http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD4]	Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45 http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf
[RD5]	DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf
[RD6]	IDABC Work Programme Third Revision http://ec.europa.eu/idabc/servlets/Doc?id=25302
[RD7]	DIRECTIVE 2004/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

2 Glossary

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *Entity:* anyone or anything that is characterised through the measurement of its attributes in an eIDM system. This includes natural persons, legal persons and associations without legal personality; it includes both nationals and non-nationals of any given country.

- *eIDM system*: the organisational and technical infrastructure used for the definition, designation and administration of identity attributes of entities. This Profile will only elaborate on eIDM systems that are considered a key part of the national eIDM strategy. Decentralised solutions (state/region/province/commune…) can be included in the scope of this Profile if they are considered a key part of the national eIDM strategy.

- *eIDM token (or 'token')*: any hardware or software or combination thereof that contains credentials, i.e. information attesting to the integrity of identity attributes. Examples include smart cards/USB sticks/cell phones containing PKI certificates, …

- *Authentication*[1]: the corroboration of the claimed identity of an entity and a set of its observed attributes. (i.e. the notion is used as a synonym of "entity authentication").

- *Authorisation*: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

- *Unique identifiers*: an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context. Examples may include national numbers, certificate numbers, etc.

- *Official registers*: data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal of factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.

[1] For the purposes of this Profile, the notion of authentication is considered to be synonymous with 'entity authentication', as opposed to 'data authentication'. The notion of 'identification should be avoided to avoid confusion.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

- *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

- *Advanced electronic signature*: an electronic signature which meets the following requirements:

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

  (c) it is created using means that the signatory can maintain under his sole control; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

  Again, this definition may cover non-PKI solutions.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[2].

- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

[2] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

2.2 Acronyms

A2A ..... Administration to Administration

A2B ..... Administration to Businesses

A2C ..... Administration to Citizens

CA ..... Certification Authority

CRL ..... Certificate Revocation Lists

CSP ..... Certificate Service Provider

eID ..... Electronic Identity

eIDM ..... Electronic Identity Management

IAM ..... Identity and Authentication Management

IDM ..... Identity Management

OCSP ..... Online Certificate Status Protocol

OTP ..... One-Time Password

PKCS ..... Public-Key Cryptography Standards

PKI ..... Public Key Infrastructure

SA ..... Supervision Authority

SOAP ..... Simple Object Access Protocol

SCVP ..... Server-based Certificate Validation Protocol

SSCD ..... Secure Signature Creation Device

USB ..... Universal Serial Bus

TTP ..... Trusted Third Party

XAdES ..... XML Advanced Electronic Signature

XML ..... eXtensible Markup Language

XML-DSIG ..... XML Digital Signature

3 Introduction

3.1 General status and most significant eIDM systems

At present, there are several eIDM systems in place in Italy, although only some of them are widespread to a significant part of the population.

Italy was one of the first countries to adopt an electronic identity card (i.e. a formal identification document, whose card body is secured by holograms, microprints, etc.). A Ministry of Interior Decree dated July 19th, 2000 officially introduced the Electronic ID Card, or "CIE". The first electronic ID cards were released to citizens about 1 year later.

Despite this early start, due to a set of reasons (technical, political, organisational, etc.) the Electronic ID Card has - still today – a very limited spread to citizens (less then 2 millions).

In subsequent years the CNIPA (National Centre for IT in the Public Sector) decided to develop a national specification for the smart cards issued to citizens by Public Administrations and aimed to improve the access to e-government services. The national specification was developed by a dedicated workgroup which however was left open to contribution and participation of those private companies which were active in the smart card field and interested in the oncoming business. The national specification, named "CNS" (National Service Card), mainly comprises the following:

- a definition of the subset of OS commands (APDUs) to be supported by any CNS compliant smart card, regardless of its producer/vendor;
- a definition of a subset of the internal data structure of the microchip, to be present on every CNS compliant smart card;
- a prescription for the issuer of the digital certificate(s) installed on the card, which has to be included in the national list of the certification authorities accredited for issuing qualified certificates held by the CNIPA;
- a set of rules to be followed by the Public Authorities wishing to issue CNS compliant cards;

It is important to note that the CNS standard does not aim to provide a specification for "official" identification documents (i.e. State documents, such as the previously mentioned Electronic ID Card, etc.). For this reason it does not include any specification for the security of the card body. Vice versa, an ID document can comply with certain parts of the CNS standard, and this is what happens in practice, especially to guarantee the interoperability between all Government cards issued in Italy.

It can be said that the main advantage of the CNS standard was just in insuring a high level of interoperability between different cards and projects.

There were several interesting projects which are referred as "CNS" projects. The main ones were the SISS[3] project (Health card of Regione Lombardia, with its 9M+ cards issued) and the CNS of Regione Friuli. Other projects, like the one of Regione Veneto, are still in their pilot phase.

Besides the National ID Card, intended for all citizens, and the CNS compliant service cards, aimed to satisfy specific needs (for example in the field of e-health), another document started to migrate from its traditional paper format to a smart card by the year 2003. This document is the Identification Card of the Public Employee, or "AT model". In fact, in Italy each civil servant or public employee has a sort of "company badge", which by definition is also considered a valid ID document, the "company" being the State itself. The new document is then considered an "AT-E model", standing "E" for electronic.

The first Administration which started to substitute the traditional badge with the new document was the Defence, which started to issue the so called "Carta Multiservizi della Difesa" or "CMD" since 2003. Later on, when other Administrations (Justice) issued a tender for the adoption of the same card, the name was changed in "Carta Multiservizi del Dipendente" i.e. Multiservice (Public) Employee Card, which left the acronym unchanged.

As previously mentioned, the CMD is then a valid ID document (like the National ID Card). It includes several security features of the card body. With respect to the National ID Card the CMD has an interoperable, CNS-like subset of information but also a set of services which are instead specific for its on-field use. Two interesting examples of these specific services are the military health data structure and the certificate for mail signature and encryption.

The last electronic document to be issued has been the Electronic Residence Permit, or PSE ("Permesso di Soggiorno Elettronico). This is simply a variant of the electronic ID card, dedicated however not to Italian citizens but to non EU individuals resident in Italy.

Obviously, on top of these projects, also Italy complied with the VISA Waiver program by setting up and issuing electronic passports since October 26th, 2006.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

Italy is organized in 20 Regions with autonomy on many fields (e.g. health). Each Region is composed of one or more provinces, and within each province municipalities also have a strong role in proposing e-government services to citizens. Many initiatives in the e-government field are then conceived and carried out at a local level, even if a central coordination, on behalf of the national government, is considered of strong importance. For this reason, in the past years a specific Ministry (Innovation in PA) has been set up.

