

# eSanté

## Work Package WP12

### Health Professional Card

### Part 2 - State of the Art

Deliverable

Hanan Bouzid, Uwe Roth

Version 1.0

Final

04.02.2011





## Objective of the Document

This document describes state of the art health professional cards, citizen cards and impacts of the HPRO card initiative. Additionally some standards are listed, which are in the context.

## State of the Document

The information contained in this document describes the current view of the issues discussed until the date of publication. The authors cannot guarantee the accuracy of any information presented after the date of publication.

## Change History

Version	Status	Date	Author	Modification
1.0b6	Draft Beta	06/08/2010	URo	Splitting into Part 1: Concept Part 2: State of the Art
1.0b7	Draft Beta	23/08/2010	HBo	Content
1.0b8	Draft Beta	25/08/2010	URo	Review
1.0b9	Draft Beta	07/09/2010	URo	HPRO Card Review
1.0b10	Draft Beta	14/09/2010	SBe URo	Review Integration of Review
1.0rfc1	Request For Comments	14/09/2010	URo	First RFC Version
1.0rfc1.RK	RFC Comments	27/09/2010	RKr	Review
1.0rfc1.1	RFC Update	06/10/2010	URo	Update
1.0rfc1.2	RFC Update	12/10/2010	URo	Standards
1.0rfc2	RFC Comments	13/10/2010	URo	Second RFC Version
1.0rfc3	RFC Comments	10/12/2010	URo	Minor changes
1.0rfc4	RFC Comments	22/12/2010	URo	EU Directive
1.0rc1	Release Candidate	12/01/2011	URo	State of the Art by STORK added
1.0	Final	04/02/2011	URo	Final Version



## Table of Contents

<b>§1 Standards</b>	<b>5</b>
§1.1 Identification Cards	5
§1.2 Contactless Cards	5
§1.3 European Card Standards	6
§1.4 De-Facto Card Standards	6
§1.5 Signatures	7
§1.6 Hardware Security Modules	7
§1.7 Access Control	8
<b>§2 European Parliament and Commission</b>	<b>9</b>
§2.1 EU Directive 2005/36/EC	9
§2.2 EU Parliament Resolution 2006/2275(INI)	9
<b>§3 State of the Art of Exemplary Countries</b>	<b>10</b>
§3.1 General	10
§3.2 Special Health Professional Cards and Certificates	12
§3.3 Citizen Cards or Unspecific Authentication and Signing Cards	13
<b>§4 European HPRO Card Initiative</b>	<b>15</b>
§4.1 Overview	15
§4.2 Use Cases	15
§4.3 Functions	16
§4.3a Identification and Authentication	16
§4.3b Validation of the Credentials Stored on the Card	16
§4.3c Management of the Authorization of Access to Applications	16
§4.3d Connexion with Applications	17
§4.3e Mutualisation of the Functions	17
§4.4 Impact for the Development of a Luxembourgish Health Professional Card	18
§4.4a Layout of the Card	18
§4.4b Technical Specifications	18
§4.5 Impact for the Development of a Luxembourgish eHealth Infrastructure	19
§4.5a Necessary Systems	19
§4.5b Organisational Recommendations	19

# eSanté

<b>§5</b>	<b>Studies of STORK .....</b>	<b>20</b>
§5.1	European Citizen Cards .....	20
§5.2	Mobile Electronic Identity .....	21
§5.2a	Cell Phones .....	22
§5.2b	Mobile Tokens / Hardware Tokens.....	23
§5.2c	PDA's.....	24
§5.3	RFID & NFC.....	24
§5.3a	Components of an RFID System.....	24
§5.3b	Classification of RFID Systems.....	25
§5.3c	Transponder Construction Forms.....	25
§5.3d	Range, Frequency and Coupling.....	25
§5.3e	Internal Structure of Transponders.....	26
§5.3f	State-of-the-Art Contactless Smart Cards.....	26
§5.3g	Security.....	27
§5.3h	Identification Applications.....	28
§5.3i	Near Field Communication (NFC).....	28
§5.4	Trust Federation and Identity Frameworks.....	29
§5.4a	Shibboleth .....	29
§5.4b	OpenID.....	30
§5.4c	Conclusion.....	31
<b>§6</b>	<b>Cards in a Nutshell .....</b>	<b>32</b>
§6.1	Special Health Professional Cards.....	32
§6.1a	Germany.....	32
§6.1b	France .....	32
§6.1c	Suisse .....	32
§6.1d	Lombardy (Italy) .....	33
§6.1e	Slovenia .....	33
§6.1f	Republic of China (coll. Taiwan) .....	33
§6.1g	Québec .....	33
§6.2	Citizen Cards .....	34
§6.2a	Belgium.....	34
§6.2b	Finland .....	34
§6.2c	Italy .....	35
§6.2d	Estonia .....	35

# eSanté

## §1 Standards

### §1.1 Identification Cards

#### ISO/IEC 7810

Describes the physical characteristics.

- ID-1: 85.60 × 53.98 mm      Banking cards, ID cards
  - ISO/IEC 7813: Thickness, corner routings
  - ISO/IEC 7811: Recording data on card (magnetic)
  - ISO/IEC 7816: With embedded chip, contact surface (see below)
- ID-2: 105 × 74 mm / A7      German ID card (until 31.10.2010)
- ID-3: 125 × 88 mm / B7      Passports, visas
- ID-000: 25 × 15 mm      SIM Cards
  - ISO/IEC 7810 Annexe B: As part of ID-1 size card

#### ISO/IEC 7816

Contact surfaces with an embedded chip - Smartcard

- ISO 7816-1: Physical characteristics
- ISO 7816-2: Dimensions and location of the contacts
- ISO 7816-3: Electronic signals and transmission protocols
- ISO 7816-4: Inter-industry commands for interchange
- ISO 7816-5: Numbering system and registration procedure for application identifiers
- ISO 7816-6: Inter-industry data elements for interchange
- ISO 7816-7: Inter-industry commands for Structured Card Query Language
- ISO 7816-8: Security related inter-industry commands
- ISO 7816-9: Enhanced inter-industry commands
- ISO 7816-10: Electronic signals and answer to reset for synchronous cards
- ISO 7816-11: Personal verification through biometric methods
- ISO 7816-12: Cards with contacts - USB electrical interface and operating procedures
- ISO 7816-13: Commands for application management in multi-application environment
- ISO 7816-15: Cryptographic information application

### §1.2 Contactless Cards

#### ISO/IEC 14443

Contactless integrated circuit(s) cards - Proximity cards

# eSanté

- Part 1: Physical characteristics
- Part 2: Radio frequency power and signal interface (type A + B)
- Part 3: Initialization and anti-collision
- Part 4: Transmission protocol

## ISO/IEC 15693

Contactless integrated circuit(s) cards - Vicinity cards

- Part 1: Physical characteristics
- Part 2: Air interface and initialisation
- Part 3: Protocols
- Part 4: Registration of applications/issuers

## §1.3 European Card Standards

### prCEN/TS 15480

Identification card system - European Citizen Card

- Part 1: Physical, electrical and transport protocol characteristics
- Part 2: Logical data structures and card services

### prEN 14890

Based on CWA 14890 E-SIGN-K

Application interface for smart cards used as secure signature creation devices

- Part 1: Basic Services
- Part 2: Additional Services

### CEN CWA 15264

- CWA 15264-1: Architecture for a European interoperable eID system within a smart card infrastructure
- CWA 15264-2: Best Practice Manual for card scheme operators exploiting a multi-application card scheme incorporating interoperable IAS services
- CWA 15264-3: User Requirements for a European interoperable eID system within a smartcard infrastructure

## §1.4 De-Facto Card Standards

### PC/SC

- Part 1: Introduction and Architecture Overview
- Part 2: Interface Requirements for Compatible IC Cards and Readers
- Part 3: Requirements for PC-Connected Interface Devices
- Part 4: IFD Design Considerations and Reference Design Information

# eSanté

- Part 5: ICC Resource Manager Definition
- Part 6: ICC Service Provider Interface Definition
- Part 7: Application Domain/Developer Design Considerations
- Part 8: Recommendations for ICC Security and Privacy Devices
- Part 9: IFDs with Extended Capabilities
- Part 10: IFDs with Secure Pin Entry Capabilities

## §1.5 Signatures

RFC 2315, 2630, 3369, 3852, 3370, 4853, 5083, 5754, 5652

Cryptographic Message Syntax, PKCS#7

RFC 2634, 5035

Enhanced Security Services for S/MIME

ETSI TS 101 733

Electronic Signature Formats

W3C XAdES, ETSI TS 101 903

XML Advanced Electronic Signatures

W3C XMLDSig

XML-Signature Syntax and Processing

## §1.6 Hardware Security Modules

FIPS 140-1, 140-2

Requirements for cryptography modules

The standard FIPS 140-2 defines four levels of security. All requirements of a lower level are part of the higher level<sup>1</sup>:

- Level 1: The lowest level with basic security requirements for the cryptographic module and no requirements concerning physical security.
- Level 2: Tamper-evidence including temper-evident coating or seals. Seals must be broken to get physical access to the cryptographic keys. Role based authentication of the operators against the module.
- Level 3: Prevention against intruders. Identity based authentication. Separation of security critical interfaces and others.
- Level 4: Physical protection mechanisms more complete. Resistant against environmental attacks (temperature fluctuations, voltage fluctuations).

