eID Interoperability for PEGS

NATIONAL PROFILE FRANCE

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 French 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

The most significant eIDM system in France consists of the health network based on two different smart cards meant to authenticate beneficiaries (Vitale Card) and professionals (Healthcare professional cards –*Carte professionnelle de la Santé*- the so-called CPS card). The CPS card contains a function of authentication and signature. The Vitale card only contains a function of authentication, although a second generation of cards, more secure and technology-updated, is being issued since the beginning of 2007. This second generation integrates a function of electronic signature, although it is not yet activated. More information is available at: www.sesam-vitale.fr as regards the Vitale card, and at: www.gip-cps.fr as regards the Health professional card.

The VITALE card is delivered to any Social Security beneficiary older than 16 years and defines its rights to be reimbursed. It is based on the RNIAM number (National repertory inter-regimes of Health Insurance beneficiaries) issued on the basis of the national registration number (NIR, *numéro d'inscription au repertoire*) which functions as an authentic source of civil status information.

The Healthcare Professional card (*Carte Professionnelle de la Santé*) is based on the personal number of the owner (ADELI and SIRET numbers). The system is closely link to ADELI, the national register of healthcare professionals, and to the SIREN directory, the national register of legal persons which are economically active on French territory, from where the SIRET number is extracted.

Specific eIDM tokens to be used in e-administration processes, the Daily life card [*Carte de la vie quotidienne*], have been launched in 2003 on an experimental basis and definitively adopted in 2005. These cards are issued by local bodies (cities, provinces and regions) to manage their public services (access to library, cinema, public transportation, etc.). General and mandatory interoperability and security reference frameworks have been defined by the central administration to allow users to use a unique token in their relations with the Administration. These cards usually maintain a credit card format and offer a wide range of authentication functionalities. The identifier will depend on the sector based identifier used by the authority issuing the card.

Finally, the project of national electronic identity card should be mentioned, as the identity card, despite not being mandatory, is required in most administrative procedures to authenticate users. This project is of paramount importance in France as it is intended to substitute a series of identification means and to integrate an authentication and electronic signature block. However, the launch of the project has been accompanied with large public debate where strong opposition was manifested against the creation of a centralised citizens' databases and the use of biometrics. The project has been suspended temporarily, and should be resumed after the Presidential elections of 2007.

From a practical perspective, usage and uptake can be summarised as follows:

eIDM system	Potential user base	Actual penetration	Actual use
National eID card	French citizens (no age	Not developed yet	No public statistics are

(project)	limit)		available
Daily Life Card	Every user of a public service	No data available	No public statistic available
Vitale Card. (currently limited to health sector but planned to be used as authentication means in other sectors)	Estimated at 59 millions of Vitale Card 2 to be distributed.	50 millions of Vitale Cards and 234,677 Health care professional cards.	No public statistics are available

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

The use of eIDM systems is coordinated by the DGME, the State Modernisation General Directorate [*Direction générale de la modernisation de l'État*] (www.modernisation.gouv.fr)[4]. Created in 2006, this General Directorate, subjected to the Budget and State reform Ministry, has replaced three specific agencies established in 2003 to carry out the Action Plan 'RE/SO 2007 for a Digital Republic in the Information Society' [*Pour une République numérique dans la Société de l'Information*] presented in November 2002. In 2004, this plan gave way to a four-years Electronic Administration Strategic Plan [*Plan stratégique de l'administration électronique*] (PSAE) and Electronic Administration Action Plan [*plan d'action de l'administration électronique*] (ADELE) for the period 2004-2007.[5]

An Ordinance approved in 2005[6] has provided legal certainty to the development of eGovernment. It regulates the electronic exchanges between public authorities and between these and theirs users. Article 4 of this Ordinance compels public administrations to comply with the interoperability and security standards when they implement e-processes. Such standards have been developed by the DGME during the Daily life cards pilot projects. Moreover a specific middleware is being designed by the DGME and GIXEL, a private consortium of the card industry, and is expected to be generally used by public authorities in their e-processes.

As a consequence, at local level, public authorities manages and issue their eID token, so-called Daily Life cards, according to their specific needs and in accordance with the general framework of

[3] Decree 2005-1792 of 30 December 2005, JORF 1st January 2006.

[4] Decree 2005-1792 of 30 December 2005, JORF 1st January 2006.

[5] Coudert F., Debet A., De Hert P, 'Chapter 4: Constitutional Rights and New Technologies in France' in KOOPS, B.J., LEENES, R. and DE HERT, P., Constitutional Rights and New Technologies. A comparative study of Belgium, Canada, France, Germany, Sweden and the United States, Report commissioned by the Dutch Ministry of the Interior and Kingdom Relations, Tilburg, February 2007.

[6] Ordinance n°2005-1516 of 8 December 2005, J.O. 9 of December 2005.

reference established under the supervision of the DGME. A specific website (www.cvq.fr) has been launched in order to provide them with all the information required to build up their project.

3.2.2 eGovernment cooperation

In order to foster the cooperation between local authorities and lower the costs relative to the implementation of Daily Life cards, the use of Public Interest Groups (*Groupements d'intérêt public*, GIP) is advocated by the central government.

The Act for Law Simplification[7] states that Public Interest Groups [*Groupements d'intérêt public*] (GIP) comprise public legal persons or public and private legal persons to favour the use of information technologies for the development of e-administration or to manage hardware of common interest in this field (Article 3.II). This specific legal form has been introduced by the Act n° 82-610 of 15 July 1982 regarding research and technological development [*loi d'orientation et de programmation pour la recherche et le développement technologique de la France*] (article 21).

They offer flexible management structures more adapted to the needs of e-administration development. A representative of the Administration is mandatory and it is possible to have an audit performed by Public Finance Courts. Furthermore their statutes should be approved by the State and they can not be for-profit companies. [8]

This form has already been adopted for the deployment of the Vitale and CPS cards.

3.2.3 Traditional identity resources

ID and residence Cards

The first French ID Card was instituted in 1921 in order to secure the authentication process, for until then it was necessary to appear with two witnesses. It is only in 1940 that the card was generalised and became mandatory in order to prove one's identity from 16 years old and onwards, in the context of population control measures. This Law has been amended in 1955 and made the card optional. French Law foresees the possibility to prove one's identity by any means. In 1995, its format was secured, and in 1998 it became free of charge. It is valid for 10 years but even after this period, it can be used for authentication purposes whenever the photograph is sufficiently capable of identifying to the owner.

[7] Act nº 2004-1343 of 9 december 2004, op.cit.

[8] http://www.senat.fr/rap/r03-402/r03-4023.html

It is the sole official document which has been exclusively created for the authentication of its owner and not to grant him rights or provide him access to services. It includes not only information relative to the owner but also to the public authority which has delivered it. It is exclusively delivered to French citizens. Foreign citizens are delivered a residence card by the prefecture.

The secured ID card delivered since 1995 is a plastic card with an optical stripe which records the surname, names, gender, birth date and the number of the card (each card is attributed a specific number). However, this stripe has never been used in practice. In case of change of address, its modification on the card is facultative and the owner should ask for a new card to have it changed.