[3] The SISS project is a pilot of the Netc@rds initiative for interoperability of health cards in Europe.

Then, at the central level, the Ministry of Innovation in Public Administration has in particular the role of legislative coordination while the CNIPA (National Centre for IT in Public Administration) is active in designing and publishing technical regulations and guidelines.

3.2.2 National eGovernment cooperation and coordination

The Minister of Innovation in Public Administration Nicolais and the Undersecretary Magnolfi have introduced the strategic lines for the realization of the national e-government system, based on seven macro-objectives which will be further organized in one single Directive. The emphasis is on simplification, to be obtained through the combined use of all possible levers: norms, technologies, organisation, human resources.

The seven macro-objectives are briefly described below:

Objective N. 1 – To improve the efficiency of the Public Administration

This goal can be reached by:

- Innovating the PA processes in a context of strong coordination between central and local Administrations, to simplify and reduce times and cost of administrative procedures;
- Actuating the Code of the Digital PA ("Codice della PA digitale") to reorganizing and automating the processes;
- Providing on-line training for the PA personnel

Objective N. 2 – To realise interoperability and full cooperation between Public Administrations

This goal can be reached by:

- Defining a cooperation model for the PA, which clearly defines services and relative service level agreements
- Finalising the implementation of the necessary instruments, like document management systems, authentication systems, digital signature, digital archiving, etc.;
- Integrating the national registers and data bases, by defining common access rules and homogeneous description of data.

Objective N. 3 – To improve the transparency of the Public Expenses

This goal can be reached by:

- Further improving the use of information systems in finance applications. For example, payments from and to the PA.
- Promoting electronic procurement processes through the Net.

Objective N. 4 – To build up "digital citizenship"

This goal can be reached by:

- Improving e-democracy, in its various forms

- Lowering the digital divide
- Implementing a national identification system to secure the access and exploitation of electronic PA services by citizens.
- Implementing procedures which allow on-line payments in full security
- Guaranteeing accessibility and quality of PA portals, even through their integration/rationalization

Objective N. 5 – A "systemic" approach to quality and efficiency in the Public Administration

This goal can be reached by:

- Verifying any action with respect to quality/quantity evaluation parameters, as a multilevel approach, with reference to the phases "Planning – Implementation – Monitoring – Improvement".
- Promoting a network of excellence with the contribution of research centres, universities, with the goal of identifying the best practices and introducing them as general practice for the entire PA system.

Objective N. 6 – To ease/improve the competitiveness of private companies and the growth of the ICT industry

This goal can be reached by:

- Making the PA a driver for the market, by committing innovation and advanced services.
- Setting up a permanent dialogue with private companies to receive suggestions and learn the most innovative experiences from the market.
- Promote software development and the use of Open Source in Public Administration

Objective N. 7 – Let Italy become a key player of the process of innovation of the PA in Europe

This goal can be reached by:

- Strengthening the integration of the national e-government system with those of other countries, to play a more active role on the theme of Information Society.
- Actuating the EU strategies defined in Lisbon

3.2.3 Traditional identity resources

The identity card was introduced by a Royal Decree (N. 773) dated Jun 6th, 1931. A following Decree (N. 635), dated May 6th, 1949, stated in its article 288 that the identity card has to be considered a "police" identification document, i.e. a document that citizen must show to policemen when requested to prove their identity.

The main information printed on the document (which is also present on the card body of the new electronic version) is the following:

- Municipality which issues the document
- Last (family) name
- First name

- Municipality of birth
- Date of birth
- Gender
- Number of birth certificate
- Height (cm)
- Number of the document
- Photo of the holder
- Official residence
- Address
- Date of issuing
- Date of expiration
- Citizenship
- Fiscal code
- Hand signature
- Indication about the validity of the document abroad

Each municipality keeps a register of its residents and issues the identity card to citizens. The identity of a citizen is verified on the register of the municipality where the citizen is resident whenever he/her requests the issuance of a new identity card.

The issuance of the identity card on behalf of the municipalities has been kept in force also for the new electronic ID card.

Until the introduction of the new electronic ID card, there was no central storage of personal data of citizens. With the introduction of the electronic ID card, a central database was set up, but in it each record is encrypted with the public key of the issuing municipality, in order to preserve the privacy of citizens. In practice, this means that no real change in the way citizen data are used took place.

Besides the identity card, public employees have a specific identification document, the so called “Modello AT”, which they can use for identification instead of the identity card, even when they go abroad.

Each citizen is also identified by a “Fiscal Code”, which is uniquely attributed by the Ministry of Finance not only to citizens but also to non individuals (i.e. legal persons). The Ministry of Finance is also responsible for keeping and managing the register of the fiscal codes.

On the health side, Regions deliver to citizens the so called “Tessera Sanitaria”, (health card) which in some cases (for example Regione Lombardia) is a smart card (that complies with the CNS standard); but in general it is simply a plastic card with a magnetic stripe. The purpose of the TS is to collect essential information for the access of citizens to the health system.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

Main systems

As already mentioned in the introduction, there are at least 3 eIDM systems worth of mentioning, the CIE (e-ID Card), the CNS (National Service Card), and the Public Employee Card or AT-E Model. The Electronic Residence Permit can instead be considered more or less as a variant of the Electronic ID Card (CIE). Each of these systems has a specific target and goal; however, many of the functionalities are common.

The target population for those eIDM tokens is then as follows:

eIDM system	Acronyms used	Target
Carta d'Identità Elettronica (Electronic ID Card)	CIE	All citizens
Carta Nazionale dei Servizi (National Service Card)	CNS	Specific e-government projects, mostly on regional basis
Carta Multiservizi del Dipendente (Multiservice Employee Card)	CMD, or AT-E model	Public employees
Permesso di Soggiorno Elettronico (Electronic Residence Permit)	PSE	Non EU Residents in Italy

The next figure offers a synthetic description of the main features of the various eIDM tokens especially with respect to the two dimensions of security and services.

