

tudor

PUBLIC RESEARCH CENTRE HENRI TUDOR
SANTEC - Healthcare Technologies

CRP Henri Tudor

SANTEC

Research Centre for Healthcare Technologies

2a rue Kalchesbrück

L-1852 LUXEMBOURG

Phone: +352 42 59 91-250 Fax: +352 42 59 91-251

Web: www.tudor.lu

eSanté

Work Package WP11 Identification of Patients Part 2 - State of the Art

Deliverable

Uwe Roth, François Wisniewski

Version 1.0

Final

09.05.2011

CR SANTEC

Project	eSanté	
Work Package	WP11 - Identification of Patient	
Head of the Department	RLe	Robert Lemor
Head of the Unit	CPo	Claude Poupart
Project Manager	SBe	Stefan Benzschawel
Team	URo	Uwe Roth
	FWi	François Wisniewski
	HBo	Hanan Bouzid
	MdS	Marcos Da Silveira
	HZi	Heiko Zimmermann

Contact

CRP Henri Tudor - SANTEC
Research Centre for Healthcare Technologies
Dr. Uwe Roth
2a rue Kalchesbrück
L-1852 Luxembourg
Phone: +352 42 59 91-298 / Fax: +352 42 59 91-251
EMail: uwe.roth@tudor.lu

Objective of the Document

This document describes a concept about the identification of patients and patient cards.

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 1.0

1.0a1	Draft Alpha	11/08/2010	URo	Splitting Document into Part 1 and Part 2
1.0a2	Draft Alpha	27/08/2010	URo	Structure
1.0a3	Draft Alpha	01/09/2010	URo	epSOS
1.0a4	Draft Alpha	08/09/2010	URo	STORK, Steps
1.0a5	Draft Alpha	16/12/2010	URo	RFID
1.0a6	Draft Alpha	14/01/2011	URo	STORK State-of-the-Art moved to WP12
1.0a7	Draft Alpha	20/01/2011	URo	NETC@RDS
1.0a8	Draft Alpha	25/01/2011	URo	e-EHIC
1.0b1	Draft Beta	26/01/2011	Uro	State of the Art of Exemplary Countries
1.0b1_versRKr	Draft Beta	07/02/2011	RKr	Review
1.0b2	Draft Beta	10/02/2011	URo	Integration of Review
1.0rfc1	RFC	31/03/2011	URo	RFC Version
1.0rfc2	RFC	20/03/2011	URo	Update
1.0	Final	09/05/2011	URo	Final

Table of Contents

§1 State of the Art of Exemplary Countries	5
§2 NETC@RDS for e-EHIC	8
§2.1 Overview	8
§2.2 Goals and Benefits.....	8
§2.3 Target Users and Operators	9
§2.4 Functions.....	9
§2.5 e-EHIC Technical Requirements	9
§2.5a Features.....	9
§2.5b Supported Cards	10
§2.5c Interoperability	11
§2.6 Impact for the Development of a Luxembourgish Patient Card	11
§2.7 Impact for the Development of a Luxembourgish eHealth Infrastructure	11
§3 epSOS.....	12
§3.1 Overview	12
§3.2 Use Cases.....	13
§3.2a Use Case 1: Patient Summary.....	13
§3.2b Use Case 2: ePrescription	13
§3.3 Identity Management.....	13
§3.3a Definition: Identity.....	14
§3.3b Definition: Identification.....	14
§3.3c Definition: Authentication	15
§3.3d Identification and Authentication of Patients	15
§3.4 Impact for the Development of a Luxembourgish Patient Card	17
§3.5 Impact for the Development of a Luxembourgish eHealth Infrastructure	17
§4 STORK	18
§4.1 Overview	18
§4.2 Use Cases.....	19
§4.3 Impact for the Development of a Luxembourgish Patient Card and eHealth Infrastructure	20
§5 STepS - Connecting STORK and epSOS	21
§6 Cards in a Nutshell.....	23
§6.1 Special Patient/Insurance/Social Security Cards	23
§6.1a Germany.....	23

§6.1b France 23

§6.1c Austria 24

§6.1d Italy 24

§6.1e Suisse 25

§6.1f Belgium 25

§6.1g Slovenia 26

§6.1h Republic of China (coll. Taiwan) 27

§6.1i Québec 27

§6.2 Citizen Cards 28

§6.2a Italy 28

§6.2b Finland 29

§6.2c Belgium 29

§6.2d Estonia 30

§1 State of the Art of Exemplary Countries

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

Identification

This table shows the identification method for each country.