The identity card contains a number of data printed on it, specifically:

- surname, name, place and date of birth, gender, height, nationality, place of residence;
- authority who had delivered the document, his date, validity period, name and signature of the authority;
- number of the card;
- photograph and signature of the owner.

The requesting of an ID card implies that fingerprints must be taken, with the only aim of preventing fraud or of identifying a person within a judicial process. The fingerprints are not automatically processed, nor are they incorporated into the card.

In order to issue the new cards, the Ministry of Internal Affairs has been authorised to create a new centralised processing system with all information relative to the owner and the authority which has delivered the card. It contains information on the nature of the civil document produced and the date and authority which have delivered it, date and place of the request, date of reception of this request by the competent authority and by the production service, date of issuing of the card by this service, date of handover to the owner and for minors and adults under supervision, their legal representative. Fingerprints, photograph and signature are not included in this file, nor can they be transferred.[9]

National directory of natural person's identification (RNIPP)[10]

The national directory of natural persons' identification (RNIPP, *répertoire national d'identification des personnes physiques*) was created in 1941 by the Ministry for Internal Affairs of the Vichy Government with the purpose of organising administrative files and establishing demographic statistics. It has been maintained after the war but its administration was transferred to the INSEE, the National Institute for Statistics and Economic Studies (*Institut National de la Statistique et des études économiques*)[11]. Currently, the RNIPP is regulated by a Decree of 1983.[12] Every individual born in the French territory or who becomes a beneficiary of the French Social Security is assigned a registration number (NIR - *numéro national d'inscription au répertoire des personnes physiques*). It thus appears

[9] http://www.cnil.fr/index.php?id=1774

[10] Coudert F., ID number Policies – Report for France, in FIDIS Deliverable 13.3, not published yet.

[11] Decree n°46-1432 of 14 June 1946 relative to INSEE, an update version is available at: www:legifrance.gouv.fr

[12] Decree n°83-103 of 22 January 1982, relative to the national directory of natural persons' identification, an update version is available at: www:legifrance.gouv.fr

more as a population than a French citizens' directory. [13] The sole purpose of the Directory is to prevent mistakes on the identity of individuals. Its use for purposes of tracking individuals is explicitly forbidden, except under the circumstances foreseen by the Law (Art.7) which mainly refers to judicial proceedings (Art. 60-1, 77-1-1 and 93-3 of the Penal Procedure Code).

The NIR is a meaningful identifier, it's contents being based on the gender and the year, month, province and city of birth of the individual (Art. 4).

After World War II, it has been largely used by the Public Administration as a reliable identifier and particularly by Social Security Agencies. However, in 1972, its computerization with the aim of obtaining a unique identifier for French citizens together with the launch of a large project of police databases' centralisation (SAFARI) triggered a large public debate. The fear raised by the impact of this project on private life, individual freedom and public liberties led to the adoption of the Data protection Act in 1978. This Act restrains the use of the NIR and of data matching processing to a previous authorisation given either by the French Data Protection Authority, the CNIL (*Commission Nationale de l'Informatique et des Libertés*) (Art. 25.6°), by legal provisions, or by regulatory provisions issued after obtaining the (non-binding but public) opinion of the CNIL (Art. 27.1°) and under the control of the State Council (*Conseil d'Etat*)[14]. The infringement of these provisions is punished by five years of imprisonment and a fine of 300,000 euros (Art. 226-16-1 of the Penal Code). The RNIPP is currently used by Social Security agencies.

The opinion of the CNIL as regards the use of the NIR as identifier will be discussed as it is expressly adopted by the French government in its e-administration policy.[15] Since 1984, the CNIL has insisted that the RNIPP was a civil status' directory, created for preventing mistakes in the identity of individuals based on homonymy. [16] A "universalistic" concept of the NIR which would convert it to a national identifier should be avoided. This means that the NIR cannot be used as unique identifier and should be complemented by other information such as the address, etc, when it is used. Moreover, the use of this number by Public Agencies for the linking of databases is limited to a strict application of the finality principle[17]: if two public agencies are legally authorised to use the NIR and to transfer personal data to each other, then they can use it as a key for their transfers of personal data. In any other case, the CNIL considers that the sole need of linking two databases is not sufficient for justifying the use of this number.[18] This interpretation has played a key role in preventing the use of the NIR by Public Agencies as common identifier for the linkage of distinct public databases, compelling them to create their own identifiers and maintaining its use, each time broader, within the health sector.

---

[13] Lecerf J-R, Intelligent Identity and Liberties [*Identité intelligente et libertés*], Information Report to the Senate n°435, 29 June 2005, available at : http://www.senat.fr/rap/r04-439/r04-439.html

[14] The State Council is the highest administrative jurisdiction in France. It ensure the legal validity of administrative acts.

[15] Ministry of Civil Service, State Reform and Land settlement, Electronic Administration Strategic Plan (PSAE) 2004-2007, p.15

[16] CNIL, Délibération n° 83-058 du 29 novembre 1983, available at : http://www.cnil.fr/index.php?id=1380&delib[uid]=35&cHash=52a059c87b

[17] Under the finality principle, data controllers must obtain data only for specified and legitimate purposes, and must not carry out any further processing which is incompatible with those purposes. For more information about data protection principles, see FIDIS, D.11.1. "Collection of Topics and Clusters of Mobility and Identity – Towards a Taxonomy of Mobility and Identity", available on-line at: http://www.fidis.net/fidis-del/period-2-20052006/d111/doc/31/ (last access on 17 April 2007).

[18] CNIL, 20th Annual Report, 1999, p. 65

This doctrine has only been breached once by the legislator in 1998 when the Finance Act of 1999[19] authorised some Fiscal Agencies to use the NIR for fraud control. The provision allows these Agencies to use the NIR with the only purpose to avoid mistakes on identity and to verify the address of individuals in the framework of some of their competences. This provision has been challenged before the Constitutional Council which has validated it. The fact that Agencies' employees are bound to professional secrecy and that control competences have been accorded to the CNIL, as well as the existence of data protection legislation, were considered as sufficient safeguards. The Council also observed that the finality was clearly defined and that the use of the NIR would not conduct to data processing unrelated with the competences of Social Security and Fiscal Agencies.[20]

This identifier is also used to verify the information contained in the RNIAM (National repertory inter-regimes of beneficiaries of Health Insurance) and for issuing the VITALE Card. The identifier in this case is a series of 15 ciphers: the 13 ciphers of the NIR and two more for the key attributed. This identifier is also called "NIR with key". It is used in salary forms, social security claim forms and social data declarations.[21]

Foreigners register (AGDREF)[22]

Information relative to foreigners are recorded by prefectures and in a national register (AGDREF, *Application de gestion des dossiers des ressortissants étrangers en France*) administrated by the Ministry of Internal Affairs. This register contains the following information: civil status, nationality, family situation, address, conditions of entry in France, profession, administrative situation. A permanent identification number is attributed to each foreigner.

Residence cards are delivered to foreigners with the same format and information as national identity cards.

ADELI Register

The inscription in the ADELI [*Automatisation Des LIstes*] national register, relevant to the Health Ministry, is mandatory for healthcare practitioners prior to starting their activity. It contains information on the civil status of the practitioner, his professional situation and the activities he has carried out in the past. The ADELI number is used as an identifier in their relation with the Administration and it is used to issue the CPS cards and to authenticate these practitioners in the social security network.