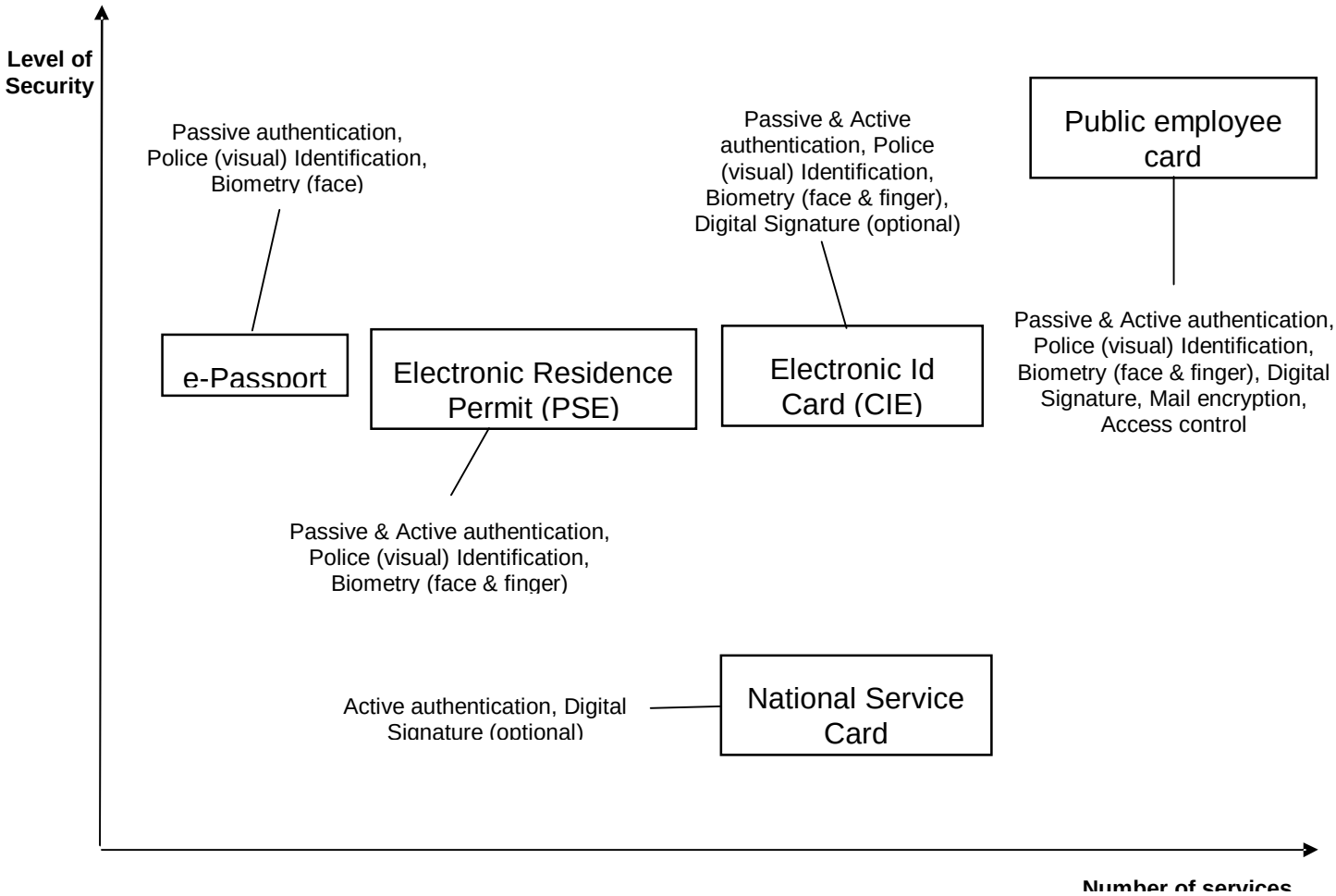

Fig. 1 - Security vs Services for various eIDM tokens issued in Italy

One question may arise by comparing the CIE and the CNS and considering that, while both tokens are conceived to be delivered to generic citizens (if with different modalities), the CNS supports only a subset of the functionalities supported by the CIE. Then why the CNS? The answer can be found in the difficulties that prevented the CIE, until now, from being delivered to the full population. These difficulties convinced the Minister of Innovation and Technologies of the previous Government, Mr. Lucio Stanca, to decide for a simpler card (while awaiting the massive delivery of the National ID Card), which could be distributed more easily to citizens thus improving the exploitation and development of e-government services. It is then planned that the CNS should be substituted by the CIE as soon as it will be available to citizens.

It must be said, however, that reasonably the CNS can be expected to survive. In fact it is clear enough that some projects have needs that are simply not possible to address with only the ID Card. Just as an example, some Regions (Lombardia, Sicily, etc.) issued or plan to issue health cards, whose card body layout has necessarily to differentiate from that of the National ID Card.

From the point of view of the organisation of the data residing on the chip, more or less all the Italian eIDM tokens follow the same organisation. An attempt to describe this organisation is provided in the following Figure 2.

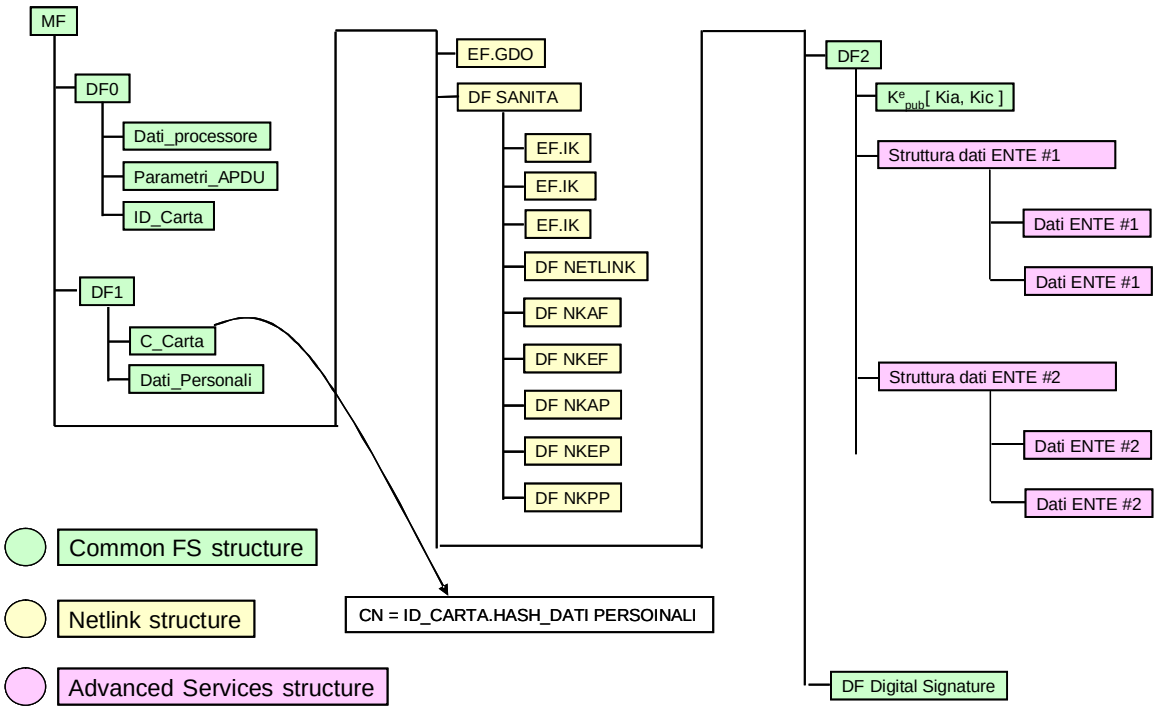

Figure 2 - High level dataset for the CIE, CNS, CMD and PSE eID tokens

The green boxes show the parts which are common to all cards (even if unused; this is e.g. the case for the digital signature, which is often optional).