---

<sup>1</sup> FIPS PUB 140-2, Security Requirements for Cryptographic Modules. Federal Information Processing Standards Publication, pp1-3, 2010-12-21. URL:<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>. Accessed: 2010-12-21. (Archived by WebCite at <http://www.webcitation.org/5v8prLRKf>)

# eSanté

## CEN CWA 14167

### Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures

- CWA 14167-1: System Security Requirements
- CWA 14167-2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)
- CWA 14167-3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)
- CWA 14167-4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP

## CEN CWA 14169

### Secure Signature-creation devices 'EAL 4+'

## §1.7 Access Control

### ISO/TS 22600

#### Privilege management and access control”

- ISO/TS 22600-1: Overview and policy management
- ISO/TS 22600-2: Formal models
- ISO/TS 22600-3: Implementations

### ISO/TS 21298

#### Structural and functional roles



## §2 European Parliament and Commission

### §2.1 EU Directive 2005/36/EC

Directive of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications. Section 32:

*"[...] The introduction, at European level, of professional cards by professional associations or organisations could facilitate the mobility of professionals, in particular by speeding up the exchange of information between the host Member State and the Member State of origin. This professional card should make it possible to monitor the career of professionals who establish themselves in various Member States. Such cards could contain information, in full respect of data protection provisions, on the professional's professional qualifications (university or institution attended, qualifications obtained, professional experience), his legal establishment, penalties received relating to his profession and the details of the relevant competent authority."*<sup>2</sup>

### §2.2 EU Parliament Resolution 2006/2275(INI)

European Parliament resolution on the impact and consequences of the exclusion of health services from the Directive on services in the internal market. Section 43:

*"[The parliament] [c]alls on the Commission to set up a system for collecting data and exchanging information between the various national authorities on health care providers, and to set up a European card to provide access to information on the skills of health care professionals and to make that information available to patients, as well as to develop a reliable health information system for service providers, with an obligation for national authorities to share that information;"*<sup>3</sup>

---

<sup>2</sup> Directive 2005/36/EC on the recognition of professional qualifications. European Parliament and Council. 2005-09-30. URL:<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:255:0022:0142:en:PDF>, L 255/26. Accessed: 2010-12-21. (Archived by WebCite at <http://www.webcitation.org/5v8pV2o5e>)

<sup>3</sup> Resolution on the impact and consequences of the exclusion of health services from the Directive on services in the internal market (2006/2275(INI)). European Parliament. 2017-05-23. URL:<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0201+0+DOC+XML+V0//EN>. Accessed: 2010-12-21. (Archived by WebCite at <http://www.webcitation.org/5v8rEfSxB>)

# eSanté

## §3 State of the Art of Exemplary Countries

This chapter describes the state of the art of exemplary countries. Some countries use a special Health Professional Card, others use the national e-ID and one country uses only login/password. The information is listed in different sections. Some are general and cover all types of identification method; others are only relevant for the Health Professional Cards or the national e-IDs.

### §3.1 General

#### Identification

This table shows the identification method for each country.

	Identification Method	Remark
France	Health Professional Card	Carte Professionnelle de Santé (CPS) including an identification number of the Health Professional
Slovenia	Health Professional Card	
Denmark	Login/Password Soft Certificate	The health professionals have to identify themselves via the public Danish e-Health portal sundhed.dk, which provides an access to Danish health care services. The digital signature is used for authentication in the portal.
Sweden	Health Professional Card National ID Card	The health professional can be identified by the SITHS Card (Secure IT for Healthcare Systems), card with the SIS label (Swedish ID card) usable everywhere (not only for healthcare).
Estonia	National ID Card	
Belgium	National ID Card	

#### Specialisations

The section gives information about the different types of specialisations, which are managed by the card or system.

France	The CPS is reserved to all physicians who are linked to the medical society e.g. physicians, dentists, midwives and pharmacists; and to the other health professionals like nurses, physiotherapists, chiropractors, speech therapists, orthoptists, ergotherapists, psychomotricians
Slovenia	<i>no information found</i>
Denmark	<i>no information found</i>
Sweden	All professions: Cards are given to healthcare providers and secretaries or sometimes people who work with healthcare providers.

# eSanté

## Applications

This section lists the main applications, for which the Health Professional has to authenticate himself.

France	Equipped with a card-to-card system the CPS will give access to the information in the VITALE card of the patient The CPS is used for authentication and for signing electronically
Slovenia	The card is used to access various databases and to access the identification data of patients on their insurance card
Denmark	The national digital signature infrastructure (based on PKI) is used for authentication in the portal
Sweden	The card is used for visual identification, electronic access, authentication, digital signature, and secure electronic exchanges

## Issuer

The following table lists the issuer of the card or the certificate.

France	The CPS is emitted by ASIP Santé. This group joins together the professional orders, professional associations, the hospitals, the state, the complementary insurances and the health insurance
Slovenia	The card is delivered by the Health Insurance Institute of Slovenia (HIIS)
Denmark	Certificates are issued by the Public Certificates for Electronic Services (OCES)
Sweden	The National Board of Health and Welfare deliver the Health Professional Card

## Supplier of Information

Issuing a card is only one part of the creation process of a card or certificate. This section now lists the institution, which is responsible for the correctness of the information provided in the card or certificate.

France	The card is emitted by ASIP Santé after agreement of the competent authorities (Medical Society, DDASS-Departmental direction of the sanitary and social Affairs, and CPAM-organism of Social Security) The DDASS guarantees the correctness of the stored information in the card.
Slovenia	The provided information is guaranteed by the HIIS.
Denmark	The provided information is guaranteed by the Public Certificates for Electronic Services (OCES)
Sweden	The provided information is guaranteed by the Certification Authority SITHS

# eSanté

## Management of Information

This section describes, how the information about the Health Professional is managed inside the infrastructure.

France	The Competent Authority collects the professional identification data; the health professionals receive an electronic certificate managed by the GIP, which correspond as an electronic identity paper. This certificate is published in a repertory and in the case of revocation; it is also indicated in the revocation lists.
Slovenia	Information is managed by the infrastructure of the nationwide health insurance card system that is connected to the HIIS
Denmark	<i>no information found</i>
Sweden	<i>no information found</i>

## §3.2 Special Health Professional Cards and Certificates

### Technical Specification

This section describes some technical details of existing Health Professional Cards

France	Microprocessor: Smart MX (NXp ex Philips) P5CD144 / 080 Dual: contact, contactless (RFID) Card: Oberthur ISO 7816 and EMV
Slovenia	Microprocessor: SAMSUNG S3CC91C Card: Gemalto, Personalisation centre -Cetis
Sweden	Two certificates: <ul style="list-style-type: none"> <li>• Personal certificate by Telia (a company of public Telecom) to sign e-documents</li> <li>• Professional certificate by SITHS, the certification Authority responsible for the technical infrastructure</li> </ul> Microprocessor: 32k SetCOS version 4.4.1, revision A2 by Gemalto

### Information Stored Inside the Card or Certificate

In case of customised Health Professional Cards the information that is stored inside the card is also be customised.

France	Social security serial number, first name, patronymic name, profession and speciality, modes and places of work, is activity sector, identification of place of work.  Identifiers card number: The RPPS (Répertoire Partagé des Professionnels de Santé) number has 11 digits. It is not significant and is attached to the person throughout his life
Slovenia	Identifiers card number (9 digits = 8 digit consecutive number + mod11 control

# eSanté

	number), serial number, first name, surname, profession, specialization, country code, number of the institute of public health, type of authorization  If a cardholder is not a physician, the professional card also contains the country code of the authorised legal entity, the number of the institute of public health of the authorized legal entity, and its title.
Denmark	<i>no information found</i>
Sweden	Identifiers card number (19 figure serial number, 4 digits = country, 4 digits = specified organisation, 3 digits = type of card. 8 digits = common serial number.  The professional certificate contains the profession, the first name, the surname, the id country council (SE-(order number 12 digits)-(serial number 4 digits)) and the email address. The storage syntax used is the X.509 standard with a subset of extensions for the public health care sector.

## Place of Work

Some countries store information the place of work inside the card.

France	The CPS contains the activity sector and identification of the place of work
Slovenia	The professional card contains the Institute of Public Health number of the authorized legal entity, and its title
Denmark	<i>no information found</i>
Sweden	<i>no information found</i>

## Processes in Case of Renewal / Loss / Defect

Which processes are established?

France	The keys of certificates are periodically renewed and also the keys for authentication and signing of the professionals are renewed at the same time with the card (the identity of the health professional is not re-checked)  The health professional has to complete a dedicated application form for the renewal  After a revocation, the attribution and the certification of new keys follow the procedure of the initial demand  In the case of loss, the professional has to inform the authority that gives the card, the GIP, and they will authenticate him by checking the proper information for his identification.
Slovenia	<i>no information found</i>
Denmark	OCES certificate can be renewed for four years at a time
Sweden	<i>no information found</i>

## §3.3 Citizen Cards or Unspecific Authentication and Signing Cards

These types of cards are not specific to Health Professionals. So a link between Health Professional and Card somehow must be established and managed.

# eSanté

## Linking Card with the Health Professional

This list shows, how the link between card and Health Professional is been established.