---

[19] Art. 107 of the Act no 98-1266 of 30 December 1998, J.O. n° 303 of 31 December 1998, p.20050.

[20] Constitutional Council, DC n°98-403, Finance Act for 1999, 29 December 1998, Recueil p. 326 – J. O. of 31 Décember 1998, p. 20138.

[21] Direction Générale de la modernisation de l'Etat, Référentiel Général Interopérabilité Volet sémantique V.0.93, available at : https://www.ateliers.modernisation.gouv.fr/ministeres/domaines_d_expertise/architecture_fonctio/public/rgi/referentiel_general7230/downloadFile/file/Referentiel_general_Interoperabilite_Volet_Semantique_V0.93.pdf

[22] More information on this register is available at: http://www.cnil.fr/index.php?id=1812#2626, (last access on 17 March 2007)

National directory of legal persons (SIRENE)[23]

The National directory of legal persons is managed by the INSEE. It contains the "civil status" of all legal persons which deploy an activity within French territory, irrespective of their legal form, their sector and area of activity. Six million companies are registered.

The directory is formed by the name and address of the company, its legal category, its main activity, and its establishments.

The legal person is attributed a SIREN number which last for the whole lifetime of the company. It consists of 9 ciphers, the first eighth are attributed sequentially, except for public bodies which start with 1 or 2, and the ninth is the control key. This identifier is used in the relations with the Administration.

Each establishment is attributed a SIRET number which consists of an association of SIREN number of the parent company and an Internal classification number (NIC - *Numéro Interne de Classement*) formed by 5 ciphers.

The SIREN number is also used for issuing other identifiers for legal persons, such as for instance the European VAT number or the identification of independent.

The French identification system of legal persons is consistent with the ISO 6523 standard.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

Authentication policy

Article 4 of the Ordinance n°2005-1516 requires public authorities to comply with the general Interoperability and Security frameworks of reference. The Interoperability framework of reference defines technical rules ensuring the interoperability of public information systems and relates to data

[23] Direction Générale de la modernisation de l'Etat, Référentiel Général Interopérabilité Volet sémantique V.0.93, available at : https://www.ateliers.modernisation.gouv.fr/ministeres/domaines_d_expertise/architecture_fonctio/public/rgi/referentiel_general7230/downloadFile/file/Referentiel_general_Interoperabilite_Volet_Semantique_V0.93.pdf

repositories, norms and standard administration (Art. 11 Ordinance). A recent decree[24] defines the conditions for its elaboration, modification and publication. It aims at making consistent all public information systems and ensuring an easy integration of new ones and their general evolution, as well as an easy utilisation by the user. The initiative "Digital identities and access rights" has set up a series of organizational functionalities in order to manage the process of authentication. (More information can be found at: http://synergies.modernisation.gouv.fr/rubrique.php3?id_rubrique=16).

The general Security framework of reference (*référentiel général de sécurité*)[25], the so-called Security inter-sector framework of reference [*Politique de référencement intersectoriel de sécurité*] (PRIS), distinguished three different security levels according to the sensitivity of the data exchanged and the risk of identity theft: middle, strong/standard and strengthened. The level of security required for each service offered is defined by the public authority providing the service.

It should be mentioned that the CNIL has set up a 'gradual security principle' in its opinion on the Electronic Administration Plan[26]. It advocates for the respect of anonymity where the authentication is not required for the provision of the public service. Where authentication is required, the authentication means should also pass a strict proportionality test: security requirements should be adapted to each e-process. The use of electronic signatures should not be systematic and, according to the CNIL, does not constitute a prior condition for the implementation of e-processes.

Actually, most existing e-processes do not use electronic signatures, but rather rely on authentication processes based on identification codes attributed by the administrative body and a password chosen by the user. The electronic signature is not intended to be generalised, but only to allow the dematerialisation of services which require a high level of security. It is currently used for VAT e-payment, medical acts with health professional cards, income e-declaration and for certain services provided through Daily Life Cards.[27]

The process of identification is based on the procedure developed by the Ministry of Economy, Public Finances and Industry in the year 2000 when the first e-processes were launched. The DGME (ex-ADAE) has extended the procedure to all public administration in 2004 and integrated it into the PRIS.

As regards the identifiers used for authentication functions, the French government expressly opted for adopting sector based identifiers in accordance with the position of the CNIL on the use of the NIR. [28] It is foreseen to use federated identities which would allow the user to get a unique identifier for accessing public services and prevent any link to be made between public databases. Therefore,

[24] J.O. nº53 of 3 March 2007.

[25] Decree nº2007-284 of 2 March 2007 on Interoperability general frame of reference [*relatif au referential general d'interopérabilité*], J.O. nº 53 pf 3 March 2007, page 4060.

[26] CNIL, 26 February 2004, Op. cit.

[27] http://www.senat.fr/rap/r03-402/r03-4023.html

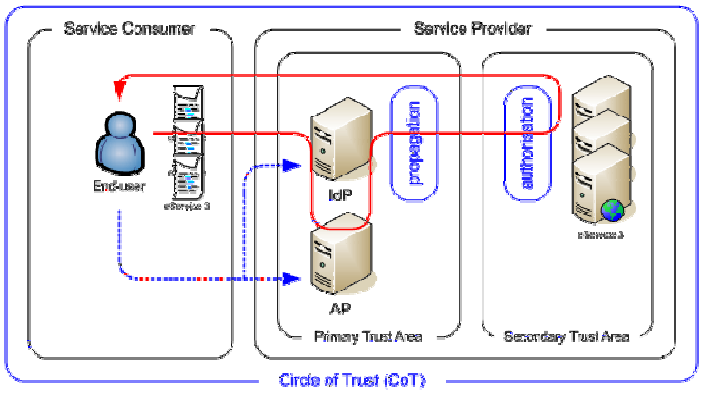
[28] Ministry of Civil Service, State Reform and Land settlement, Electronic Administration Strategic Plan (PSAE) 2004-2007, p.16

public authorities issuing an eIDM system will be able to adopt the same identifier they use in their relation with their users.[29]

Also, 4 main authentication scenarios have been advanced (http://synergies.modernisation.gouv.fr/article.php?id_article=663):

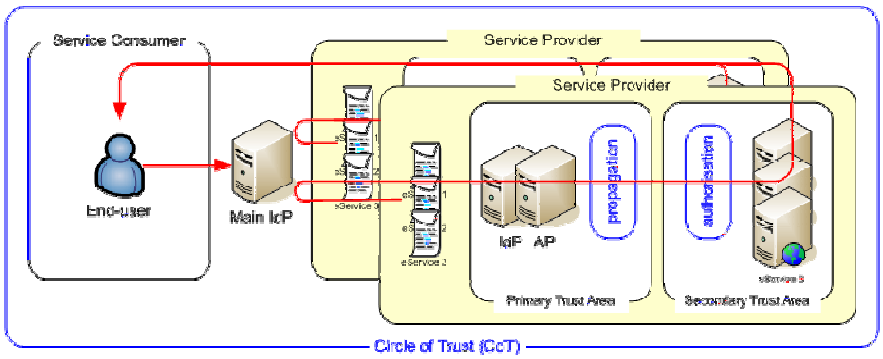
Scenario 1a:

- The authentication and access control area are hosted by the Service Provider and are offered to end-users who do not have any technical device.