The red boxes show particular applications (sub data structures) that differ for each card (but all have to be allocated under the common DF2 dedicated file).

The yellow boxes show the health data structure, which complies with the Netlink interoperability standard and can be present or not depending on the card and the project.

Then, mainly, the data are organized into three groups:

DF0 data: configuration data, pre-personalisation information, card number;

DF1 data: personalisation data (cardholder information), including the digital certificate for authentication;

DF2 data: left free for custom applications, that can be loaded also after the card issuing.

One interesting feature of the Italian eID tokens is the format of the authentication digital certificate, whose common name (as it can be seen in the figure) does not directly contain (at least in the CIE and CNS cases) the name of the holder. Instead it contains the SHA-1 hash of the file “Dati Personali” (personal data), thus preventing anybody from accessing the personal information of the holders (for example, from the directory of certificates) without their explicit permission. In case of necessity, the file Dati Personali can be read too, its hash computed, and the result compared with that contained in the common name of the certificate.

Similarly, because the file "Dati Personali" contains also the hash of the biometric features (photo, fingerprint templates), the verification of the certificate serves also as a Passive Authentication, more or less like what happens with the EF.SOD data file in the e-passport case.

As previously said, the register of citizen data is kept on behalf of the Municipalities, while the central database contains only encrypted information. However, at least in the case of the CIE, it collects also the log of the issuing of each card and the keys needed by the municipalities to "open" the card for writing during its personalization.

Any of the eID tokens described above supports the service of network authentication, through the digital certificate assigned to each holder.

The process is strictly compliant with the SSL v3 standard, i.e. a challenge-response procedure is invoked between the server and the client and the holder is required to enter his/her (authentication) PIN number to unblock the private key operation run inside the chip. The private key operation is needed to correctly answer the challenge coming from the server. When the card also has a digital signature certificate on board, this can have a different PIN number to avoid misuse.

The information sent to the server during the authentication phase is that contained in the common name of the certificate that, as said before, hides the personal data of the holder. In this case we have a difference between the cards.

Privacy has been considered an absolute must for the CIE; in this case, besides the hash of the personal data of the holder, the common name only contains the serial number of the card. Whenever personal data are strictly required, the server has then to send to the client an applet for reading also the personal data file[4], compute its hash and compare it to the one contained into the common name. The CNS lowers this requirement a bit, by also including the Fiscal Code of the citizen in the common name, which allows a much bigger range of services to be delivered without the need for also reading the personal data file. It is not clear at the moment if the CIE will adopt the same measure in the future or not.

A difference with respect to the above mentioned cards is offered by the CMD, which is– at the end – an employee card, and then necessarily has to include into the certificate some elements that ease, for example, the use of the card for mail encryption and signature. However, in this case also the need of a strong privacy is lower than in the other cases.

Finally, it should be noted that, while the eID tokens actually present in Italy are powerful enough to allow an advanced use and exploitation of e-government services, these are still greatly under-used

[4] The personal data file could be in principle protected from unauthorized reading by a PIN, so that it cannot be read without a clear consensus of the holder. However, in the actual version of the id card, the consensus is considered granted when the card is inserted into the reader. The personal data have in fact to be readable in case of a Police control, without the need of an explicit ok by the citizen to do so. A possible scheme, for solving this problem, could be to condition the reading of the personal data to two logical tests, one using a key dedicated only under Police control.

and under-developed. One of the main reasons, as can be easily imagined, is the need of a smart card reader. For this reason, the Lombardy region has recently issued a tender for the acquisition of several millions of readers, to be distributed for free to all citizens/families.

Other initiatives remained, until now, more or less only good pilots. One of the most interesting was conducted with the CIE, using it as the key of an automatic voter's identification procedure, within the framework of a test of an electronic voting system. The project was an EU research funded project, named e-Poll. The most significant test of the e-voting platform which relied upon the use of the CIE was conducted in the town of Specchia.

3.3.2 Legal framework

As already mentioned, the identity card was introduced by a Royal Decree (N. 773) dated Jun 6th, 1931. The relevant laws/decrees that introduced the electronic ID card were:

The law N. 191 of Jun 16th, 1998 where, at Article 2, is written:

- *"La carta di identità e i documenti di riconoscimento devono contenere i dati personali e il codice fiscale e possono contenere anche l'indicazione del gruppo sanguigno, nonché delle opzioni di carattere sanitario previste dalla legge".*[5]
- *"Il documento, ovvero il supporto magnetico o informatico, può contenere anche altri dati, al fine di razionalizzare e semplificare l'azione amministrativa e la erogazione dei servizi al cittadino".*[6]

As can be clearly understood, at the moment when this wording was introduced, the discussion on adopting a new support which could offer not only the traditional police identification functionality, but also innovative services to citizens (thanks to the use of the upcoming new technologies) was already started.

The official introduction of the electronic ID card – however – took place only in the year 2000, with a Ministry Decree dated July 2000.

The Decree, at its Article 1, states that:

> "*per carta-servizi [si intende] l'insieme dei dati [identificativi]… - ad esclusione della fotografia e della firma - e delle informazioni amministrative di cui all'art. 1, comma 1, lettera e) e dell'art. 3, comma 4, del D.P.C.M" [22.10.1999, n. 437*]".[7]

---

[5] *"The id card and any other identification document must contain the personal data of the holder and may contain the blood type and other options related to health care according to law".*

[6] *"The document, or its magnetic or other kind of data storage, may contain also other data, in order to rationalise and simplify the administrative action and the provision of services to citizens".*

[7] "*As "service card" it is meant the set of identification data (excluding photo and hand signature) and of the administrative information cited at …[other Decree reference]"*

This wording introduced the distinction between the two main uses of the electronic identification card, i.e. the Police identification (which, as it was already in use, still required the picture of the holder and his/her hand signature on the card body) and the electronic (network, or "active") authentication with the goal of obtaining the fruition of advanced on-line services of the type G2C.

3.3.3 Technical aspects

Before entering the discussion of the architectural and organisational models of the various eIDM tokens mentioned above, it is important to better understand the three types of authentication supported by these tokens, which include:

- Visual identification
- Passive authentication
- Active authentication

The visual identification is a process that requires the traditional security means of previous documents, for example holograms, microprints, etc.