Estonia	Health professionals use an eID card as a health professional card. They have the same card like for the patients, and they use the same portal to connect and access to the health information system (DIGILUGU portal). Access via login/password.
Belgium	Health professionals don't have any professional card to identify themselves. Chambers deliver a certificate to prove their registration. Soon they are going to use their national electronic identity card as an Identification / authentication and signature tool for health professionals.

## Information about the Health Professional

This section shows which information is managed outside the card.

Estonia	<p>The health professional information is stored in a certificate. A web server certificate is used to prove the authentication of the user. The eID Estonian card is used as a primary domestic identification document. The health professional can also sign documents digitally with it. The information contained in it are the holder's surname, given names, sex, citizenship, date of birth, place of birth, personal code, photo, signature, date of issue and date of expiry, and document number.</p> <p>In the register for Estonian Health professionals you will have the following data: given name, family name, profession, date of registration, number of the order of the registration and his specialisations.</p>
Belgium	<p>The information is stored in the portal environment (<a href="https://www.ehealth.fgov.be">https://www.ehealth.fgov.be</a>). The eID card contains all identity data that is visible in printed form on the card plus the address of the cardholder. Additionally the card contains a certificate for authentication and a certificate for the signing of documents.</p>

## §4 European HPRO Card Initiative

This chapter gives an overview about the HPRO Card<sup>4</sup> initiative and the impact of this initiative for a Luxembourgish Health Professional Card and eHealth infrastructure. This section is mainly an extract of the original HPRO Card deliverables and therefore contains mainly citations.

### §4.1 Overview

*"The main objectives of the card will be to facilitate the free movement of health professionals in Europe while protecting patients from the small number of professionals that could be subject to severe disciplinary sanctions."*<sup>5</sup>

*"In order to advance in the harmonization, the main task of the HPRO Card project will be a study on the interoperability issues, on the usages of the card, on the authentication techniques of the health professional along with the building of the list of the competent authorities."*<sup>6</sup>

*"[...] [T]he [...] harmonized side [of the European health professional card] is European and clearly states the contact details of the competent authorities of the originator country."*

*"[...] [T]he [Health Professional] card will hold some information (on a microchip) which could be used to contact the database of the competent authority of the health professional originating country and to check immediately whether or not the professional is entitled to practice"*<sup>7</sup>

### §4.2 Use Cases

This chapter gives an overview about the use cases, which are foreseen for the HPRO Card.

#### Use case 1: Free Providing of Services

*"[...] [A] health professional wants to practice in another EU State Member for a temporary providing of services"*<sup>8</sup>

#### Use case 2: Access to Medical Data Abroad

*"[...] [A] health professional has to access medical data of a foreign patient in the patient's country of origin"*<sup>9</sup>

#### Use Case 3: Usage Of a Professional Identity Card

*"[...] [A] health professional wants to be recognized as a health professional in another country"*

---

<sup>4</sup> HPRO Card: <http://www.hprocard.eu/> (accessed 07.09.2010, archived by WebCite at <http://www.webcitation.org/5sYvVER7p>)

<sup>5</sup> HPRO Card - Description: <http://www.hprocard.eu/en/description/description.html> (accessed 07.09.2010, archived by WebCite at <http://www.webcitation.org/5sYwoYEnP>)

<sup>6</sup> HPRO Card: <http://www.hprocard.eu/>

<sup>7</sup> HPRO Card - Description: <http://www.hprocard.eu/en/description/description>.

<sup>8</sup> HPRO Card: Workpackage 4 - The Interoperability of different health professionals' authentication systems - Deliverable 6 - Report concerning the convergence and interoperability of existing health professional smart cards: <http://www.hprocard.eu/images/20091015-hpc-wp4-deliverable6.pdf>, pp18, 28 (accessed 07.09.2010, archived by WebCite at <http://www.webcitation.org/5sZ6myBcY>)

<sup>9</sup> HPRO Card: Workpackage 4 - The Interoperability of different health professionals' authentication systems - Deliverable 8 - Report on qualified interoperability scenarii: <http://www.hprocard.eu/images/20091015-hpc-wp4-deliverable6.pdf>, pp19, 25ff (accessed 07.09.2010, archived by WebCite at <http://www.webcitation.org/5sZ7n9NGa>)

# eSanté

## §4.3 Functions

This chapter describes the functions of the card and how it is been used to manage the use cases.

*"The functional system of the project should allow for the implementation of [four] major functions:*

- *Identification [and] authentication of the person who is logging on with their card*
- *Validation of the credentials stored on the card*
- *Management of the authorization of access to applications*
- *Connexion with the application."*<sup>10</sup>

### §4.3a Identification and Authentication

*"This involves a function that allows you to ensure that the person who is connecting to the system truly is who they say they are.*

*The target system works using a strong authentication ensured by the presentation of a healthcare professional smart card (HPRO Card). Typing in a PIN code completes the presentation of the card. These two factors ensure strong authentication of a healthcare professional.*

*The function uses the authentication credentials stored on the card.*

*The system should also work for healthcare professionals from countries where they are not issued with smart cards. In this case, entering a username / password is an alternative solution. However this is no longer a strong authentication"*<sup>11</sup>

### §4.3b Validation of the Credentials Stored on the Card

*"This involves a validation of the credentials stored on the card and used for authentication. This function is no use in the case of authentication using username / password.*

*The function includes checking that the credential does not appear on the revocation list managed by the [...] Manager [of the Public Key Infrastructure (PKI)].*

*This function therefore requires access to a "technical" party, the manager of the [certificate] revocation list [(CRL)] that corresponds to the card [...].*

*In order to ensure this function, it is therefore necessary to have [the certificate revocation] list available [...]."*<sup>12</sup>

### §4.3c Management of the Authorization of Access to Applications

*"This function requires the prior implementation of two sub-functions:*

---

<sup>10</sup> HPRO Card: Workpackage 3 - Conditions for the implementation of strong authentication of health professionals - Deliverable 4 - Proposal for adapted architectures that integrate the conditions of confidentiality of personal information exchanges: <http://www.hprocard.eu/images/20091012-hpc-wp3-deliverable4.pdf>, chapter 4, pp 20 (accessed 07.09.2010, archived by WebCite at <http://www.webcitation.org/5sZ8qsNuQ>)

<sup>11</sup> HPRO Card: Workpackage 3 - Conditions for the implementation of strong authentication of health professionals - Deliverable 4 - Proposal for adapted architectures that integrate the conditions of confidentiality of personal information exchanges: chapter 4.1.1, pp 20

<sup>12</sup> HPRO Card: Workpackage 3 - Conditions for the implementation of strong authentication of health professionals - Deliverable 4 - Proposal for adapted architectures that integrate the conditions of confidentiality of personal information exchanges: chapter 4.1.2, pp 20

# eSanté

- *Management of the levels of credentials stored on each card in each country. This information enables the management of an equivalence database for the credentials on different cards.*
- *Management of a list of strong authentication user applications with the following access conditions for each of them: level of credential, profile of the user which could include the following items: level of security for the credential, profession of [the cardholder], country of origin, etc.*

*These two sub-functions are work of a 'professional' nature. They can only be carried out at a European level by an organization that would be able to understand the equivalence between the levels of security required by national security policies, those of the applications and the level shown by each credential stored on the card.*

*To date, this type of organization does not exist.*<sup>13</sup>

## §4.3d Connexion with Applications

*"In a proactive way (the moment [when the] access to an application is requested), the equivalence databases mentioned above, ensure the following for each individual requesting access to an application:*

- *Verification that the credential produced to access an application corresponds to the security policy for this application*
- *The production of a security token, which represents all of the verification mechanisms and assure the user applications that they have been carried out successfully.*

*To date, this type of management does not exist in the member states of the European Union. It is therefore an activity that needs to be set up.*<sup>14</sup>

## §4.3e Mutualisation of the Functions

*"We assume that the various functions described above could be mutualised. Mutualisation is necessary due to the complexity of the management of the functions described above for one application in particular (that of a relevant authority who wishes to make their information available via the internet for example). [...]"*

### [Scenario 1]

*[This] scenario takes in account the total mutualisation: one solitary part is realising all the functions. So the scenario could have two hypotheses:*

- *A first one, which places one party at a European level*
- *The second one, which places one party per country; in each country the party will realise the same tasks*

---

<sup>13</sup> HPRO Card: Workpackage 3 - Conditions for the implementation of strong authentication of health professionals - Deliverable 4 - Proposal for adapted architectures that integrate the conditions of confidentiality of personal information exchanges: chapter 4.1.3, pp 20-21

<sup>14</sup> HPRO Card: Workpackage 3 - Conditions for the implementation of strong authentication of health professionals - Deliverable 4 - Proposal for adapted architectures that integrate the conditions of confidentiality of personal information exchanges: chapter 4.1.3, pp 20-21

# eSanté

## [Scenario 2]

*[This] scenario could be to consider the possibility to share the tasks of assuring the functions. [It] is based on the conclusions linked to the first scenario. It could have also two hypotheses:*

- *A first one, which previews a dialog between the HPROCard servers in each country*
- *The second one, which previews the use of a single server of HPROCard<sup>15</sup>*

## §4.4 Impact for the Development of a Luxembourgish Health Professional Card

### §4.4a Layout of the Card

There is no specification for the national side of the HPRO Card. All countries can keep their own national side graphic but it has to show "at least

- *the name and surname,*
- *the professional identifier,*
- *the date of the card validity,*
- *an hologram (covering the personalized data),*
- *[and optional a photo]<sup>16</sup>.*

The HPRO Card consortium recommends a graphical layout for the European side of the card, which can be requested from the HPRO Card project coordinator.