Scenario 1b:

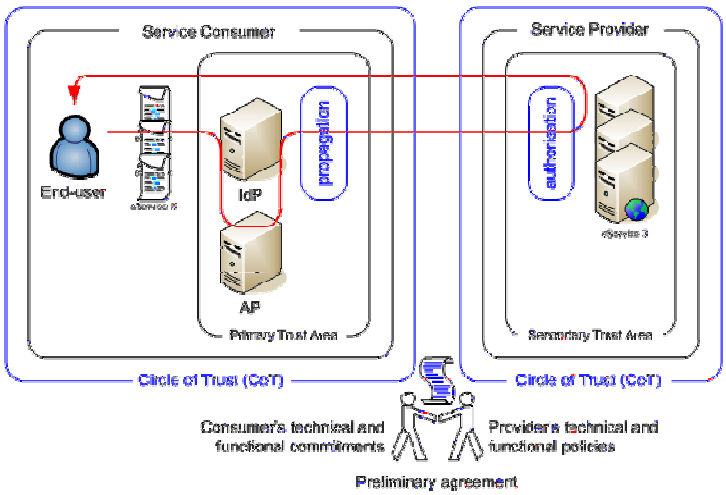
- The authentication and access control area are hosted by the Service Provider (extension of the previous scenario for end-users who don't have any technical device)
- The end-user identifiers are federated ; the main IdP hosts the federation keys



Scenario 2a:

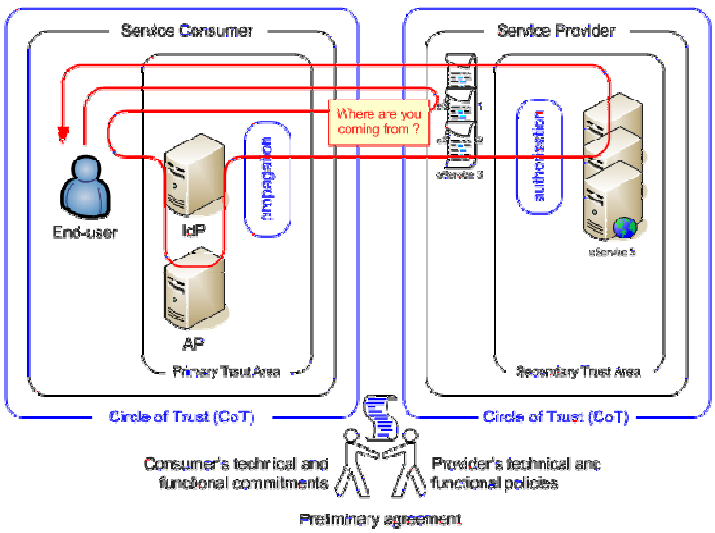
[29] Ministry of Civil Service, State Reform and Land settlement, Electronic Administration Strategic Plan (PSAE) 2004-2007, p.16

- The authentication area is hosted by the Service Consumer
- The access control area is hosted by the Service Provider
- An agreement describes how Circles of Trust are federated
- Use case : for organisations with authentication device, big diversity or particular « business » roles



Scenario 2b:

- The authentication area is hosted by the recipient
- The access control area is hosted by the Service Provider
- An agreement describes how Circles of Trust are federated
- Use case : for organisations with authentication device, few diversity or standardized « business » roles



The Daily life card

The ADAE (now integrated into the DGME) has promoted and developed the project « Daily Life Card » (*Cartes de vie quotidienne*) which intends to provide access to all services provided by the municipality, province of region (or all of them) such as public transportation, library, school, swimming pool, etc). These smart cards can be provided with authentication, payment and signature functions. This project intends to give an impulse to public services, stimulating concrete initiatives in benefit of the user, carried out by local bodies and based on customisation.[30]

In June 2003, the Ministry for State reform called for tenders. The goal was to experiment with as many types of services as possible with a view of generalising such cards, as well as encouraging the sharing of experiences. This project laid down four main principles: respect of (recommended) technical standards, development based on open source software, study of the card uptake by the users and public/private innovating partnership. 14 pilot projects from 60 presented were selected. [31]

In 2005 the experimentation phase has terminated and several local entities have started to develop their own projects. It thus gave way to the second step, focused on resource sharing in order to lower project costs on the basis of the general technical, legal and organisational frameworks of reference intended to local bodies and private partners.

A specific website (www.cvq.fr) has been created by the central government with all the required information in order to design a project of implementation of these smart cards. This website provides a toolbox for local administrations which are willing to implement e-processes and more specifically to deliver smart cards to their users. Furthermore, this frame of reference will be used as basis for a label recognising initiatives and giving a better visibility to the actors of the project.[32]

The authentication procedure of the user will therefore depend on the options selected by the local authority. For instance, in Paris, the Navigo card deployed by the RATP, the Parisian public transportation company, is a contactless smart card with RFID technology which enables its user to use public transportation. In Issy-les-Moulineaux, an authentication card has been issued to users of cultural services which allow them to book equipments on-line, etc. This card will be extended to the educational sector, and eventually to remote management of electronic administrative acts which will require PKI functions.

The Vitale Card and Healthcare Professional Card

Deployed in 1998, SESAM-Vitale intended to computerise the healthcare system and to modernise, simplify and accelerate exchanges between the administration, the user and the healthcare professionals. The first step consisted of a claims form dematerialisation which entailed the deployment of more than 60 million chip cards to the users (Vitale card) and 256,766 cards to healthcare professional (Healthcare professional card). However, use of the card is not mandatory

[30] http://www.adep-france.fr/v2/decouvrir-les-avancees/cvq-projetADAE.html

[31] http://www.adep-france.fr/v2/decouvrir-les-avancees/cvq-sites-porteurs.html

[32] http://www.adep-france.fr/v2/decouvrir-les-avancees/cvq-projetADAE.html

and the user still has the option of using paper based claim forms, although it is intended to replace and secure the reimbursement procedure.

The Vitale card is a personal card attributed to every beneficiary of French social security from 16 years on. Since 1996, the Health Insurance Funds [*caisses d'assurance maladie*] has the obligation to deliver to every beneficiary the "electronic individual card", the so-called Vitale-card (Art. L.161-31 of Social Security Code). Its use however is not mandatory.

The card has the dimensions of a bank card and allows its user to justify his reimbursements rights. It contains the NIR, name and surname of the owner and its beneficiaries, the social security regime, the competent administration in charge of his file and its reimbursement rights (Art. R.162-33—1 Social Security Code. This card should be updated at 'green access points' whenever the situation of the owner has changed. Since 2004, the owner should indicate his family doctor.[33]

In 2005, two engineers have identified a breach of security in these cards as the data were not encrypted but only codified. The software of encryption had not been activated for economic reasons. It was thus possible to access the data and to forge cards.

Aiming at preventing fraud, The Vitale card 2 will integrate a photograph of its owner on the printed face and in the chip. The chip could contain more information, e.g. relative to the person to call in emergency cases, the holder's blood group, the name of their general doctor, details of their social insurance company and their choice with regard to organ donation. It is being distributed since 2007.