The passive authentication requires that the link between the personal data and the biometric data of the holder is a digital signature of some Authority whose certificate is known. The signed data file is registered on the memory support (chip, mag stripe, optical stripe, 2D bar code, etc.) and can be verified by an external application.

Finally, the active authentication requires computing process for a private key operation that has to occur within the token itself in response to a challenge sent by a server. In this case, only chip cards can be used. The active authentication, however, is the only which guarantees a strong authentication over the network (i.e. when parties are not one in front of the other).

Besides, another distinction is sometime used between the possible uses of a private key to prove the request/fruition of a service:

- Authentication
- Attestation
- Signature

In all cases, a private key operation is performed. However, when we speak about authentication, we intend that a random challenge sent by the server to the client is signed, and no evidence of this operation remains to the server. In other terms, the service provider can securely identify the requester of a service and grant access to him to provide an on-line service, but after the transaction is complete, no proof of this remains to the server (the signed challenge is lost).

We call attestation a process that polls the client for a true signature (i.e. not a random challenge, but the hash of a request form is signed by the client and remains to the server as a proof that the client required a specific service. The difference that is intended – in Italy – between attestation and signature resides on the type of key used: for attestation, the same key used for authentication is considered valid. For signature, instead, only qualified certificates issued by certification authorities included in the official list of CNIPA are considered valid by law.

The ID Card can be used also for attestation. I.e. its authentication certificate can also be used to sign an online form as a request of service.

Visual identification is instead not supported by the CNS that, as already mentioned, is only intended (as its name states) as a service card.

However, each of these cards has (at least) one digital certificate on board (for authentication and/or attestation). Both the CNS and the CIE have – as an option left free to citizens[8] – the possibility to install a second certificate (issued by one of the certification authorities in the trust list of CNIPA) for law enforced digital signature. The CMD can have one to three certificates depending on the issuing administration (for example the Defence department set up its own signature PKI, present in the CNIPA list, to issue also digital signature certificates). The third certificate is the one for encryption.

The key generation procedure varies depending on the issuing scheme. In the case of the national ID card, which is personalised (in a decentralized way) by the municipalities, the key generation occurs on-board of the card and the PKCS#10 certificate request is then sent to the trust centre for processing. In the case of the CNS, which is personalized centrally, the key pair is instead generated outside the card (but inside the trust centre) and then inserted into the card. In the case of the CMD (at least for the Defence case), the card is personalised centrally (i.e. in a Trust Centre), but the key is generated internally. In all cases, however, when a digital signature key (also)has to be generated, this has to occur within the secure confines of the chip-card.

The PKI infrastructures vary depending on the project. The following schemes try to describe the situation (to the best knowledge of the author).

[8] Also if this feature is supported by the card, this possibility – for what is known to the author – has however not been used up to now.