### §4.4b Technical Specifications

Following the existing health professionals' certification authorities, the technical recommendations provided by the HPROCard workgroup are:

- *"X509 Electronic certificates,*
- *Chip cards,*
- *Standard API to dialog with the card [...]*
- *Respect of the Common Criteria certification*

*[...] In order to work together with a host computer, smart cards require an additional device that provides an electrical interface for data exchange, a so-called smart card reader. They nowadays can be found built into an increasing number of desktop computers. This makes smart card services available to the full range of PC and Web/Internet applications and lets them play a major role for access control on the Internet."<sup>17</sup>*

---

<sup>15</sup> HPRO Card: Workpackage 3 - Conditions for the implementation of strong authentication of health professionals - Deliverable 4 - Proposal for adapted architectures that integrate the conditions of confidentiality of personal information exchanges: chapter 4.2, pp 21

<sup>16</sup> HPRO Card: Workpackage 4 - The Interoperability of different health professionals' authentication systems - Deliverable 6 - Report concerning the convergence and interoperability of existing health professional smart cards, chapter 3.5.1, p 22

<sup>17</sup> HPRO Card: Workpackage 4 - The Interoperability of different health professionals' authentication systems - Deliverable 6 - Report concerning the convergence and interoperability of existing health professional smart cards, chapter 3.5.3, p 25

# eSanté

For the demonstrator, an SDK from the Open Limit Company was used to access the different health professional card types of France, the Netherlands, and Germany.<sup>18</sup>

Some open questions are still in discussion and are addressed to further work group and normalisation activities:

- *"The health professional card interoperability mechanisms are being integrated in ISO Standards*
- *The interoperability is achieved with:*
  1. *A common set of health professional card commands and data structures specified,*
  2. *A middleware which makes any health professional card look the same for the external world,*
  3. *The definition of health professional card profiles.*
- *The interoperability is based on Middleware / Open Interfaces*
- *The health professional card security policy is compliant with EU Directive on Electronic Signature.*
- *The health professional card security policy is based on the targets of the ECC (European Citizen Card)."*<sup>19</sup>

## §4.5 Impact for the Development of a Luxembourgish eHealth Infrastructure

### §4.5a Necessary Systems

A repository that contains data on health professionals is needed, containing data that are useful for the registration and identification. Additionally a security directory is required, which is used for the strong authentication process and the electronic certificates revocation lists control.

### §4.5b Organisational Recommendations

*"The services that have to be implemented in the same time than the production of the cards itself:*

- *Exchanges and common projects involving the different institutions those refer to health professionals' information (Chambers, Ministry, Health Insurance, etc.)*
- *Databases synchronization between the different levels (local, regional and national) and between the different information systems regarding health professionals' data.*
- *Writing and publishing of a certification policy,*
- *Card lifecycle management (what did happen when the health professional is losing his card or when it doesn't work?),*
- *Assistance and hotline for users and for computer services companies that have to integrate the health professionals' authentication or signature techniques. [...]*

*These services can be provided by the different component of the health information system."*<sup>20</sup>

<sup>18</sup> HPRO Card: Workpackage 4 - The Interoperability of different health professionals' authentication systems - Deliverable 6 - Report concerning the convergence and interoperability of existing health professional smart cards, chapter 4.1, p 28-29

<sup>19</sup> HPRO Card: Workpackage 4 - The Interoperability of different health professionals' authentication systems - Deliverable 6 - Report concerning the convergence and interoperability of existing health professional smart cards, chapter 3.5.3, p 25



## §5 Studies of STORK

In the European Initiatives, several work packages of STORK (Secure Identity Across Borders Linked)<sup>21</sup> also deal with the analyses of state of the art initiatives and technologies.

An entire copy of the results is not useful, as it would go beyond the scope of this document, but some results and conclusions are worth to be cited. For further information, please take a look at the original sources.

### §5.1 European Citizen Cards

*"The European Citizen Card (ECC) is a smart card issued under the authority of a government institution or an entitled private organisation, either national or local, which carries credentials in order to provide all or parts of the following services:*

1. *Verify the identity;*
2. *Act as an Inter-European Union travel document;*
3. *Facilitate logical access to e-government or local administrative services."*<sup>22</sup>

*"The technical specification (CEN/TS 15480 - Identification card systems - European Citizen Card) consists of a set of four documents describing specifications reaching from smart card characteristics to operational profiles. The technical specification, developed by the CEN/TC 224 WG15, consists of the following four parts:*

- *[ECC] Part 1: Physical, electrical and transport protocol characteristics*
- *[ECC] Part 2: Logical data structures and card services*
- *[ECC] Part 3: European Citizen Card Interoperability using an application interface*
- *[ECC] Part 4: Recommendations for European Citizen Card issuance, operation and use*

*[...] ECC part 3 [...] provides technical specifications for a middleware- architecture. This middleware provides an application interface - called the Service Access Interface - which is based on ISO/IEC 24727-3.*

*[...] [F]uture eID smart cards should consider compliance with the ECC specifications regarding the physical, electrical, transport protocol characteristics (part 1) and perhaps also with the specified logical data structures (part 2). This would certainly ease the development of applications supporting cards from various Member States. Furthermore, to provide a unified smart card access the interoperability processes and functionalities defined in the ECC specifications (part 3) should be also considered for future eID applications."*<sup>23</sup>

---

<sup>20</sup> HPRO Card: Workpackage 4 - The Interoperability of different health professionals' authentication systems - Deliverable 6 - Report concerning the convergence and interoperability of existing health professional smart cards, chapter 3.6, pp 26

<sup>21</sup> STORK, URL: <https://www.eid-stork.eu/>

<sup>22</sup> Mivkovic, M. Preliteiro. STORK Work Item 3.2.3 - European Citizen Card, chapter 2, p 5. 2010-04-14. URL:[https://www.eid-stork.eu/index.php?option=com\\_processes&Itemid=&act=streamDocument&did=1211](https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1211). Accessed: 2011-01-11. (Archived by WebCite at <http://www.webcitation.org/5vf1rxgl6>)

<sup>23</sup> M. Ivkovic, M. Preliteiro, STORK Work Item 3.2.3 - European Citizen Card, chapter 5, p22

# eSanté

*"The German eCard-API-Framework is an example for a national open specification offering a set of simple and platform-independent interfaces. These interfaces standardise the communication between applications and chip cards being used.*

*The goal of the eCard-API-Framework is to provide a simple and uniform interface which should ease the access to different available chip cards. [...] [The framework] consists of four different layers: Application Layer, Identity Layer, Service Access Layer and Terminal Layer. [...]*

*The Service Access Layer primarily offers functions for cryptographic primitives and biometric mechanisms in correspondence with cryptographic tokens. This layer contains the ISO24727-3 interface and a support interface [and is therefore closely related to the ECC]."<sup>24</sup>*

## §5.2 Mobile Electronic Identity

*"There are various technical and organisational approaches for how mobile devices may serve as means for authentication. A common approach is the use of special SIM cards with PKI functionality that securely store private keys and certificates. This solution includes "secure elements" (SE) on the SIM card. These secure elements enable the SIM card's owner to carry out signatures "on-board" the mobile device by using the SIM card as cryptographic device, the handset for PIN entry and the mobile operator's network as backchannel.*

*Other approaches involve other types of mobile devices, like PDAs or security tokens. Also concepts with (Web-)server-based secure elements where mobile devices act as additional authentication factor are conceivable and actually have been deployed in e-government environments. The communication between the authentication device and the relying party may not only be established by using the operator's network, it may also be performed via WiFi, NFC, RFID or Bluetooth."<sup>25</sup>*

*"[...] Electronic Identity' is defined as [...] a collection of identity attributes in an electronic form. These attributes specify characteristics, like a name, a membership, a role or any other information suitable to uniquely identify a person or a thing.*

*The term 'mobile electronic identity' implies these electronic identities to be portable. This involves device and user mobility, meaning that the service can be accessed with a device while moving as well as that a service can be used independently from device and location [...]. [...]*

*[The study] focus[es] on usage of mobile eID with the need stationary devices or specific installations. [...] [T]here are typical types of mobile eIDs that can be distinguished[.]"<sup>26</sup>*

- Cell Phones
- Mobile Tokens / Hardware Tokens: disconnected, connected, contactless
- PDAs

<sup>24</sup> M. Ivkovic, M. Preliteiro, STORK Work Item 3.2.3 - European Citizen Card, chapter 3, pp9-10

<sup>25</sup> M. Ivkovic, U. Keskel, T. Knall, H. Leitold, T. Martens. STORK Work Item 3.3.6 - Mobile eID. chapter 1.1, p5, 2010-04-14. URL: [https://www.eid-stork.eu/index.php?option=com\\_processes&Itemid=&act=streamDocument&did=1215](https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1215). Accessed: 2011-01-11. (Archived by WebCite at <http://www.webcitation.org/5vf2BsyD8>)