This is a smart card consistent with the ISO 7816 standard with re-writable technology and a crypto-processor (Art. 1 of Ministerial Decree of 14 March 2007[34]). The chip contains two certificates, the first allowing the authentication of the card and of its user. The latter certificate will permit to activate an electronic signature function (Art. 2).

Moreover, this card will be the key to the Medical personal file which should be available to all beneficiaries from July 2007 (Article L161-36-2 of the Social Security Code). Furthermore, it is foreseen that this new card could be used as authentication means outside health sector.

The CPS cards contain mostly the same information expect from the photograph (Article R.161-62 Social Security Code). The identifier used is not the NIR but the identification number of the owner (ADELI and/or SIRET number). This chip card contains two certificates, one to authenticate the user through a PIN code and the other with electronic signature functions.

The future eID card

[33] http://fr.wikipedia.org/wiki/Carte_Vitale

[34] Ministerial decree of 14 March 2007 relative to physical and logical features of health insurance card and to the data contained in this card [*relatif aux spécifications physiques et logiques de la carte d'assurance maladie et aux données contenues dans cette carte*], J.O of 17 March 2007

In 2003, a project for an eID card, INES (Secured electronic national identity - *Identité Nationale Electronique Sécurisée*), more secured and which would incorporate biometric features, has been launched. However, after a large public debate, numerous objections to the project have been raised leading to its suspension. Although the eID card is still in its planning phase, its importance in eGovernment policies when it will be implemented and the expectations it raises justify its inclusion in this report.

This eID card is foreseen to improve the security of the card, preventing fraud and ID thefts, mostly by securing and centralising the delivery procedure and the introduction of two biometrics identifiers (picture and fingerprints). The project suggests also a possible combination of the current ID card and the passport, which would effectively imply the suppression of the former. Several points are under discussion as regards the identifier to be used or the possible mandatory nature of the ID card. A general fear has emerged from the debate as regards the constitution of a centralised database of French citizens, increased by the announced use of biometrics identifiers (fingerprints).

Moreover, it is planned to provide the IDCard with electronic signature function to be used in public and private sector. This option however raises the concern of the liability of the State as certification authority and of its effects on the market.

3.3.2 Legal framework

The main legal framework is laid down in the following Acts:

- Vitale Card:
  - Art. R.161-33-1 to R.161-33-10 of the Social security Code
  - Act n° 2004-810 of 13 August 2004 related to Health Insurance[35]
  - Decree n° 2007-199 of 14 February 2007 related to the health insurance card[36]
  - Ministerial decree of 14 March 2007 relative to physical and logical features of health insurance card and to data it contains[37].

- Healthcare Professional (CPS) Card:
  - Decree n° 98-271 of 9 April 1998 relative to healthcare professional card[38]
  - Articles R161-52 à R161-58 of Social Security Code
  - Ministerial Decree of 9 April 1998 relative to physical and logical features of healthcare professional cards[39]

[35] J.O. of 17 August 2004

[36] J.O. of 15 February 2007

[37] J.O of 17 March 2007

[38] J.O. of 12 April 1998

[39] J.O. of 15 April 1998

- e-Administration:
  - Ordinance n° 2005-1516 of 8 December 2005 on electronic exchanges[40].
  - Decree of 2 March 2007 relative to the Interoperability general frame of reference[41]

- Electronic signatures:
  - Act n° 2000-230 of 13 March 2000 adapting evidence Law to information technologies and to electronic signature.[42]
  - Decree n° 2001-272 of 30 March 2001 in application of article 1316-4 of the Civil Code and relative to electronic signature.[43]
  - Ministerial decree of 26 July 2004 relative to acknowledgment of certification service providers' and the official recognition of the evaluation bodies[44]

The Ordinance on electronic exchanges between public authorities and users and public authorities have established a general framework for the development of e-administration in France. This Ordinance specifically deals with authentication procedures compelling public authorities to comply with a general Interoperability and Security frame of reference. The Security frame of reference which relates to authentication procedures is under elaboration by the DGME. However a draft version can be consulted at: http://synergies.modernisation.gouv.fr/article.php3?id_article=381

Authentication procedures are established in the Interoperability frame of reference, which can be consulted at: https://www.ateliers.modernisation.gouv.fr/ministeres/projets_adele/adele_121_gestion_de/public/adele_121_-_gestion/view

The access and use of the information in the eIDM, as well as the basic rights of the user are subject to the provisions of the Data protection Act. It should be mentioned that a specific electronic space will be allocated to every user by the central government. This space, the so-called "monservicepublic.fr", will enable the user to store any relevant documents to his relation with the administration. The user will able to transfer these documents directly to the public authorities which require it. However, this space is strictly personal and can not be accessed by the public authorities. (Art. 7 of the Ordinance n°2005-1516). It is confided to a safe whose key is handled by the user who can open it on a case-by-case basis in his relationships with the administration.

As regards the use of identifiers, as mentioned above, French government has opted for a sector based identifier, following the opinion of the CNIL issued from the use of the NIR by the Administration. In order to simplify the authentication procedure to the user, a federated identities mechanism based on Liberty Alliance standards is foreseen to be implemented.

[40] J.O. 9 December 2005

[41] J.O. of 3 March 2007

[42] J.O. of 14 March 2000

[43] J.O of 31 March 2001, consolidated version available at : www.legifrance.gouv.fr

[44] J.O. n° 182 du 7 août 2004

The future e-ID is planned to be able to be used as an electronic signature means by the private sector. Currently, the only law that foresees authentication means for the private sector is the e-Signatures law of 13 March 2000, which faithfully transposes the provisions of the e-Signatures Directive.

3.3.3 Technical aspects

Technical frames of reference

Two frames of reference have been defined by the DGME. Their specifications apply to any eIDM issued for the providing of public services. In addition, the central government has developed a specific middleware intended to be used by all public authorities, but does not impose providers nor to the administration nor to the users who can use any of the officially recognised tokens.

The Interoperability general frame of reference [*Référentiel Général d'Interoperabilité*] defines a set of standards which intend to make consistent the whole public information systems and to facilitate the integration of new ones, as well as its general use. As regards identifiers, the Government advocates the use of federated identities and the standard set up by the Liberty Alliance in order to avoid the use of a single unique identifier. This system allows the user to use a unique identifier to access every services without the possibility of linkage of public databases.[45]