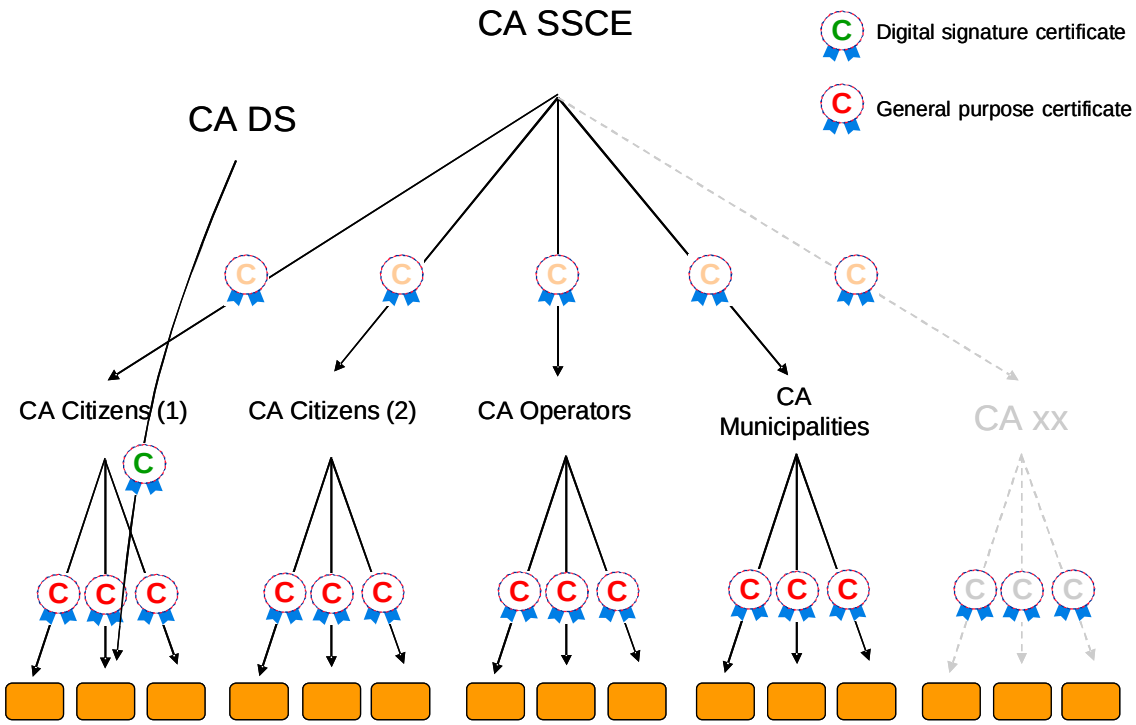

Fig. 4 – ID Card PKI architecture

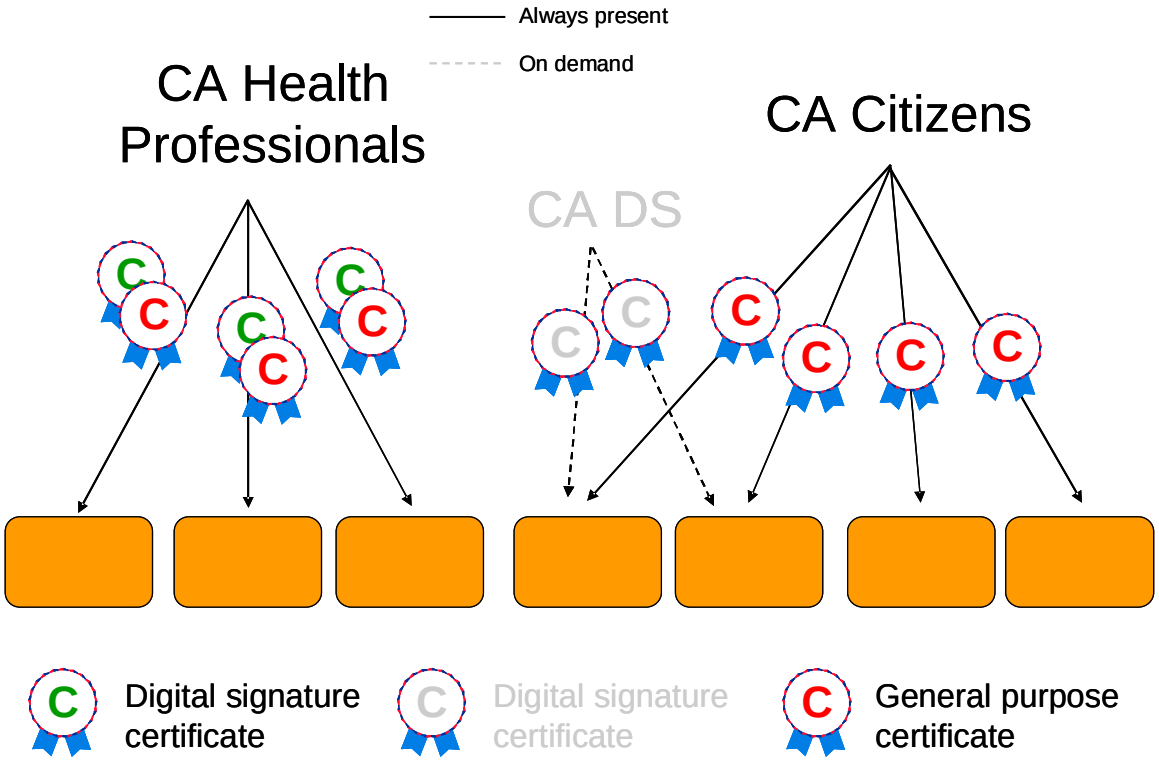

Fig. 5 – CNS (CRS-SISS project) PKI Infrastructure

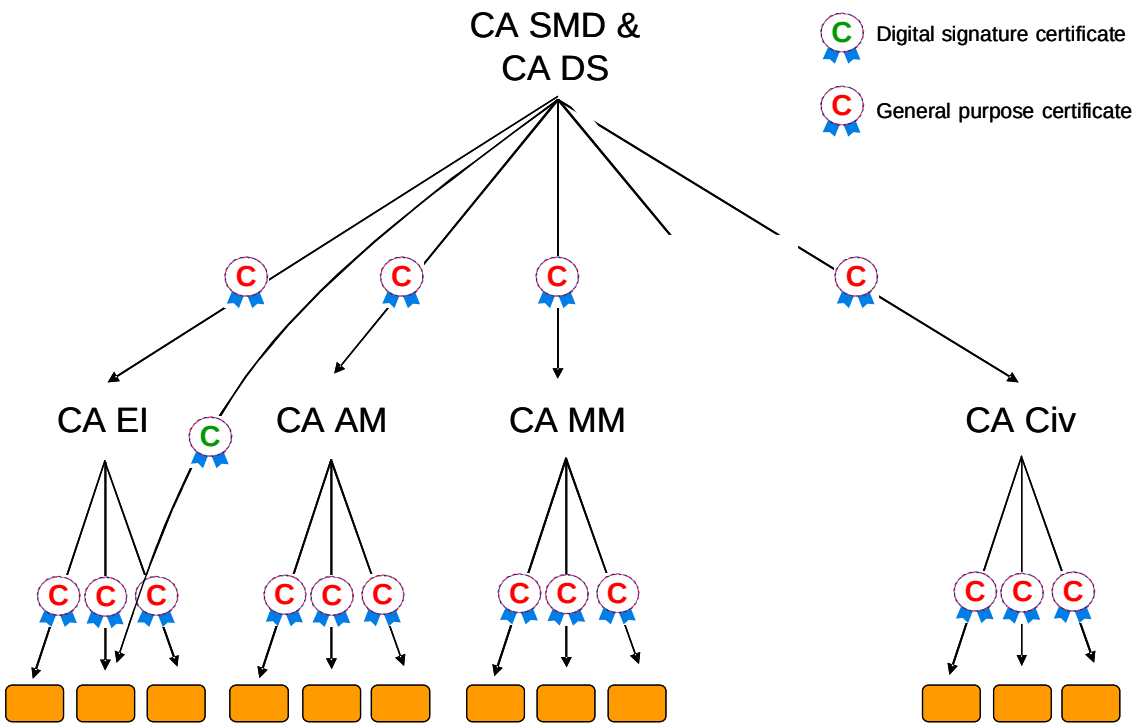

Fig. 6 – CMD PKI (Defence card case)

The PKI is managed by different entities depending on the project.

For the ID card, the CA is owned directly by the Ministry of Interior. For the Defence's CMD, by the Defence (both for authentication and digital signature); for the Justice's CMD, by Postecom (one of the Italian certification authorities in the CNIPA list). For the CNS of the SISS project, there are multiple CAs, owned both by the issuer (Region Lombardy) and by IT Telecom (another Certification Authority in the CNIPA list).

Middleware

For all these cards, the standard PKCS#11 and CSP middleware is available and often published on the issuer web site.

For the CIE, a specific CIE-API middleware was also made available, to simplify the use of the card by software developers.

Chip suppliers

There are several card manufacturers able to supply cards. The requirement for all of them is to comply with the subset of the operating system commands published on the CNIPA web site, to favour interoperability. The Administration can then issue tenders without having to change the behaviour of the card and its commands with respect to other national projects. A tender for a CNS provision was issued by CNIPA in summer 2005.

At present, the main suppliers are:

- Siemens
- Incard
- Oberthur

While Siemens and Incard offer native operating systems, Oberthur offer a Java card. In all cases, the OS comply with the CNS specification and are thus interoperable.

3.3.4 Organisational aspects

Depending on the owner of the system, the organisation is different.

The owner of the ID card is the Ministry of Interior, which has the overall responsibility of the project and manages the Trust Centre (including the PKI). However, the role of the national print-house (IPZS, Istituto Poligrafico e Zecca dello Stato) is very important, because it is in charge of the physical manufacturing of the cards and of their pre-personalization.

The responsibility of the issuing is up to the municipalities, which receive and process the citizen requests and physically consign the card. The process is carried out on-line and takes, in normal conditions, about 10 minutes from the enrolment to the delivery of the card.

The CNS has no single owner, so the organisation depends upon the particular administration adopting it. The most important CNS project is the one of Regione Lombardia. In this case, obviously the owner is the Regional Government and the card is delivered by a consortium and manufactured by its subcontractors (the main is Siemens, which was responsible for two subproject, "cards" and "card management"). The trust centre is under direct control of the Region.

Also the CMD has no single owner. In the case of the Defence, the full process (with the only exception of the card manufacturing, in charge of the IPZS), is under direct responsibility of the Defence Administration. Because the PKI is hierarchical, each of the armed forces has direct control over one of the sub-roots (and relative directories).