	Identification Method	Remark
France	Patient Card	Carte Vitale 2
Slovenia	Health Insurance Card (HIC)	2nd Generation
Estonia	National ID Card	
Belgium	National ID Card	BELPIC
	Social Security Card	Carte SIS

Application

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

France	Identify the insured person. Electronic transmission of the sheets of care, Access to Medical Record, Authentication, Signing
Slovenia	Identify the insured person. Access key to services by the means of a network of terminals in self-service: Data of medical assistances technical (prosthesis, wheel chairs, ...), Relative data with the allergies and vaccination, Voluntary engagement to donor organs, Electronic prescription, Update online HIC, Allow medical professionals access to data in back-office systems. Access own data in back-office systems of health insurance companies and healthcare providers
Estonia	Digital Prescription, eHealth Record
Belgium	BELPIC: Access to eHealth portal
	Carte SIS: Identify the insured. Allows caregivers to have some form of electronic data on the situation of insurability under the care insurance health and implement the plan if possible third-party payment

Issuer

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

France	SESAM-Vitale
Slovenia	Health Insurance Institute of Slovenia
Estonia	Ministry of Internal Affairs, Citizenship and Migration Board
Belgium	BELPIC: Belgian Government, operated by Certipost
	Carte SIS: INAMI Institut national d'assurance maladie-invalidite

Management of Information

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

France	SESAM-Vitale
Slovenia	Health Insurance Institute of Slovenia
Estonia	Population Register
Belgium	BELPIC e-ID: National Register
	Carte SIS: INAMI Institut national d'assurance maladie-invalidite

Technical Specification

This section describes some technical details

France	Smartcard, Certificates, PIN Protected
Slovenia	Smartcard, Certificates, DES, DES-3, RSA, 1024 Bit, 1536 Bit, 2048 Bit
Estonia	Smartcard, Certificates, 1024 Bit RSA, PIN Protected
Belgium	BELPIC: Smartcard, Certificates, 1024 Bit RSA, PIN Protected
	Carte SIS: Memory Card, PIN Protected

Information Stored Inside the Card or Certificate

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

France	INSEE number, First name, Last name, Insurance data, Mode of insurance Security social, Biometric ID, Emergency data, 4 signed prescriptions, Last transaction of treatment, Information about additional insurances
Slovenia	Health insurance number, Card number, First name, Last name, Date of Birth, Address, Gender, Health insurance data, Data concerning the usually consulted doctors (general practitioners, podiatrists, gynaecologists, dentists)
Estonia	Card holder handwritten signature, Photo, Name, PIC, Birth Data, Gender, Citizenship, Card number, End date of card validity, Cardholder birth country, Card issuing date, Residence/work permit details (optional)
Belgium	BELPIC: Last name, First name(s), Date of birth, Place of birth, Gender, Place of card issuance, Validity period of the card, Title of the card, Number of the card, Picture of the bearer, National register number, Picture of handwritten signature
	Carte SIS: Social security number, Name, Initial of second name, Last name, Birth date, Gender, Validity period of the card, Card number, Number of the regional office, Membership number from regional office, Right for health care, Right to direct payment scheme

Information Stored Outside the Card

This section shows which information is managed outside the card.

France	Prescriptions, Patient Files
Estonia	Prescriptions, eHealth record
Slovenia	Personal data in back-office systems of health insurance companies and healthcare providers

Linking Card with the Patient

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

Estonia	Personal Identification Code / Isikukood / IK
Belgium	Carte SIS: Social security number

§2 NETC@RDS for e-EHIC

This chapter gives an overview about the NETC@RDS¹ for e-EHIC ID² project. The main target of the project is the possibility to check the status of the health insurance cross border.

§2.1 Overview

"The [...] NETC@RDS for e-EHIC ID project is aiming at achieving initial deployment of an on-line service for the "electronification" of the European Health Insurance Card (e-EHIC)[...]. [...]"

More specifically, NETC@RDS enables the Health Practitioners to check foreign patients' entitlement to health care. It is based on an agreement [...] between Health Insurance Organisations (HIO) aiming to provide easier access to cross-border healthcare for citizens travelling abroad but inside the EEE/EU and Switzerland.