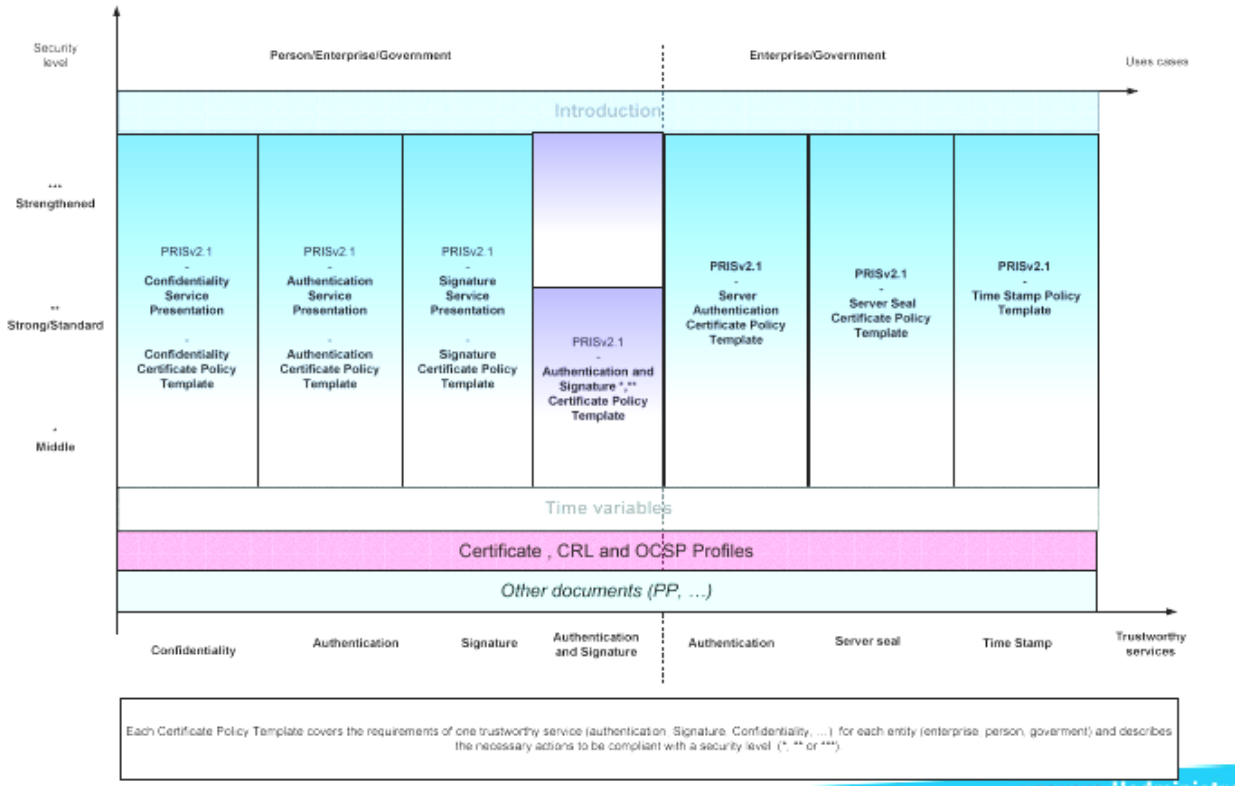
Shibboleth has been chosen by the Universities and some other standardized SAML use-cases are used by the Social Protect Organisations and the National Education Academies.

However, the linkage of systems should not be deployed in detriment of security. The security frame of reference (PRIS) defines security functions requirements such as electronic signature, authentication, confidentiality, timestamping and e-archiving, as illustrated in the table below[46]. It defines three levels of security depending on the existing risk of ID theft (middle, strong/standard, strengthened). This assessment is carried out by public authorities issuing the eIDM. Daily Life cards, Vitale Card and the future eID card are considered to require a high level of security.[47]

[45] Ministry of Civil Service, State Reform and Land settlement, Electronic Administration Strategic Plan (PSAE) 2004-2007, p.16

[46] The graph is extracted from Schiavo M., PRIS V.2.1, A general security frame of reference, available at: http://synergies.modernisation.gouv.fr/IMG/pdf/061129_PRIS_US_ENISA.pdf

[47] Ministry of Civil Service, State Reform and Land settlement, Electronic Administration Strategic Plan (PSAE) 2004-2007, p.22



It applies to security products and trustworthy service providers within electronic exchanges between users and public agencies and between public agencies. The general PRIS framework is based on standards ISO TS 101456 and RFC 3647. The authentication function is based on asymmetric keys and X509 certificates. The following table describe the different authentication requirements set up by the PRIS:

Trustworthy service providers	Strengthened	Strong	Middle
Registration phase	Face to face	Face to face	- Sending of a registration file in paper form (with certified copy of the identity papers) or in electronic form or communication of a specific element of the subscriber allowing to identify it within an administrative data base.
Delivery /acceptance of a certificate	-Delivery in person with face to face if not done during registration phase -- If AC does not generate the key, to check if the certificate is well associated with the corresponding private key -- Explicit acceptance of the certificate by the subscriber	-Delivery in person with face to face if not done during registration phase -if possible, explicit acceptance of the certificate by the subscriber or tacit acceptance starting from a sufficiently reliable handover date.	- Delivery by email - Tacit acceptance

Trustworthy service providers	***	**	*
Certificate revocation	Formal authentication of the request via a strong mechanism (ex: series of 4/5 questions/answers, use of a certificate and tool **,...) - Service : - available 24/24 and 7/7 - unavailable maximum : 2h per month. -Time between validation of the request and update of information less than 24h (7/7)	Formal authentication of the request (ex: series of 3/4 questions/answers, use of a certificate and tool *,...) - Service : - available 24/24 and 7/7 - unavailable maximum : 4h per month. -Time between validation of the request and update of information less than 24h (7/7)	- Authentication of the request by checking one or two information on the person (phone number, address, …) - Service : - available at least during working days - unavailable maximum : 4h per month. -Time, between validation of the request and update of information less than 1 working day
Certificate Revocation List	-At least, publication of CRL. - Recommendation of implementation of deltaCRL and an OCSP service. - Service : - available 24/24 and 7/7 - unavailable maximum : 4h per month.	-At least, publication of CRL. - Recommendation of implementation of deltaCRL and an OCSP service. - Service : - available 24/24 and 7/7 - unavailable maximum : 4h per month.	-At least, publication of CRL. - Recommendation of implementation of an OCSP service. - Service : - available at least during working days - unavailable maximum : 32h per month.
CA Key pair protection	-Generation and protection of the CA keys and certificates in a cryptographic module certified at a level CC EAL4+ - Key Ceremony under the control of at least two people (security responsibility) and at least two external witnesses (of which a recommended public officer). - CA Private keys controlled by at least two people with security responsibility (secret share) - Private CA keys activated by at least two people with security responsibility	-Generation and protection of the CA keys and certificates in a cryptographic module certified at a level CC EAL2+ -Key Ceremony under the control of at least two people (security responsibility) and at least one external witness -CA Private keys controlled by at least two people with security responsibility (secret share) - Private CA keys activated by at least two people with security responsibility	-Generation and protection of the CA keys and certificates in a cryptographic module compliant to the requirements in the CP Template --Key Ceremony under the control of at least one person (security responsibility) and several witnesses -CA Private keys controlled by at least one person with security responsibility - Private CA keys activated by at least one person with security responsibility
Subscriber Private key generation (if generated by CA outside the authentication device)	-Generation in a cryptographic module certified at a level CC EAL4+	-Generation in a cryptographic module certified at a level CC EAL2+	Generation in a cryptographic module compliant with the requirements in the CP Template

Authentication Key length	- RSA : 2048 b - DSA : 2048 b /q = 256	- RSA : 2048 b - DSA : 2048 b /q = 256	- RSA : 1024 b or 2048 b - DSA : 1024 b/q=160 or 2048 b/q = 256
Authentication device	- A device CC Certified at a level EAL4+ .	- A device CC Certified at level EAL2+	- Compliant to the requirements in the CP Template
Authentication application	- An authentication application CC certified at a level EAL2+ .	- An authentication application CC certified at level EAL2+ should be used	
Module to verify the authentication process	- A module CC certified at a level EAL2 should be used	- A module CC certified at a level EAL2 should be used	

The French government has set up a CA hierarchy with a general accreditation body (the COFRAC *Comité français d'accréditation*). This body accredits certifications authorities which qualifies trust service providers, according to the requirements stated in the PRIS. These certification authorities are usually constituted in GIP and sector specific (GIP-CPS, GIP-SESAM, GIP-MDS, etc.). This procedure has been developed by the Ministry of Economy, Public Finances and Industry in the year 2000 when the first e-processes were launched (e-VAT, e-Income). The DGME (ex-ADAE) has extended the procedure to all public administration in 2004 and integrated it to the PRIS.