<sup>26</sup> M. Ivkovic, U. Keskel, T. Knall, H. Leitold, T. Martens, STORK Work Item 3.3.6 - Mobile eID, chapter 1.3, p6

# eSanté

## §5.2a Cell Phones

*"A secure approach for the realization of mobile electronic identification is to perform digital signature directly on the phone, using built-in secure elements, secure elements on special SIM cards or secure elements implemented on external hardware plugged in the handset.*

*The private key needed to conduct signatures is securely stored within the secure elements. Its usage is protected by a PIN known only to the holder of the phone so that the holder has the exclusive control over her/his credentials. The result of a digital signature is usually transferred to a communication partner, either using a GSM channel or some other communication technology like RFID, NFC or Bluetooth."*<sup>27</sup> This is a list of exemplary implementations:

### Subscriber Identity Module (SIM)

*"Each subscriber is uniquely linked to the SIM which stores the user's private key needed for authentication based on signatures in tamperproof manner.*

*A SIM card in a phone can be regarded as a smart card fully integrated with reader and display in combination with networking functions.*

*In order to conduct authentication against a service provider by creating a signature a connection between SIM card and a background system, mostly maintained by the mobile phone operator, has to be established. This can be done by a so called 'Over the Air (OTA)' communication [...] allowing the operator to communicate with, download applications to, and manage SIM cards by sending special messages without being physically connected to the card. [If] the network operator [...] wants to execute a certain kind of operation on a client's SIM [it] sends a request to his OTA gateway, which then transforms the abstract request into special short messages (SMS). In order to comply this task the gateway maintains a database containing information on the specific subscriber's SIM. Bases upon this information the gateway formats the message according to the specific type of SIM. This message is sent to a SMS gateway which finally delivers it to the subscriber's SIM. [...]*

*The user's PKI enabled SIM card recognizes the special short message, optionally shows the user a kind of verification code for the text to be signed [...] and waits until the user confirms the signature by entering the appropriate PIN code. The result of the signature is sent back to the mobile phone network operator in the first place. As final step the mobile operator transmits the signature to the service provider who in turn may conduct a signature verification and a certificate validation."*<sup>28</sup>

### WAP Identity Module (WIM)

*"One of [the WAP (Wireless Application Protocol)] specifications describes a security module named "WAP Identity Module (WIM)".*

*This specification covers two possible types:*

- *WIM as a separate application on an additional chip card. This type requires an additional second Dual-SIM-Slot, which did not become widely accepted*
- *WIM as additional application on a SIM-, USIM9- or UICC10 card*

<sup>27</sup> M. Ivkovic, U. Keskel, T. Knall, H. Leitold, T. Martens, STORK Work Item 3.3.6 - Mobile eID, chapter 3.1, p13ff

<sup>28</sup> M. Ivkovic, U. Keskel, T. Knall, H. Leitold, T. Martens, STORK Work Item 3.3.6 - Mobile eID, chapter 3.1, pp13-14

# eSanté

*The specification of WIM is based on the cryptographic token information format standard (PKCS#15). Although the main task of the WIM is the cryptographic protection of a WAP data connection it can also be used for authentication purposes based on electronic signatures."*<sup>29</sup>

## Micro SD Card

*"Independently of each other Giesecke & Devrient [(G&D)] and certgate developed a mobile eID solution which can be used to upgrade cell phones with mobile eID and mobile signature capabilities. Both implementations are natively based on the microSD-Interface [...].*

*[...] [The G&D Java based module is] equipped with a secure element providing smart card functionality like PKI key management or on-board key generation. [...] The [certgate] module [...] provides digital signature, RSA encryption, the generation of random numbers, initialization with certificates and keys and finally on-board key generation."*<sup>30</sup>

Both modules are certified Common Criteria EAL 5+ and might be used with the commonly used mobile operating systems.

## Server Side Authentication

*"The idea of a server based eID solution is that no electronic signatures have to be carried out on the phone itself. The cell phone solely acts as [a] second authentication channel (receiving TANs via SMS) enhancing the security. While common authentication procedures only involve the 'knowledge' of credentials, the cell phone as second authentication channel additionally requires its 'possession' [...].*

*The advantage of this solution is that there are no special requirements regarding the phone, except the fact that a working SIM card is required and that the phone has to be capable of receiving SMS."*<sup>31</sup>

## §5.2b Mobile Tokens / Hardware Tokens

*"The idea [behind the use of chip cards for authentication] is that the particular software needed for the authentication at a certain service provider can be automatically downloaded as Java applet or ActiveX component by the user's browser [...]. [This software has] access to local resources [and] allow[s the] use the card reader for instance. The user who is willing to perform authentication against a web[-]portal [...] does not have to install a proprietary piece of software which makes the drafted solution 'mobile' to a certain extend.*

*[...] [T]he advantage is that software updates can be easily done by updating the component on the server since the particular piece of software is downloaded by the user's browser anyway."*<sup>32</sup>

As an alternative USB-based tokens may be used. *"The operating system recognizes the token and starts the software stored in the flash memory. [...]. As an enhanced alternative there are also tokens on the market that provide small keypads to allow entry of a PIN or tokens that protect stored private keys with biometry like fingerprints.*

<sup>29</sup> M. Ivkovic, U. Keskel, T. Knall, H. Leitold, T. Martens, STORK Work Item 3.3.6 - Mobile eID, chapter 3.1, p14

<sup>30</sup> M. Ivkovic, U. Keskel, T. Knall, H. Leitold, T. Martens, STORK Work Item 3.3.6 - Mobile eID, chapter 3.1, p14

<sup>31</sup> M. Ivkovic, U. Keskel, T. Knall, H. Leitold, T. Martens, STORK Work Item 3.3.6 - Mobile eID, chapter 3.1, pp15-16

<sup>32</sup> M. Ivkovic, U. Keskel, T. Knall, H. Leitold, T. Martens, STORK Work Item 3.3.6 - Mobile eID, chapter 3.2, pp16-17

# eSanté

*Apart from [that] there are also tokens with built-in secure elements that provide secure on-board generation of private keys, enabling secure digital signatures as well as user authentication.*"<sup>33</sup>

## §5.2c PDAs

*"Since PDAs are just normal computers they are prone to the same attacks and dangers just normal computers are. The provision of a safe environment for mobile eIDs may become questionable considering a software[-]based solution where an electronic signature needed for authentication is carried out by the on-board software.*

*[...] [T]he combined usage of smart card technology [...] or [the] (micro)SD card [solutions may be an acceptable compromise]. The generation of the private keys as well as the conductance of the signature itself has to be done by secure elements.*"<sup>34</sup>

## §5.3 RFID & NFC

*"In the last decade radio frequency identification (RFID) has become a widespread technology in various fields. RFID systems are used to identify persons, objects or animals in different contexts. The device attached to the object to be identified is called contactless transponder (or tag). As its name implies, RFID uses radio waves to exchange information. A typical RFID system consists of a reader and one or more contactless transponders. The complexity of the transponders used strongly depends on the field of application. In a tracking process of a good, a simple tracking number stored in the tag might be sufficient to stay informed about the position of the object in transfer. A security critical identification device, like a passport, probably needs to provide more information.*

*RFID systems are classified in several categories depending on different features. The features used to differentiate one RFID system from another one are: operating frequency, type of coupling between the reader and the tag, maximum range of operation, a.s.o. [The focus lies] on RFID systems complying with the ISO/IEC 14443 standard. Such systems consist of a reader, called proximity coupling device (PCD) and a contactless smart card, called proximity integrated circuit card (PICC). The reader and card are inductively coupled over an electromagnetic field that operates at a frequency of 13.56 MHz and is provided by the reader. The card is sometimes referred to as passive transponder. A passive transponder does not have an internal power supply. The reader's electromagnetic field is used to supply the card with power. Due to the passive concept, the maximum operating range is limited to ≈10 cm. Currently, the maximum bit rate defined by the standard is 848 kbit/s.*"<sup>35</sup>

### §5.3a Components of an RFID System

*"A typical RFID system [...] always consists of two components:*

- 1. a transponder, that is attached to the objects to be identified, and*
- 2. a transceiver or reader, depending on whether it is capable of writing and reading or just reading [...].*

<sup>33</sup> M. Ivkovic, U. Keskel, T. Knall, H. Leitold, T. Martens, STORK Work Item 3.3.6 - Mobile eID, chapter 3.4, pp17-18

<sup>34</sup> M. Ivkovic, U. Keskel, T. Knall, H. Leitold, T. Martens, STORK Work Item 3.3.6 - Mobile eID, chapter 3.3, p17

<sup>35</sup> M. Ivkovic, J. Haid. STORK Work Item 3.3.3 - RFID & NFC. STORK. 2010-12-09. chapter3, p3, URL:[https://www.eid-stork.eu/index.php?option=com\\_processes&Itemid=&act=streamDocument&did=1382](https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1382). Accessed: 2011-01-12. (Archived by WebCite at <http://www.webcitation.org/5vg5u5Jjn>)

# eSanté

*During normal operation, the reader represents the master and the transponder the slave (the reader controls the communication process and therefore the transponder). A reader has some kind of radio frequency module to interact with the contactless chip card. [...]*