The service can be provided via an eye-readable EHIC, a national health insurance electronic card, or via certain national e-ID chip cards issued by the responsible government authorities of the participating partners. An on-line verification provides assurance to support acceptance procedures for both health insurances and health care providers. [...]"³

§2.2 Goals and Benefits

"The [...] goal [...] is to achieve full integration with the existing and emerging national/regional infrastructures for eHealth and eID through the initial deployment of common administrative dataset and process supporting the use of electronic health and insurance cards.

The project is aimed at:

- *Providing reliable and interoperable solutions for the European Health Insurance Card electronification*
- *Enhancing interstate data exchange while using secure IT network software applications incorporating professional and personal smart cards with PKI and Digital Signature*
- *Contributing to mobility and skills convergent policy while improving Health Care Access for Mobile citizens*

These objectives will contribute to:

- *[...]*
- *Reduce fraudulent or irrelevant claims, thus avoiding expensive interstate health costs claim procedure*
- *[...]*
- *Enable patients and health professionals to collaborate and share insurance and other patient data for continuity of care*
- *Offer a user-friendly and secure systems to provide healthcare workers with important administrative information*
- *[...]"⁴*

¹ NETC@RDS - A Step Towards the Electronic EHIC. <http://netcards-project.com>

² Electronic European Health Insurance Card

³ NETC@RDS - A Step Towards the Electronic EHIC. NETC@RDS. URL:<http://netcards-project.com/web/frontpage>. Accessed: 2011-01-14. (Archived by WebCite at <http://www.webcitation.org/5vja7zUIA>)

⁴ NETC@RDS - Project Information - b) Objectives and Benefits. NETC@RDS. URL:<http://netcards-project.com/web/information>. Accessed: 2011-01-14. (Archived by WebCite at <http://www.webcitation.org/5vjaHuuJB>)

§2.3 Target Users and Operators

Primary Target Users: Insured European Citizens

*"The most important target users are the insured European mobile citizens who could be supported by the European-wide awareness and adoption of NETC@RDS services whenever they need to access unplanned health services in other participating countries."*⁵

Secondary Target Users: Health Care Insurance, Cost Clearance Organisations

*"The secondary target users are health insurance and cross border cost clearance organisations [...], involved in the reimbursement process. Electronic data capture and automated checking mechanisms will provide a much better base for clarification of inconsistencies, acquisition of statistical data, and improvement of the pan-European reimbursement process."*⁶

Primary Operators: Health Care Providers

*"The primary operators of the NETC@RDS services are health care providers in hospitals and ambulatory health care offices. Administrative staff in these medical units already frequently encounter persons coming from abroad and presenting their European Health Insurance Card. The value-added benefit of using NETC@RDS is that it can read the EHC electronically. This enables manual and paper based administrative processes to be reduced and has the added benefit of providing an accurate electronic EHC data set for post processing."*⁷

§2.4 Functions

"The NETC@RDS service for electronification of the EHC serves three distinct processes:

- *automated data capture for identification based on a common set of data elements*
- *on-line verification of entitlement rights via national portals, and*
- *minimal data provision which can contribute to subsequent back-office interstate-billing.*

The specific content of the NETC@RDS service is predicated on the patient EHC data, and verification data in the national health insurance databases. The specification of this data is provided by the European regulatory bodies.

*The common area of interest is in mutual use and recognition of the pan-European standardised eEHC as a means of validating entitlement to unplanned health care. In addition two other cases are included: optical recognition of existing EHC cards, and data capture of an eEHC identification data set, incorporated in a national e-ID from specific member states of the participating partners. [...]"*⁸

§2.5 e-EHC Technical Requirements

§2.5a Features

Netc@rds builds on the electronic European Health Insurance Card (e-EHC⁹):

⁵ NETC@RDS - Project Information - b) Users

⁶ NETC@RDS - Project Information - b) Users

⁷ NETC@RDS - Project Information - b) Users

⁸ NETC@RDS - Project Information - d) The service

⁹ In this section referred as "eEHC"

- *"It will carry the same dataset in electronic form that is defined by the data printed on the outside of the EHIC,*
- *it will be electronically read in the premises of the Health Care Providers (general practitioners, pharmacists, hospitals, dentists and other health related practitioners) equipped with appropriate technology (card reader and workstation with a computer program able to read from the card) and*
- *its validity as well as the entitlement of the card holder could, under certain conditions and depending on the Member States, be verified on-line.*