More information is available at:

http://synergies.modernisation.gouv.fr/article.php3?id_article=381

The French eIDM system is based on Liberty Alliance standards and functions with Trustworthy service providers, decentralized repositories of attributes and different identity providers. The identity is federated through a web portal.

Consistent with Liberty Alliance standards, the French government has opted for a decentralised repository of attributes. Each public administration manages its own databases. When additional information is required from other administrations for the provision of the service, it will be exchanged between both administrations on the basis of the consent of the user.

As mentioned above a specific middleware has been developed by the DGME/SDAE and a private consortium of cards' industries, GIXEL (Cards Industrial Group - *Groupement des Industriels de la carte*), named IAS, to guarantee the interoperability of public information systems. It includes functions of authentication, encryption (files and emails), electronic signature (qualified or not). The objective is to be able to use a sole card driver IAS for any e-administration card on any computer. The first version has been issued in October 2004 with a limited diffusion, which could be run under Windows XP, 2000 and ultimately under Vista. An adaptation has been made to run the middleware under Linux and Mac OS 10.4. A review of features is currently taking place, planned to be operative under Windows XP during the second trimester of 2007.

This middleware can be used either with smart cards or USB keys. In particular, it is foreseen to be used with civil servant's cards (*carte Agent*), Vitale cards 2, future national eID cards and with any other card compliant with the standard.

The middleware is based on the following standards:

- ISO 7816, ISO 7816-15
- API standards:
  - CWA 14169 (PP Secure Signature Creation Device)
  - CWA 14890 E-Sign Area K (Application Interface for Smart Card used as Secure Signature Creation Device, Part 1 and 2)
- PKCS#15 for certificates X509 V3
- PRIS V2 and cryptographic objects.

Only the contact mode is currently taken into account.

It consists of three different modules:

- a module CSP with CAPI interfaces (Microsoft environment)
- a module PKCS#11 interfaces (other environments)
- a module called Specific IAS API which offers interfaces to manage qualified signatures, mutual authentication (card, server), any functions necessary to the establishment of a secure channel and a transparent function allowing the sending of APDU segments and the access to files.

These modules are delivered together with tools facilitating the use of cards and certificates.

To be officially recognised, a card should comply with a qualification reinforced level (PP SSCD), middleware IAS, card readers, interoperability with e-processes, i.e. with areas of e-administration data.

The identification can be done on the basis of a PIN Code or biometrics data.

Vitale Card 2 and Healthcare professional Card [48]

A new card, more secure and with more possibilities of use started being rolled out across the country from the beginning of 2007, the so-called Vitale 2. All the current cards are expected to be replaced by 2010. It has new technical features:

- more capacity (32ko Eeprom memory)
- crypto-processor
- certified common criteria EAL4+ (PPSSCD;PP9911)
- standard ISO7816, EMV

[48] GIP SESAM-VITALE, Vitale Card 2, available at : http://www.sesam-vitale.fr/ps/pdf/carte_vitale2_fr_eng_br.pdf

- Base identification, authentification, signature (IAS standard, middleware developed by the central administration).

The security standard is equivalent to bank cards. The print face will integrate the owner's photograph and the card will be individual and not familiar as for the current Vitale card.

The future eID Card[49]

The new card will adopt the format of credit card. On the card, the same information as on the actual identity card will be printed. The information stored in the chip will be divided in several and distinct blocks:

- Identity block: confidential and with a high level of cryptography, it will be accessible only to authorised authorities (logged of accesses, nominative authorisation of agents, etc.). It will contain the same information as the one printed in the card, the digitalised picture and two fingerprints.
- Authentication block: it will contain the mechanism allowing the automatic proof of the authenticity of the card (to prevent fake cards). This mechanism will be anonymous in order to ease its use in daily life.
- Owner authentication block or qualified authentication by a PIN Code: it will allow the access to public or private e-processes.
- Electronic signature block: it will allow through a PIN Code to sign electronically authentic documents for any transaction.
- Personal file block: it will allow the owner to store complementary information on his card either to ease certain electronic transactions, e.g. to store his name, surname, address in an exportable format to fulfil forms, or to substitute other documents such as driving license, tax number, etc.

The card will be initially provided with two interfaces: the access of identity data by authorised authorities will be wireless but the other functionalities would be used by the use of a PIN Code through a card reader.

The card will incorporate biometric data such as a photograph and fingerprints. These data are foreseen to be centralised into a national database.

[49] Ministère de l'Intérieur, de la sécurité intérieure et des libertés locales, INES Programme, 31 January 2005.

3.3.4 Organisational aspects

In practice, authentication services using smart cards implement the specific middleware provided by the central government. The user authenticates himself using a standard interface prompting him for his PIN Code, using a generic PC or a specific public point of access.

French government has opted for a decentralised storage of the data with limited exchanges of information between public authorities as general rule. Some exceptions are foreseen due to the nature of certain services provided which will be strictly regulated in collaboration with the CNIL. These exceptions will be carried out in practice only when no other options are possible.[50]

The decentralised system promoted in France leaves every public authority in charge of managing the whole process of issuing, delivering and administration of the card. For instance, the VITALE card is issued by the Health Insurance Fund (related to the Health Ministry) and the Daily Life card by each local authority (cities, department, regions). The future eID will be issued by the Ministry of Internal Affairs. These public authorities are verifying and guaranteeing the accuracy of the information stored in the card as, because of the sector specific identifier policy adopted by the French government, they are the only ones entitled to access to the specific directory.

The federation of identity solution retained by the central government makes each public administration an authority of attributes, by managing their own specific directories or repositories.

As regards the interoperability wished by the central government between the different eIDM implemented, federated identifiers are foreseen to be used. The DGME is a formal partner of the Liberty Alliance.

Currently the option being experimented with is to manage the federation of identities through a unique portal, www.monservicepublic.fr. The procedure implemented is thus specific to this project[51]. The user first has to create an account on www.monservicepublic.fr (MSP). When doing so, he defines the authentication means he wants to use to access his personal account. Different levels can be defined. The authentication information is recorded by the MSP's authentication module and associated with an account created by the MSP's Identity provider. The latter thus know the user by his MSP identifier. To initiate the mechanism and create the federation's first access account, the creation of MSP portal accounts is accompanied by its federation with the MSP Identity Provider. The MSP Identity provider generates a first federation key that will be transmitted to the MSP portal in the capacity of the user's federation key for the pair MSP Identity provider (Identification Provider)/MSP portal (Service Provider).