Management of biometric data

One important issue deals with the management of biometric data. Templates are always used instead of full images. Particularly, for the CIE, templates are only stored on the card, so that the verification possible is only of the type "one to one".

Management of personal and sensitive data.

As said before, each municipality has access to its civil register. No difference exists with respect to the previous organisation from this perspective. However, a shared pointer to the local register is in place (INA, Indice Nazionale delle Anagrafi). This allows, under certain conditions, to exchange relevant information between administrations.

In the case of health data, the citizens also have to provide a written consent to allow the processing of their data.

Interoperability (at national level)

Interoperability was addressed with main focus to the country. However the approach followed is interesting, because it allows a full interoperability both between card vendors and card projects.

Interoperability between card vendors was achieved by the issuing of a national standard, on behalf of CNIPA. It comprises all the OS commands which have to be supported by any vendor wishing to sell cards for one of these projects[9]. This means that, for example, within the scope of one single project cards of different vendors may coexist[10]. Obviously, this approach is of great advantage for the Administration, which can this way purchase the same product by a number of vendor.

[9] More precisely, the standard is issued only as CNS, but – as already mentioned – the differences with the other cards are negligible and in the near future, an official adoption of the CNS commands is most probable.

[10] This is what happened, for example, for the ID Card and the CNS in the SISS project, where both Siemens CardOS and Incard Incrypto are used with the same applications and middleware.

Interoperability between projects was achieved by defining a common subset of the internal data structure (see previous figure 2). Having the same subset of OS commands and the same subset of the internal data structure, all applications can indifferently read the common parts from any of the cards, even if belonging to different projects.

The two following figures summarize what described above.

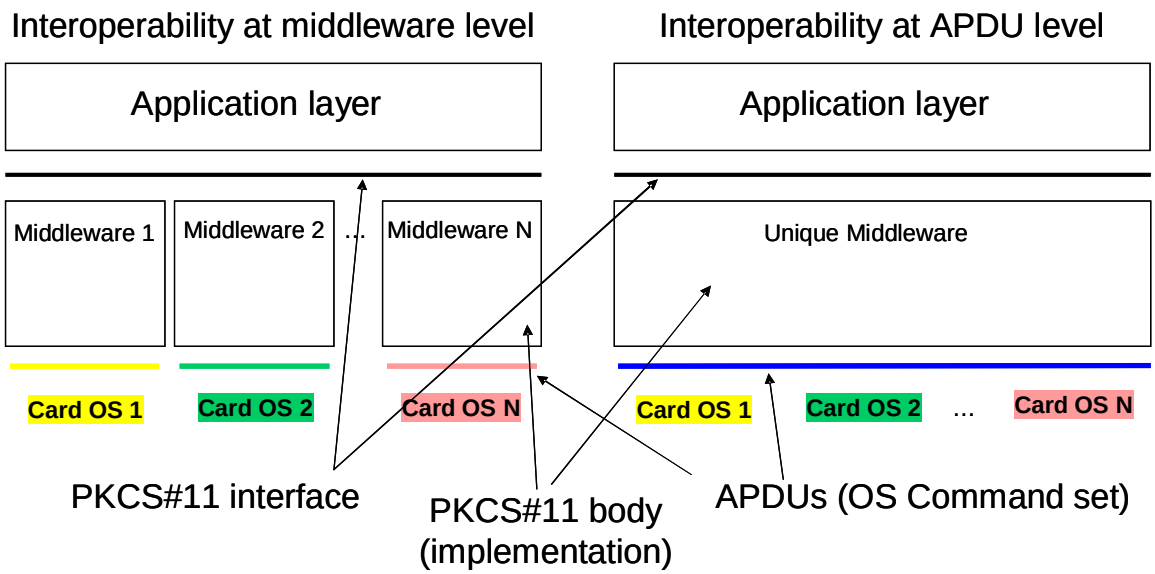

Fig. 7 – Advantages of specifying a common subset of OS commands

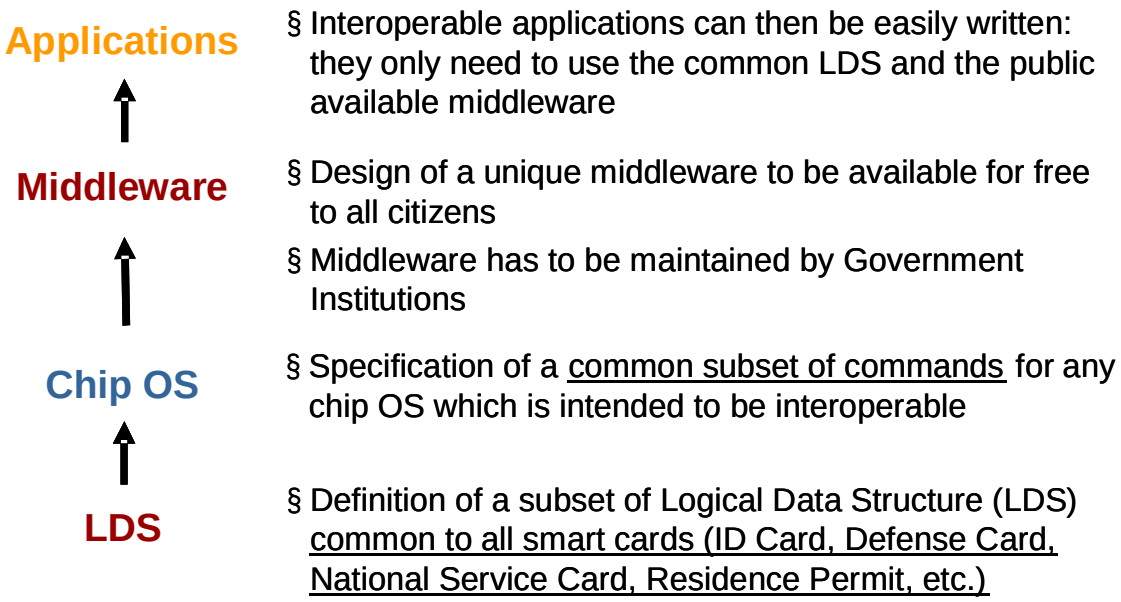

Fig. 8 – Resulting interoperability strategy

3.4 Interoperability

Interoperability at an international level was addressed especially by the SISS project (a CNS implementation). This project is in fact one of the pilots of the Netc@rds initiative. Due to the differences that exist between the various countries, the interoperable data are still only a minor portion of what is contained into the CNS card. However this pilot has a noticeable importance because it depicts a guideline toward interoperability of eHIC (electronic Health Insurance Cards) and has been joined already by a considerable number of partners (both from public and private sector).