[The following alternatives for the Members States are defined:]

- 1) Staying with the eye readable EHIC system,*
- 2) Issuing an eEHIC (that might be a brand new national card or an already existing one)*
- 3) Adapting the healthcare professionals' infrastructure for reading eEHIC issued in other Member States,*
- 4) Issuing an eEHIC and adapting the healthcare professionals' infrastructure for reading eEHIC issued in other Member States.*

*The non-electronic EHIC already on the field will therefore be allowed to remain in full use all over Europe even as the eEHIC is already introduced."*¹⁰

§2.5b Supported Cards

"[...] eEHIC is conceived as a Smart Card. [...] [I]t must be usable as an eye-readable ID-1 plastic card.[...]

[Two purposes will be served by the specification], i.e. creating a "new" eEHIC Smart Card with optional security functions based on European Citizen Card standard or share an legacy national Smart Card infrastructure. [...]

[The specification] sets out to define an open solution that can support the use of different types of eEHIC smart card solutions ranging from single only restricted eEHIC usage to accessing multiple applications at different types of system terminals.

In particular, the specification supports the following facilities:

- *[Type 1:] A completely new smart card implementation, either open to other services or not*
- *[Type 2:] A Card pointing to a Card-Info-File containing information on where the EHIC data are stored (outside of the card)*
- *[Type 3:] An existing card where the eEHIC service can be added to its list of services*
- *[Type 4:] An existing card without that capability"*¹¹

"[...] [For the first] three types [...] ISO/IEC 24727 eEHIC cards are foreseen: [...]:

- *[Type 1] cards store the EHIC data on the card according to the normalized data set format, i.e. a description of the data and how they are stored that is part of the specification*
- *[Type 2] cards retrieve data stored someplace else.*
- *[Type 3] cards have already stored the relevant information for other applications."*¹²

¹⁰ Angelidis, Pantelis; Faher, Mourad; Nader, Noel; Brown, Philip. The electronic European Health Insurance Card. CEN/ISSS eEHIC PT. 2009-03. Chapter 2, Background, pp3-4. URL:ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eEHIC/white%20paper-eehic%20v10.pdf. Accessed: 2011-01-17. (Archived by WebCite at http://www.webcitation.org/5vo8pLKBq)

¹¹ Angelidis, Pantelis; Faher, Mourad; Nader, Noel; Brown, Philip. The electronic European Health Insurance Card. Chapter 3, eEHIC operating environment, p5

"For optional authentication purposes, ECC (CEN/TS 15480-2) security features elaborated under the guidance of CEN TC224 Committee by WG15 and WG16 are recommended [...]."¹³

§2.5c Interoperability

"The resources shared in an interoperable environment using smart cards may include as far as the eEHIC is concerned:

1. *the cards themselves: This would mean using one smart card for the purpose of eEHIC as well as for other purposes (like e.g. an eID or a citizen card or a health (insurance) or social security card)*
2. *terminals (workstations) supporting card readers with computer programs able to access smart cards (this could e.g. be a workstation already in place for use with a national card)*
3. *data networks and network nodes used by Healthcare (Service) Providers*
4. *the issuing institute citizen database, i.e. the institute in the home [Member State] of the citizen that issues the card*
5. *the clearing institute insured database, i.e. the institute in the home [Member State] of the citizen that is responsible for clearing cross-border insurance transaction (may be the same as the previous one in some [Member States])*
6. *data and information*
7. *card functionality, i.e. services performed by the card, as for example authentication"*¹⁴

§2.6 Impact for the Development of a Luxembourgish Patient Card

The focus of NetC@rds and eEHIC lies in the possibility to prove of the validity of the insurance of European citizens. It is more a question, if the eEHIC functionality should be part of a Patient Card or Citizen Card or not.

§2.7 Impact for the Development of a Luxembourgish eHealth Infrastructure

The setup of the NetC@rds / eEHIC infrastructure can be setup independent from the setup of the Luxembourgish eHealth Infrastructure. From a data and privacy protection perspective it might also make sense, to separate workflows, which are insurance and billing related, from services, which are health care related.