*The transponder consists of a coupling device (e.g. an antenna) and a microchip containing the data. Depending on the structure of the transponder, it might have no internal power supply. Such transponders are called passive transponders. Passive transponders use the electromagnetic field emitted by the reader for both, to exchange information and supply the integrated circuit with power."<sup>36</sup>*

## §5.3b Classification of RFID Systems

*"There is a multitude of RFID systems on the market. To differentiate one system from the other, features have to be defined to classify the different systems. The most common features used are: transponder construction form, operating frequency, maximum possible range, type of coupling and internal structure of the transponder.[...]"<sup>37</sup>*

## §5.3c Transponder Construction Forms

*"RFID transponders are available in various kinds of forms. Depending on the field of application tags can be made of different materials and in different shapes. The tags can be as small as a few millimeters or as big as 10 cm. [...] The main focus [...] will be the ID-1 format, also called contactless smartcards. This format has the same dimensions as a standard check card [...] and is widely used in payment and access control systems."<sup>38</sup>*

## §5.3d Range, Frequency and Coupling

*"The range between reader and transponder, the operating frequency of the used field and the type of coupling are important features in RFID systems. The maximum possible range determines the maximum distance between the reader and transponder with a communication still possible. This distance ranges from < 1 cm to 15 m. [...]. Depending on the range and frequency electric, magnetic or electromagnetic coupling is used. Depending on the maximum range RFID systems are divided into three groups [...].*

1. *Close-coupling-systems are limited to a range of less than one centimeter. In order to get a working setup the transponder has to be inserted into the reader or exactly positioned on its surface. The coupling used can either be electric or magnetic. [...] Nowadays this kind of systems are getting less and less important.*
2. *Remote-coupling-systems are systems with a maximum range of up to 1 m. Nearly all of those kind of systems use inductive (magnetic) coupling. Nearly 90% of all RFID systems sold belong to that category: proximity-coupling-systems (ISO 14443, contactless chip cards) and vicinity-coupling-systems (ISO 15693, smart labels and contactless chip cards) are two of them. [...]*
3. *Long-range-systems are those systems with ranges greater than 1 m. The operating frequency is located in the ultrahigh frequency (UHF) or microwave band. On account of their physical principal of operation the majority of these systems is called backscatter*

<sup>36</sup> M. Ivkovic, J. Haid, STORK Work Item 3.3.3 - RFID & NFC, chapter 3.1, pp9-10

<sup>37</sup> M. Ivkovic, J. Haid, STORK Work Item 3.3.3 - RFID & NFC, chapter 3.2, p10

<sup>38</sup> M. Ivkovic, J. Haid, STORK Work Item 3.3.3 - RFID & NFC, chapter 3.3, p10

# eSanté

*systems. Backscatter-systems do not have an actual transmitter, but they reflect the received waveform in different ways to communicate with the interrogator. The powering of those systems can either be passive (by the received field) or active (with an internal battery)."*<sup>39</sup>

## §5.3e Internal Structure of Transponders

*"The internal structure of transponders is another important feature to classify RFID systems. [D]epending on the way of data processing and the size of data memory implemented, three main groups are distinguished:*

1. *Low-end systems*
2. *Mid-range systems and*
3. *High-end systems [...]*

*Low-end systems have the simplest possible internal structure. The memory's size is limited to a few bytes and its content cannot be altered (read-only). The functionality provided by those transponders is highly restricted as well. One example of that group are EAS (Electronic Article Surveillance) [which] can only be used to determine whether an object is present in the interrogation zone of the reader or not. Another example are so-called read-only transponders. Every transponder has an (unique) identification number that is continuously transmitted by the transponder as soon as it is powered up. Due to the fact, that no anticollision procedures are implemented, it has to be ensured, that only one transponder is active at a time [...]. []*

*Transponders with increased functionality and memory size are classified as mid-range systems. The internal memory can be read and written and its size ranges from a few bytes to several 100 [K]bytes. A built-in state machine can process simple commands sent by the reader (e.g. addressing memory). To allow multiple transponders in the interrogation field of the reader, anticollision algorithms are implemented. For security critical applications even cryptographic algorithms (e.g. authentication) and data encryption can be implemented.*

*High-end systems provide the biggest memory sizes, combined with the greatest functionality. The transponders consist of a microprocessor and memory. Such transponders are often referred to as contactless smartcards due to their build-in intelligence. The flexibility of these transponders is further increased by a smartcard operating system. The use of an operating system allows to easily expanding the functionality of the smartcard. If computationally intensive cryptographic algorithms need to be used, coprocessors are added to perform this task. Such smartcards are used in ticketing applications, personal identification and as electronic purse. The standard describing the communication in those systems is ISO 14443."*<sup>40</sup>

## §5.3f State-of-the-Art Contactless Smart Cards

*"Contactless smart cards execute a more or less complex code, including security-relevant operations. A appropriate hardware is the prerequisite to perform the application according to the specifications. Basically the requirements can be split into the following categories*

- *A CPU (central processing unit) which executes the program. In most cases an 8 or 16-bit CPU is used.*

<sup>39</sup> M. Ivkovic, J. Haid, STORK Work Item 3.3.3 - RFID & NFC, chapter 3.4, pp10-11

<sup>40</sup> M. Ivkovic, J. Haid, STORK Work Item 3.3.3 - RFID & NFC, chapter 3.5, pp11-12

# eSanté

- *Volatile and non-volatile memories to store program code, data, and intermediate values of the application executed on the card.*
- *Cryptographic co-processors to accelerate security algorithms used in all contactless protocols and applications, e.g. AES (Advanced Encryption Standard) or ECC (Elliptic Curve)*
- *Contactless interface for communicating with the reader. Smart card controllers for the applications described in this study offer ISO/IEC 14443 Type A and/or Type B. The maximum speed depends on the application and ranges from 106kBit/s up to 848kBit/s."*<sup>41</sup>

## §5.3g Security

*"System based on contactless technology must cover the basic security properties which are privacy, authenticity and integrity. Therefore the systems must implement countermeasures for the wide range of known attacks, [like Sniffing, Unauthorized change of data, Man-in-the-middle, and Eavesdropping/skimming]. [...]*

*The security of a contactless system depends on the smart card controller hardware as well as on the protocols executed on it. [...]*

*Contactless smart cards, in general, provide the same security hardware than implemented on the wired cards. This includes digital countermeasures, memory firewalls, and sensors. There is a strong trend in the industry to remove sensors and instead apply digital security mechanisms, such as memory encryption, checksums, and redundancy.[...]*

*Security mechanisms are available and standardized for wired smart cards and described in ISO/IEC 7816 standards. These mechanisms include secure messaging, cryptographic tokens, and a architecture defining access rights to files and data in the card.*

*Additional security schemes are defined for specific applications. [This is an] overview of countermeasures on protocol level defined for electronic passports[:]*

- *Eavesdropping[:]* *Secure Messaging[.] A Triple DES encryption is performed on the data sent over the contactless interface.*
- *Unauthorized read-out of (less-sensitive) personal and biometric data (facial image)[:]* *Basic Access Control (BAC)[.] key for communication is based upon optical data printed inside the passport (MRZ).*
- *Unauthorized read-out of sensitive biometric data (fingerprint)[:]* *Terminal Authentication (TA)[.] the chip verifies that the terminal is authorized to read out sensitive data. Scheme based on asymmetric cryptography.*
- *Forgery of e-Passport data [.] Create and personalize arbitrary dataset [:]* *Passive Authentication (PA)[.] A digital signature is created covering the entire data written to the e-Passport. Only the owner of the official private key can create this signature. This can be verified using asymmetric cryptography.*
- *Replacement of chip, copy of read dataset[:]* *Chip Authentication (CA)[.] the scheme checks the origin of the chip keys. Asymmetric cryptography is used to verify the corresponding signature"*<sup>42</sup>

<sup>41</sup> M. Ivkovic, J. Haid, STORK Work Item 3.3.3 - RFID & NFC, chapter 4, p14

<sup>42</sup> M. Ivkovic, J. Haid, STORK Work Item 3.3.3 - RFID & NFC, chapter 5, pp17-18

# eSanté

## §5.3h Identification Applications

*With the introduction of electronic passport a major step was done to extend the use of contactless controllers for governmental purposes. Smart card controllers are not only used in electronic passports, but also in health insurance cards, driving licenses and ID cards. These electronic documents use smart card controllers which are inserted into the inlays, e.g. front or back cover of the document. [...]*

*Since the introduction of the ePassport two authentication schemes are used:*

- *BAC (Basic Authentication Control): The contactless chip on a BAC passport contains the passport data plus a facial image, with a digital signature to detect modifications. All this data remains static, unchanged from inspection to inspection.*
- *EAC (Extended Authentication Control): An extension of the BAC protocol is the EAC. It consist[s] of additional functionality to check the authenticity of both the chip (chip authentication) and the reader (terminal authentication). The cryptographic algorithms used are stronger than for BAC. [...]*

*The BAC scheme implements an authentication mechanism to protect basic identification (facial image) and personal data in the MRZ. It is based on optical information printed on passport; hence no infrastructure is needed to perform the protocol. It is intended to prevent skimming (reading out of information via contactless information without consent of passport holder) and eavesdropping (no plain information is sent over the contactless interface). The key for communication is derived from the printed [Machine Readable Zone]: passport serial number, date of birth, expiry date. Note that the [Machine Readable Zone] is only readable if the passport booklet is opened. Obviously the BAC scheme implies that the data stream from the ePassport remains the same each time it is read out.*