Some interoperability tests have been conducted also with the Austrian eIDM system, but the results were mainly due to the flexibility of the Austrian system.

3.5 eIDM Applications

In the past years, especially municipalities tried to propose e-services accessible through the ID card. However, as already noticed, the big problem was the lack of card readers and/or the incomplete distribution of cards. In both cases, the result was a lack of a consistent set of services, which could overcome the status of local pilots (practically not used by citizens).

Even in Regions where all citizens have a card, like in Lombardia, e-services encounter difficulties to be set up. For this reason the Region recently issued a tender for millions of card readers to distribute to citizens.

Looking at the CMD and its use in the Defence administration, the most important application recently deployed is the access control to buildings, also if the card could be used for a set of other functionalities.

The main conclusion of this experience is that still cultural problems, in addition to organisational ones, are preventing a convincing use of cards as a key for e-services.

The situation will be finally overcome when the citizen will start to see real advantages in using their electronic cards, which requires continuous efforts in more than one direction: organisational (design and provision of services), communication (to push citizen and manufacturers to consider smart card readers as an essential PC device), cultural (to help citizens to become familiar with the new tokens, many of them not having idea of the meaning and possibilities of the microchip).

3.6 Future trends/expectations

As already mentioned, the CNS should disappear as soon as the ID Card is spread to the entire population. However, there are some doubts that this will be entirely possible.

Besides, while the ID card (and even more the CMD) has his own significance as soon as it enhances the security of the police identification with respect to the old paper based document[11], the CNS projects, which exclusively rely upon the quantity and quality of services, have to find ways to be more attractive.

One trend towards this enhancement is the adoption of dual interface chips, which could allow, for example, the provision of transport payment applications whose value added is already well understood by citizens.

3.7 Assessment

The main advantages/disadvantages are presented below for the two biggest projects (CIE and CNS, for the SISS case).

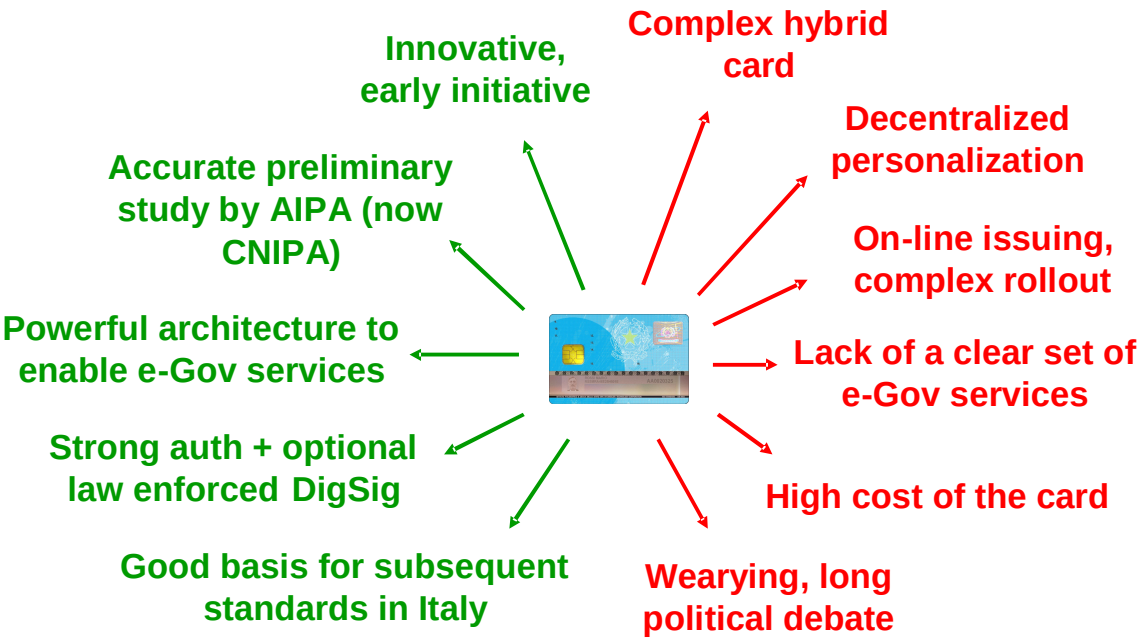

Fig. 9 – CIE advantages/disadvantages

[11] This is especially obtained thanks to the passive authentication granted by the card

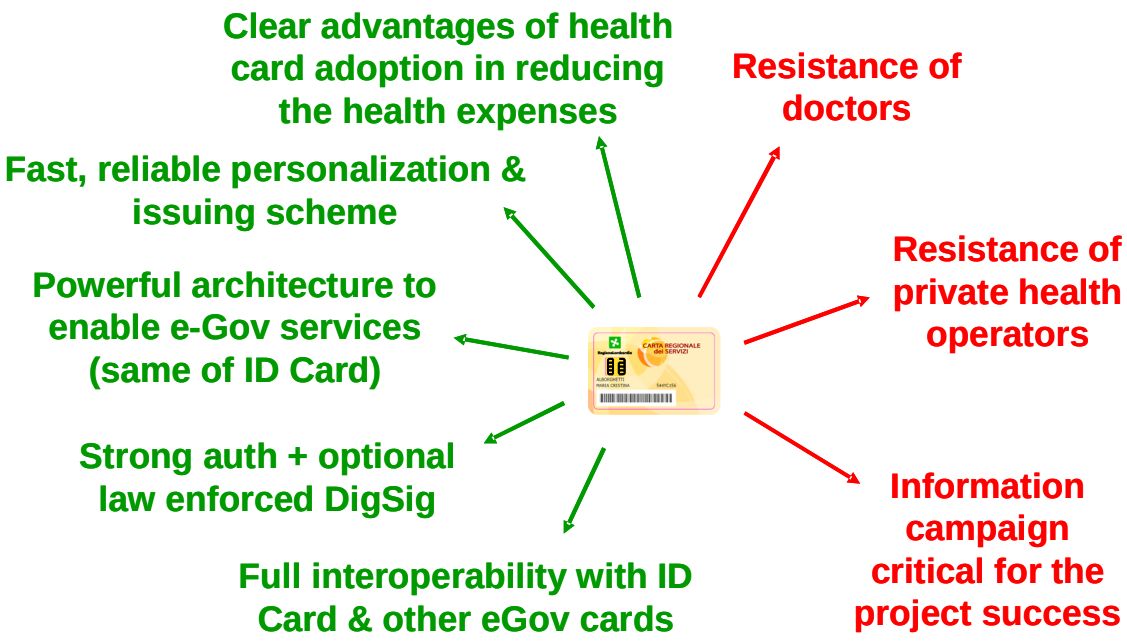

Fig. 10 - CNS (SISS case) advantages/disadvantages