¹² Angelidis, Pantelis; Faher, Mourad; Nader, Noel; Brown, Philip. The electronic European Health Insurance Card. Chapter 4.1, Implementation Principles - Openness, pp7-8

¹³ Angelidis, Pantelis; Faher, Mourad; Nader, Noel; Brown, Philip. The electronic European Health Insurance Card. Chapter 4.1, Implementation Principles - Privacy and data transparency, pp8-9

¹⁴ Angelidis, Pantelis; Faher, Mourad; Nader, Noel; Brown, Philip. The electronic European Health Insurance Card. Chapter 3, eEHIC operating environment, p5-6

§3 epSOS

This chapter gives an overview about epSOS¹⁵, "*an Open eHealth initiative for a large scale European pilot of patient summary and electronic prescription*"¹⁶. This overview has a closer look at the work package WP3.6 concerning the identity management¹⁷, especially the identification of patients.

The epSOS project does not include the definition of patient cards. It refers to other projects in the EU, esp. the STORK and NETC@ARDS project, if requirements for patient cards are addressed.

§3.1 Overview

*"The overarching goal of epSOS is to develop a practical eHealth framework and an Information & Communication Technology (ICT) infrastructure that will enable secure access to patient health information, particularly with respect to basic patient summaries and ePrescriptions between different European healthcare systems. [...] To achieve this goal, the national entities [...] test both services in pilot applications, which interconnect national solutions [(Large Scale Pilot)]. The approach [...] aims to deliver both a methodological process and durable implementations: building blocks. These building blocks will form the basis for a longer term, pan-European approach to develop interoperable service solutions."*¹⁸

"Nine specific goals for the project have been outlined:

- 1. Agreement on a dataset describing the accepted terms of patient summaries, as well as the minimum data set required for countries to connect to the services;*
- 2. Agreement on a basic dataset and other requirements for ePrescriptions;*
- 3. Agreement on a minimum set of requirements to access this information taking the needs of the various constituencies, such as citizens, healthcare professionals, and healthcare provider organisations into account;*
- 4. Design, implementation and testing of a practical technical solution for confidentiality and security requirements in a 'laboratory' setting;*
- 5. Demonstrate the practical implementation of the solution - in compliance with confidentiality and security requirements; in numerous settings as well as participating states*
- 6. Evaluation of the results following their practical implementation;*
- 7. Demonstration of the ability to access information in compliance with relevant confidentiality and security requirements, in particular including the guidelines of the European Data Protection Directive and any other formally agreed upon amendments based on Article 29 Working Party;*
- 8. Selection and usage of relevant interoperability standards;*
- 9. Advise on implementation methods, which can be replicated in all other member states;"*¹⁹

¹⁵ Smart Open Services for European Patients: <http://www.epsos.eu/>

¹⁶ About epSOS. epSOS. URL: <http://www.epsos.eu/about-epsos.html>. Accessed: 2011-01-14. (Archived by WebCite at <http://www.webcitation.org/5vjD6hhJf>)

¹⁷ Hurch, Martin; Helder, Gottfried. Deliverable: Work Package Document, WP3.6, D3.6.2 Final Identity Management Specification Definition, v1.2, Final. epSOS. 2010-06-25. URL: http://www.epsos.eu/fileadmin/content/pdf/deliverables/D3.6.2_Final_Identity_Management_Specificiation_Definition.pdf. Accessed: 2011-01-14. (Archived by WebCite at <http://www.webcitation.org/5vjDMhxB1>)

¹⁸ About epSOS. epSOS

¹⁹ Purpose of epSOS. epSOS. URL: <http://www.epsos.eu/about-epsos/purpose-of-epsos.html>. Accessed: 2011-01-14. (Archived by WebCite at <http://www.webcitation.org/5vjDfYsqh>)

§3.2 Use Cases

§3.2a Use Case 1: Patient Summery

"Two distinct types of use cases for cross-border communication have been identified:

- *An occasional visitor, for example someone on holiday or attending a business meeting. The distinguishing characteristic is that this type of visit is irregular, infrequent, and may not be repeated. This is a type of incidental encounter where the healthcare professional may have no previous record of the person seeking care.*
- *A routine case, for example someone who lives in one country but works in another. The distinguishing characteristic is that this type of visit is regular, frequent, and the person seeking care may be accustomed to using services in the country where he or she works as a matter of personal convenience. This is a type of occasional situation where the healthcare professional may have some information available from previous encounters* ²⁰