[50] Ministry of Civil Service, State Reform and Land settlement, Electronic Administration Strategic Plan (PSAE) 2004-2007, p.14

[51] Description of the federation procedure is extracted from ADAE, 'Architectural vision "Liberty Alliance" version 1.0', Sepetember 2004, available on-line at: …, p36-38.

Once created, an account in MSP which had provided him with a specific identifier, the user connects his browser to the site of the different public administrations where he has a specific identity. He uses his usual identifier recorded in the local repository of the public administration. At this stage, the user will be explained that the fact of having a Single Sign-on enables him to transparently access various public services with only one authentication, either by connecting to the MSP portal or by directly accessing the public service site.

If the user has no session open with the MSP Identity provider, the latter asks the former to authenticate. The MSP Identity provider sends the results of authentication (Authn Response), indicating success and the level to the public authority as well as the required federation elements. The Public authority retrieves the federation key and records it in its own repository. Interactions between the identification provider and the service provider take place directly using the SOAP protocol, or indirectly based on mechanisms related to the HTTP protocol.

These administrations are required to respect the provisions of the Data protection Act. This Act provides the user with a right to access the data stored in the token, to rectification and deletion. It also entails him to be informed of every transfer of his data to third parties. In that sense, the CNIL has stressed the need to respect the principle of transparency which required the data subject to be informed of the means to access, correct his personal data, and to consent to the transfers of his data to third parties.[52] The safe created by MSP empowers the owner to keep control over the disclosure of his data.

3.4 Interoperability

In the programme ADELE, the French government advocates an active participation of France in the European cooperation related to e-Administration. In that sense, the DGME (ex-ADAE) should participate in different task forces in e-governance such as ad hoc groups set up by the European Commission and in the e-Europe 2005 programme. Bilateral cooperation is foreseen, particularly with Germany in order to define common standards and interoperability of the cards with regard to citizen electronic cards and security of exchanges.

In the health sector, the GIE SESAME-VITALE is taking an active part in the European project Netcards which works on a future European card for health insurance. This project aims at allowing Europeans to use their health card in any European country. A pilot experience has been carried out with Germany in Frankfurt where beneficiaries of French Social Security have been able to use their Vitale Card.

Another example resides in the adoption of the European standard CALYPSO for all e-tickets for public transportation implemented in France.[53]

The three other main last examples concerning the “circles of trust federation” and interoperability between organisations has been hold by organisations opening their information systems to each other. They are built on standardized SAML use-cases:

[52] CNIL, 26 February 2004, Op. cit.

[53] http://www.thematiques.modernisation.gouv.fr/autres/e_lettres/archives/marge/326.html

- The Social Protect Organisations (http://synergies.modernisation.gouv.fr/article.php?id_article=508);
- National Education Academies;
- Universities (http://federation.cru.fr/).

3.5 eIDM Applications

This section will provide a short overview of key applications for the eIDM systems.

Public sector applications include a wide range of e-processes. A specific website has been established in order to centralise the access to all public services: www.administration24h24.gouv.fr. A series of e-processes such as e-VAT or e-Income require the use of electronic signature.

Other applications local specific are available through the website of the municipalities which have launched the Daily Life card.

The Vitale and CPS card are only used as described above, i.e. by persons or institutions which are professionally involved in health care services and which have been mandated to use the specific readers needed to read/edit the data on the card. From the user's perspective, the only application is therefore the automatic reading/verification of this data, so that the appropriate benefits can be provided (e.g. refunds for medication) and the correct administrative follow-up is ensured. The Vitale Card requires the use of specific software officially recognised by the National Center of deposit and accreditation [*Centre National de dépôt et d'agréément*] (CNDA). The complete list is available at: http://www.cnda-vitale.org/Listes/F_ListAgre130.htm

Other eIDM applications are available since 2003 for end-users who don't have any technical devices to authenticate themselves. Those devices are hosted by the services provider. The best practises are currently hosted by the tax portal (http://www.impots.gouv.fr), the custom portal (http://pro.douane.gouv.fr) or the social tax portal (http://www.net-entreprise.fr).

3.6 Future trends/expectations

France is at a crossroads in eIDM as several and potential competitive authentication means, i.e. Vitale Card 2, Daily Life cards and the future national eID which all include functions of electronic signature, are being implemented. Despite the political will of letting the user choose whether he prefers to use a unique authentication means for all public applications or a specific card for each different service, the launch of the eID card can threaten the sustainability of other authentication means such as Daily Life cards.

The efforts for the harmonisation regarding interoperability and security requirements aim at allowing the use of all tokens issued by authorities granted according to the PRIS in any e-process. Therefore, in theory, a user will be able to use his Vitale card to make its on-line tax declaration. The spread of electronic signature offers a high potential of expansion with regard to public services.

The project of eID cards is still under discussion and has been hanged because of the strong criticisms it has received. Even if its abandoning seems improbable taking into account the international environment, a series of concerns remain to be solved such as the fear created by the use of biometrics, the creation of a national and centralised databases or the liability of the State as a certification authority. Political worries from municipalities also have arisen as the process of issuance of the card will be taking off a large number of them.[54]

Finally, from a technical point of view, the Government seems to advocate the use of contactless technologies. In its Strategic Plan for Electronic Administration 2004-2007, it was argued that the choice made by the Government should be considered in the long run and pointed to contactless interfaces because of their versatility and because of the international context. In order to avoid any functional breach, a transitory period is foreseen until 2010 where two interfaces cards are admitted.

3.7 Assessment

The French approach has a number of advantages and disadvantages, which can be briefly summarised as follows.

3.7.1 Advantages:

- A general legal and technical framework has been delineated during the last years, providing certainty to the development which actually takes place. The two frameworks of reference (Interoperability and Security) developed by the central government and which compliance have been rendered legally mandatory ensure consistence within the different e-administration projects.

- This actual eIDM systems used, e.g. Vitale Card and Daily Life cards, or planned to be implemented, the national eID card, are designed to evolve and provide new functionalities to their users. These systems tried to integrate new technologies in order not to become obsolete. A large range of tokens should be available for public services users in some years.

- The encouragement made to local authorities to join their effort and create Public Interests Group should lower the costs of implementation and allow smaller authorities to have their own eIDM.

[54] For more information on the results of the public debate on eID card, see Forum des droit sur l'Internet, Report on national electronic identity card [*Rapport sur le projet de carte nationale d'identité électronique*], 16 June 2005.

3.7.2 Disadvantages:

- The decentralised model followed by French administration brings forth the risk of creating inequalities between users. Not all local authorities will be able or willing to implement eIDM systems, for reasons of costs or of complexity of projects. Important differences remain between rural and urban authorities.

- The decentralised model also manifolds initiatives and could slower the spread of e-administration procedures. A centralised and coordinated deployment of e-administration by the central government could have give faster and more certain results.

- The e-administration implementation is still at its beginning and a certain confusion still exists between the different initiatives launched. A risk of overlapping initiatives, such as the electronic national identity card and the daily life card, remains.