*The EAC scheme uses asymmetric cryptography to verify the reader against the card and vice versa. Furthermore at each read out of the passport a new session is generated which results in a different encryption of the contactless communication channel.*

*In more detail, the asymmetric protocol was defined to protect sensitive data, such as digital fingerprints. Therefore two components are defined: Chip authentication (CA) and Terminal authentication (TA). The CA is used to check whether the chip is authentic and was personalized by an approved issuer. This is done by verifying the signature of the issuer. In the TA procedure the card checks whether the terminal has the appropriate access rights to read out sensitive data.*

*The algorithms used for chip authentication are based on elliptic curves Diffie-Hellman key agreement (ECDH) or RSA key agreement (DH). For terminal authentication ECDSA or RSA based mechanisms are used. Furthermore on-chip asymmetric cryptographic computations needed which are based on elliptic curves (ECC) and / or RSA."<sup>43</sup>*

## §5.3i Near Field Communication (NFC)

*"NFC (near-field communication) was initiated 2004 to provide a short range wireless link on a mobile device. Basically, mobile devices - equipped with NFC interface - can read ISO 14443-compliant cards. Furthermore, the mobile device itself can behave like a contactless card."<sup>44</sup>*

<sup>43</sup> M. Ivkovic, J. Haid, STORK Work Item 3.3.3 - RFID & NFC, chapter 6.3, pp21-22

<sup>44</sup> M. Ivkovic, J. Haid, STORK Work Item 3.3.3 - RFID & NFC, chapter 6.4, pp22



## §5.4 Trust Federation and Identity Frameworks

### §5.4a Shibboleth

*"Shibboleth is an open source framework based on open standards like SAML that allows federated identity-based authentication and authorization between organisations using different infrastructures and methods for authentication. A great importance was attached to the design of its architecture in order to create a stable, flexible and enduring framework.*

*Usually users do not exclusively access services within their organisation boundaries. They often need to access outside services too. Due to the fact that these services are situated in different security domains users are normally forced to select separate credentials - mostly based on usernames and passwords - for each of these services. These usernames and passwords have all to be kept safe and secret by the user while each service provider has to administrate these user accounts and link them with roles and access rights. Apart from administration-efforts for service providers these conventional methods may also cause security vulnerabilities (users tend to choose simple passwords especially when they are forced to maintain several different credentials), drawbacks regarding usability (users have to authenticate against each service they want to use) and last but not least unnecessary disclosure of personal information. Usually service providers do not need to know who is trying to authenticate, they just need to know a certain kind of attribute like a security role.*

*The Shibboleth project has been started [...] to address particularly the following issues:*

- abolishing the need to create multiple credentials for multiple services which may reduce security*
- minimization of disclosure of personal data [...]*

*Cross-domain Single-Sign-On for users that are linked with many different attributes is one of the main use cases for Shibboleth. [...] The required pieces of information can be retrieved more effectively by using the Attribute Authentication concept of the Shibboleth System. [...]*

The Shibboleth framework is based on three major components:

- the Identity Provider (IP),*
- the Service Provider (SP)*
- and an optional component called "Where-Are-You-From-Service" (WAYF) [...]*

*The Identity Provider is responsible for maintaining and handling user credentials and attributes. In response to requests from Service Providers acting as relying parties it returns authentication assertions as well as attribute assertions. [...] The Identity Provider is divided into four sub-components [...]:*

- SSO Service: If the Service Provider determines that the user has not yet been authenticated [...] the Service Provider redirects the user's client to the Single Sign-On (SSO) Service of the Identity Provider which initiates an authentication procedure. After interacting with an Authentication Authority the SSO Service returns the result of the authentication to the Service Provider.*
- Authentication Authority: The Authentication Authority is responsible for delegating authentication to appropriate authentication components. How authentication is being performed is out of scope of the specification and not part of the Shibboleth System. The Authentication Authority assembles authentication assertions for the Service Provider. An*

# eSanté

*authentication assertion ensures the Service Provider of the authenticity of a principal at a particular time based on a certain kind of authentication method. These assertions are usually digitally signed.*

- *Attribute Authority: The Attribute Authority issues attribute assertions upon authorized attribute requests. An attribute assertion contains further information on a principal so that access control decisions can be taken by the Service Provider.*
- *Artifact Resolution Service: Depending on the used profile ["Browser/Artifact" or "Browser/POST", in accordance to the SAML- 1.1-Profiles of the same name)], assertions are either directly returned to the Service Provider via HTTP(S)-POST or they have to be fetched separately by the Service Provider sending a request to the Artifact Resolution Service. To fetch assertions (authentication assertions as well as attribute assertions) the Service Provider needs to send a so called Artifact [(which only can be used once)] along with the request to the Artifact Resolution Service. The Service Provider and the Artifact Resolution Service are communicating directly without involvement of the client's browser. [...]*

*A Service Provider is responsible for restricting and managing access to protected resources. Upon unauthenticated request attempts to protected resources the Service Provider redirects the client's browser to the SSO Service of the Identity Provider in order to initiate an authentication process. After successful authentication the Service Provider finally receives an authentication assertion as well as an optional attribute assertion. [...] [T]he Service Provider is divided into two sub-components:*

- *Assertion Consumer Service: The Assertion Consumer Service is a component that processes assertions retrieved from the Artifact Resolution Service of the Identity Provider.*
- *Attribute Requester: This component requests attributes upon a successful authentication from the Attribute Authority. [...]*

*The WAYF Service is of specific interest in terms of the usage of Shibboleth within a heterogenous context where different users perform authentication in different ways, some with username/password others with certificates and others with security tokens.*

*The WAYF Service is an optional component that enables the user to select his favourite Identity Provider. By selecting an Identity Provider the user implicitly chooses a certain kind of authentication procedure [...]. [C]itizens may be given a list of participating member states (each with its own national authentication procedure). After selecting his own country the citizen is redirected to a national Identity Provider instance that supports his type of eID.*

*[T]he WAYF Service acts as a kind of proxy that is put in between of the Service Provider and an Identity Provider's SSO service. Both the WAYF Service and the Identity Provider are based on the same HTTP interface so that a WAYF Service can be put into the queue without modification of the request parameters (these are transparently passed to the Identity Provider)."<sup>45</sup>*

## §5.4b OpenID

*"[...] OpenID aims at a solution for Single-Sign-On where users are allowed to authenticate themselves to various heterogeneous web sites using a single digital identity. [...] [T]he*

---

<sup>45</sup> Thomas Knall. STORK Work Item 3.3.4 - Trust Federation and Identity Frameworks. STORK. 2010-12-10, chapter 2, pp7-9. URL: [https://www.eid-stork.eu/index.php?option=com\\_processes&Itemid=&act=streamDocument&did=1397](https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1397). Accessed: 2011-01-12. (Archived by WebCite at <http://www.webcitation.org/5vg6J0lyu>)

# eSanté

*architecture of OpenID involves the concept of a Service Provider granting access to resources based on the assertion of an Identity Provider. Users may lodge data on themselves (attributes) at their favourite Identity Provider or - hence the standard does not specify how authentication is carried out - attributes may be retrieved by other means, like from an attribute authority for instance. Identity Providers allow the user to control the amount of personal data delivered to a Service Provider.*

*[...] [C]ollaboration on interoperability between OpenID and the Light-Weight Identity11 (LID) protocol resulted in the development of the Yadis12 discovery protocol. [...] [F]ull XRI13 support was added to OpenID as well as a first draft of the OpenID Attribute Exchange specification was released.[...]*

*The OpenID identity framework is based on two components:*

- the OpenID Provider (OP),*
- and the Relying Party (RP) [...]*

*An OpenID Provider [(Identity Provider)] is an OpenID Authentication server asserting that a certain end user has a specific identifier. According to the OpenID specification identifiers are either URL or XRI [...] based tokens. [...]*

*A Relying Party is a web application providing resources or services to endpoint users. Therefore, a Relying Party corresponds to a Service Provider in general context. Upon a user request the Relying Party checks if the user already has a security context established. If no security context (proven by a session cookie transmitted from the user's web browser to the Relying Part for instance) was found the Relying Party initiates an authentication request for the OpenID Provider. [...]*

*OpenID does not require special user agent capabilities as it's solely based on HTTP(S) requests and responses. Basically, the end user presents an identifier - which he claims to own - to a Relying Party. The main task of the OpenID protocol is to provide means to verify this claim and to return the result of the verification to the Relying Party."<sup>46</sup>*

## §5.4c Conclusion

*"[...]The Shibboleth system is designed to provide a federated identity based authentication and authorization infrastructure with the ability for Single-Sign-On. Since Shibboleth allows pure attribute based authorization, strict data protection requirements which may be compulsory within a cross-country federation may be realized. With the ability to encrypt authentication messages Shibboleth also addresses privacy concerns.*

*The design of OpenID appears to be less complex compared to the Shibboleth System. This may be one explanation why OpenID currently experiences quite a boom [...] although there are still security issues that need to be solved. At a first glance, the popularity of OpenID seems to beat Shibboleth's popularity, but on a closer examination it turns out there are many OpenID Providers for only few OpenID enabled sites.*

*In terms of interoperability Shibboleth seems to be better equipped as it is using SAML as well as providing a reference implementation and even a test service for Shibboleth installations."<sup>47</sup>*

<sup>46</sup> Thomas Knall, STORK Work Item 3.3.4 - Trust Federation and Identity Frameworks, chapter 3, pp17-18

<sup>47</sup> Thomas Knall, STORK Work Item 3.3.4 - Trust Federation and Identity Frameworks, chapter 5, p29

# eSanté

## §6 Cards in a Nutshell

The following tables give an overview about health professional cards, and citizen cards of some countries.