§3.2b Use Case 2: ePrescription

"Within the cross-border prescription area there are two basic generic use cases:

- *A patient needs medicine that is already prescribed in the home country when in another country. In this case the pharmacist should be able to electronically access the prescription from the same eHealth interface used for prescriptions ordered in the local country. When medicine is dispatched, the system should notify the home country node of the foreign patient about the dispensed drugs.*
- *A medical professional decides to prescribe medicine to a visiting patient from another country. To assist the medical professional to make the best decision on the pharmaceutical strategy to be used, the patient's medical and pharmaceutical history from her home country will be available through the patient summary. When the electronic prescription is finalized, a copy of the prescription will also be sent to the patient's national node for inclusion in the national medication summary.* ²¹

§3.3 Identity Management

"[...], [T]he declared objectives [...] were to develop processes for:

- *Identification and authentication of patients and Health Care Providers*
- *Authorisation of Health Care Providers*
- *Patient consent*
- *Audit Trail.*

[...] [T]he design of the necessary processes for identification and authentication of patients and [Health Care Professionals] supports the participating Member States in creating, or easily adapting, processes within their own infrastructures, which are fully compliant with the goals of the [Large Scale

²⁰ epSOS Use Cases - Use Case 1 - Patient Summery. epSOS. 2011-01-14. URL:<http://www.epsos.eu/use-cases.html> . Accessed: 2011-01-14. (Archived by WebCite at <http://www.webcitation.org/5vjDmPrZB>)

²¹ epSOS Use Cases - Use Case 2 - ePrescription. epSOS. 2011-01-14. URL:<http://www.epsos.eu/use-cases.html> . Accessed: 2011-01-14. (Archived by WebCite at <http://www.webcitation.org/5vjDmPrZB>)

Pilot]. [...] Many of the necessary steps or parts of the identification and authentication processes are based on technologies, which are commonly used right now.

The actual progress of comparable EU-Projects and [Large Scale Pilots] for cross-border identification and authentication was investigated before the design process [...] was started, and possible future synergies have been analyzed. [...] Due to the fact that national laws and regulations differ significantly regarding some important issues, a number of final decisions have to be postponed until the piloting phase.

There are still a number of unanswered questions and open issues concerning the handling and management of patient consent, which makes further investigations, analyses and agreements necessary. [...] Nevertheless, [the work package] proposes processes and requirements for Member States on a commonly understood and agreed basis."²²

§3.3a Definition: Identity

"Identity is an abstract notion and usually the identity of an entity can be represented by an identifier. The identifier is a non-empty set of identity information that uniquely characterises an entity in a specific domain of applicability. Typical attributes which will be combined to identifiers, are the following personal data

- Surname
- Given Name
- Date of birth (YYYYMMDD)
- Gender
- Country of origin
- Unique Identifier (if available)
- Other identifiers (e.g.: driver license number, passport no, etc.)

[...] The validity of identifiers may be limited by date (e.g. number of a passport) or changed by other reasons (e.g. changed name after marriage). So therefore, in many cases a history of all valid values for identity information - including the former ones - is necessary."²³

§3.3b Definition: Identification

"The process to determine that presented identity information (associated with a particular entity²⁴) is sufficient to recognize the entity in a particular domain of applicability is called identification."²⁵

"Identification provides an answer, whether the provided identity information is sufficient to determine the entity or not, but it does not deal with the validity of identity."²⁶

²² Heider, Gottfried. epSOS: D3.6.2- Final Identity Management Specification Definition Summary. epSOS. URL:<http://www.epsos.eu/work-plan/work-package-36/d362-final-identity-management-specification-definition.html>. Accessed: 2011-01-14. (Archived by WebCite at <http://www.webcitation.org/5vjE2SWvD>)

²³ Hurch, Martin; Helder, Gottfried. Deliverable: Work Package Document, WP3.6, D3.6.2 Final Identity Management Specification Definition, v1.2, Final. epSOS. 2010-06-25. Chapter 3.2, Identity, pp13-14

²⁴ physical person, legal person, technical device, system, document, data

²⁵ Hurch, Martin; Helder, Gottfried. Deliverable: Work Package Document, WP3.6, D3.6.2 Final Identity Management Specification Definition, v1.2, Final. epSOS. 2010-06-25. Chapter 4.1, Identification, p18

²⁶ Hurch, Martin; Helder, Gottfried. Deliverable: Work Package Document, WP3.6, D3.6.2 Final Identity Management Specification Definition, v1.2, Final. epSOS. 2010-06-25. Chapter 4.2, Authentication, p18

§3.3c Definition: Authentication

"Authentication is the process of establishing an acceptable level of assurance that a claimed identity of an entity is genuine. The authentication of a human identity is usually based on one of the following attributes of the entity. However, at least two of them are necessary to obtain a high level of authentication and at least one attribute should be secret:

- *Biometric characteristics such as retina pattern, fingerprints, iris pattern, voice, face image, handwriting, etc.,*
- *ID card, passport, authentication token, certificate, cryptographic keys,*
- *Secret data such as passwords or PIN-Codes.*

The entity attributes used for entity identity authentication must be linked in a trustworthy way to the entity. This is a task of an identity authority - an entity that can make authoritative assertions on the validity of one or more attribute values in an identity.

Identity authority examples:

- *State institution issuing passports [...]*
- *Issuer of ID cards, service cards, membership certificates [...]*
- *University [...].*

Within the epSOS [pilot] environment existing identity authorities can be used within identification and authentication processes."²⁷

§3.3d Identification and Authentication of Patients

"Patients are other key actors of epSOS [...]. They enter into many relations with other epSOS [...] entities and they cannot act as anonymous persons in all cases. Any patient needs to identify and authenticate himself in three cases:

- *When the patient needs a health service and visits a [Health Care Professional] in Country B;*
- *When the patient wants to administrate his own patient consent (in Country B it only ca be done by a [Health Care Professional] at [the Point of Care]);*
- *When the patient wants to check who has accessed his health data (for Country B it only can be done by a health data administrator in Country A).*

Following there are three valid processes of patient identification and authentication in epSOS [...] depending on the available identification and authentication mechanisms of Country A:

- *With a unique identifier*
- *With demographic data*
- *Via internet portal (with the limited potential of authentication).*
Note: Internet Portal is not part of [the] epSOS [pilot] but some [Member States] have implemented such solutions.

At least one of these possible methods to identify and authenticate patients abroad MUST be installed and maintained by a participating [Member States].

²⁷ Hurch, Martin; Helder, Gottfried. Deliverable: Work Package Document, WP3.6, D3.6.2 Final Identity Management Specification Definition, v1.2, Final. epSOS. 2010-06-25. Chapter 4.2, Authentication, p18

If the authentication of the patient fails, no further processing of patient's health data or administration of patient's consent can be done.

*For patient's identification and authentication the collaboration with the STORK project in future steps will be useful and strongly recommended."*²⁸

*"If a child has no unique Health-Care identifier (eg-. Insured by the parents) then the identification process can't started and therefore children will not be handled as patients in epSOS."*²⁹

§3.3d (1) Unique Identifier / eID

"This process describes the case in which a patient of Country A identifies and authenticates himself for epSOS [...] at a [Point of Care] in Country B using a unique identifier (e.g. eID stored on smart card or another unique authentication token). This identifier is issued by a national authority in Country A and is stored in the national infrastructure of Country A (national registry) or it can be stored in an authentic way, e.g. by a digital signature which can be validated. If the presented identifier can be successfully validated by Country A, the patient is authenticated for epSOS [...].

*If an eID is used, it is a precondition for this process that the system at [the Point of Care] in Country B must have the capability to deal with an eID (e.g. read a "foreign" smart card) of Country A."*³⁰

§3.3d (2) Demographic Data

"This process describes the case of a patient of Country A, who wants to be identified and authenticated for epSOS [...] in Country B at the [Point of Care] without having an eID. The patient needs some trustworthy document with photo and with demographic data.

Demographic data itself is stored in national infrastructure in Country A (national registry in Country A)

Minimum data elements for searching a patient:

- Surname
- Given Name
- Date of birth (YYYYMMDD)
- Gender
- Country of origin Unique Identifier (if available)
- Other identifiers (e.g.: ID number, driving license number, passport number, etc.)

Additional data elements, if necessary in different [Member States], can be added (e.g. address). [...]

As a precondition, the patient has to show a trustworthy document (e.g. driving license, passport) as an identifier to the [Health Care Provider]. This is the starting point of the identification and authentication process. [...]