### §6.1 Special Health Professional Cards

#### §6.1a Germany<sup>48</sup>

Name	Type of Data stored on the Card Functionalities	Technology	Comments
HBA Heilberufsausweis	<b>Functionalities</b> <ul style="list-style-type: none"> <li>- Identification</li> <li>- Electronic signature</li> </ul>	Security Module Card Micro-processor 32 KB - 64 KB	

#### §6.1b France<sup>49</sup>

Name	Type of Data stored on the Card Functionalities	Technology	Comments
Carte Professionnel de Santé	<b>Data</b> <ul style="list-style-type: none"> <li>- Identification number of the health professional</li> <li>- Surname</li> <li>- Name of exercise, profession and specialty</li> <li>- Data for each activity identification of practice location billing</li> </ul>	Chip card 32 KB	

#### §6.1c Suisse<sup>50</sup>

Name	Type of Data stored on the Card Functionalities	Technology	Comments
Carta Professionista	<b>Functionalities</b> <ul style="list-style-type: none"> <li>- Identification</li> <li>- Authentication</li> <li>- Authorisation for the access to systems</li> <li>- Modification update of data</li> </ul>		

<sup>48</sup> Telemedizin Führer Deutschland 2006; <http://www.dimdi.de/static/de/ehealth/karte/>; <http://www.die-gesundheitskarte.de>; <http://www.gematik.de>

<sup>49</sup> GIE CPS: <http://www.gip-cps.fr>; GIE Sesam-Vitale: <http://www.sesam-vitale.fr>

<sup>50</sup> Telemedizin Führer Deutschland 2006 (Sonderausgabe Modellegionen, Projekte und Initiativen zur elektronischen Gesundheitskarte in Deutschlands und Europa); <http://www.retesan.ch>

### §6.1d Lombardy (Italy)<sup>51</sup>

Name	Type of Data stored on the Card Functionalities	Technology	Comments
Carta Sistema Informativo Socio Sanitario SISS	<b>Data</b> <ul style="list-style-type: none"> <li>- Identification data</li> <li>- Cryptographic algorithms</li> </ul> <b>Functionalities</b> <ul style="list-style-type: none"> <li>- Identification</li> <li>- Authentication</li> <li>- Authorisation for the access of systems</li> <li>- Electronic signature</li> </ul>	Chip card 32 KB	

### §6.1e Slovenia<sup>52</sup>

Name	Type of Data stored on the Card Functionalities	Technology	Comments
Health Professional Card	<b>Data</b> <ul style="list-style-type: none"> <li>- Identification number of the professional</li> <li>- Name and last name</li> <li>- Code of the institution of health care</li> <li>- Specialisation of the professional,</li> <li>- Type of the access rights</li> </ul>	Chip card 16 KB	

### §6.1f Republic of China (coll. Taiwan)<sup>53</sup>

Name	Type of Data stored on the Card Functionalities	Technology	Comments
Health Professional Card HPC Card		Chip card Java technology 32 KB	

### §6.1g Québec

Name	Type of Data stored on the Card Functionalities	Technology	Comments
	<b>Functionalities</b> <ul style="list-style-type: none"> <li>- Identification</li> <li>- Authentication</li> <li>- Authorisation to access systems</li> <li>- Modification et Update of data</li> </ul>		

<sup>51</sup> Carta Regionale dei Servizi: <http://www.crs.lombardia.it>; Netlink project: <http://www.sesam-vitale.fr/netlink>

<sup>52</sup> Health Insurance Institute of Slovenia: <http://www.zzzs.si>

<sup>53</sup> Bureau of National Health Insurance Taiwan: <http://www.nhi.gov.tw>; Consortium TECO / GD: <http://www.gdai.com>

# eSanté

## §6.2 Citizen Cards

### §6.2a Belgium<sup>54</sup>

Name	Type of Data stored on the Card Functionalities	Technology	Comments
e-ID Card	<p><b>Data</b></p> <ul style="list-style-type: none"> <li>- Name, Last Name</li> <li>- Date and place of birth</li> <li>- Photo</li> <li>- Card number</li> <li>- Identification number of the Registre National de la population</li> <li>- Issuing Commune</li> <li>- Type of card</li> <li>- Language</li> <li>- Emission and expiration date of the card</li> <li>- No biometric data for the moment, even if in the long term the card can be able to integrate these data</li> <li>- Electronic certificate</li> </ul> <p><b>Function</b></p> <ul style="list-style-type: none"> <li>- Authentication</li> <li>- Identification</li> <li>- Electronic signature Functionalities</li> <li>- To ask official documents and to fill of the forms</li> </ul>	<p>Chip card</p> <p>Java technology</p>	<p>Already exist in Belgium a centralized database on the entire national population, whose Committee on Privacy grant access to legal persons under certain limits to the uses made of information. This database is used in applying for this card.</p>

### §6.2b Finland<sup>55</sup>

Name	Type of Data stored on the Card Functionalities	Technology	Comments
e-ID Card	<p><b>Data</b></p> <ul style="list-style-type: none"> <li>- Identification certificate</li> <li>- Name, last name</li> <li>- Unique identifier</li> <li>- Signature certificate</li> </ul> <p><b>Health Insurance Card</b></p> <ul style="list-style-type: none"> <li>- Data of the health insurance</li> </ul> <p><b>Functionalities</b></p> <ul style="list-style-type: none"> <li>- Identification</li> <li>- Authentication</li> <li>- Electronic signature</li> <li>- Access to 50 online-services</li> <li>- Verify the data in the "Population Information System" (contains data of all Finnish citizens and foreigners living in Finland)</li> </ul>	<p>Chip card</p>	<p>The electronic identity card is distributed by the police</p> <p>The "Population Information System" is managed by the "Population Register Centre" which operates through the Ministry for the Interior</p>

<sup>54</sup> Carte d'Identité Électronique (eID): <http://eid.belgium.be/>; Registre National: <http://www.registrenational.fgov.be>; Portail Fédéral.be: <http://www.belgium.be/eportal>

<sup>55</sup> Population Register Centre: <http://www.vaestorekisterikeskus.fi>; FINEID.FI: <http://www.fineid.fi>

§6.2c Italy<sup>56</sup>

Name	Type of Data stored on the Card Functionalities	Technology	Comments
e-ID Card	<p><b>Data</b></p> <ul style="list-style-type: none"> <li>- Name, last name</li> <li>- Gender</li> <li>- Size</li> <li>- Nationality</li> <li>- Birthday</li> <li>- Unique identification number</li> <li>- Address</li> <li>- Tax number</li> <li>- Validity period of the card</li> <li>- Authentication keys</li> <li>- The chip could in the long term also contain given health data, which its holder will authorize to record there.</li> <li>- Optional recording of the digital fingerprints</li> </ul> <p><b>Functionalities</b></p> <ul style="list-style-type: none"> <li>- Identification</li> <li>- Authentication</li> <li>- Electronic signature</li> <li>- Access to public services, national or local</li> <li>- Health card</li> <li>- Payment card</li> <li>- Vote registration card</li> </ul>	<p>Card hydride:</p> <p>Microprocessor card</p> <p>Optical card</p>	<p>The optical card has the ability to be used as identity card. While the information stored on the chip makes it possible to ensure identification and authentication during the use of online services.</p> <p>Used in June 2004 as a vote registration card.</p>

§6.2d Estonia<sup>57</sup>

Name	Type of Data stored on the Card Functionalities	Technology	Comments
e-ID Card	<p><b>Data</b></p> <ul style="list-style-type: none"> <li>- Name, last name</li> <li>- Date and place of birth</li> <li>- Nationality</li> <li>- Others</li> <li>- Signing certificates</li> <li>- Authentication certificate with Name Identifier Government eMail</li> </ul> <p><b>Functionalities</b></p> <ul style="list-style-type: none"> <li>- Identification</li> <li>- Authentication</li> <li>- Electronic signature</li> <li>- Social security card</li> <li>- Access to the medical record</li> <li>- Access to the national online services</li> </ul>	Chip Card	<p>The legal text controlling the electronic signature was adopted by the Estonian Parliament on December 15th, 2000 making it possible to organize and manage infrastructure PKI</p> <p>The card is obligatory</p> <p>December 2005, nearly 880,000 cards had been distributed and 175,000 foreign residents had an electronic identity card</p> <p>Use of the card to vote online by Internet at the time of the municipal elections in October 2005</p>

<sup>56</sup> <http://www.innovazione.gov.it/ita/egovernment/infrastrutture/cie.shtml>; Carta Identitta Electronica: <http://www.cartaidentita.it/cie/reader/index.html>

<sup>57</sup> Estonian ID card: <http://www.id.ee/>