The definition of needed dataset may vary from country to country and may change over the time. E.g. France needs only a predefined ID (instead of concrete demographic data) which identifies French citizens and Germany has some special requirements as part of the usage of pseudonyms and TANs for

²⁸ Hurch, Martin; Helder, Gottfried. Deliverable: Work Package Document, WP3.6, D3.6.2 Final Identity Management Specification Definition, v1.2, Final. epSOS. 2010-06-25. Chapter 7.3, 7.3.2 Identification and authentication of a patient, p38

²⁹ Hurch, Martin; Helder, Gottfried. Deliverable: Work Package Document, WP3.6, D3.6.2 Final Identity Management Specification Definition, v1.2, Final. epSOS. 2010-06-25. Chapter 7.3, 7.3.2.1 Identification and authentication of children, p38

³⁰ Hurch, Martin; Helder, Gottfried. Deliverable: Work Package Document, WP3.6, D3.6.2 Final Identity Management Specification Definition, v1.2, Final. epSOS. 2010-06-25. Chapter 7.3, 7.3.2.2 Identification and authentication of a patient with a unique identifier, p39

*data privacy reasons based on the German legislation. Any changes of these datasets should be maintained by the concerned country itself and stored in the Central Services layer. [...]*³¹

§3.4 Impact for the Development of a Luxembourgish Patient Card

epSOS does not make any assumptions about the structure of a Luxembourgish Patient Card. The only requirement can be derived out a statement in chapter §3.3d (1) "Identification and Authentication of Patient - Unique Identifier / eID". The patient card can only be used as a means to identify the patient in a foreign country, if the card is readable with standard card readers and with standard software. But for the epSOS consortium, the usage of eID is also an open issue:

"The information about the implementation and operation of smartcard-based patient identification & authentication is rather limited. The technical and architectural means of the epSOS [...] specifications, as well as the procedural and organisational requirements [...], are fully capable of transporting and communicating this electronic identity information. However, whenever a Member State has completed the implementation of formerly unknown smartcards, the epSOS [...] specifications may need to be aligned accordingly.

*In order to fully enable the epSOS [...] system to operate smartcard-based patient identification & authentication, it is of crucial importance to communicate with the respective national certificate authorities of the identity issuing Member State. As of now, not all Member States have yet stated their individual plans about providing these communication means in a cross-border fashion."*³²

§3.5 Impact for the Development of a Luxembourgish eHealth Infrastructure

*"[...] [Member states] have to implement processes and workflows for Patient identification & authentication, [Health Care Professional] identification, authentication and authorization, patient consent and audit trail."*³³

In detail, chapter 9 of the epSOS WP3.6 deliverable³⁴ describes all requirements and recommendations for the national sites. It not only describes the infrastructure, which needs to be setup but also describes the processes, which needs to be implemented.

In short the infrastructure requires

- a National Contact Point
- a directory for health care professionals with defined data elements and their roles
- a system to manage patient consent
- a internet portal service for identification/authentication

³¹ Hurch, Martin; Helder, Gottfried. Deliverable: Work Package Document, WP3.6, D3.6.2 Final Identity Management Specification Definition, v1.2, Final. epSOS. 2010-06-25. Chapter 7.3, 7.3.2.3 Identification and authentication of a patient with a unique identifier, pp40

³² Hurch, Martin; Helder, Gottfried. Deliverable: Work Package Document, WP3.6, D3.6.2 Final Identity Management Specification Definition, v1.2, Final. epSOS. 2010-06-25. Chapter 8.7, Identification/Authentication based on eID, pp64-65

³³ Hurch, Martin; Helder, Gottfried. Deliverable: Work Package Document, WP3.6, D3.6.2 Final Identity Management Specification Definition, v1.2, Final. epSOS. 2010-06-25. Chapter 8.4, Necessary Implementation at National Site, p20

³⁴ Hurch, Martin; Helder, Gottfried. Deliverable: Work Package Document, WP3.6, D3.6.2 Final Identity Management Specification Definition, v1.2, Final. epSOS. 2010-06-25. Chapter 9, Requirements/Recommendations for National Sites, pp66-78

§4 STORK

This chapter gives an overview about the European STORK³⁵ (e-ID) project.

§4.1 Overview

"The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID.

Cross-border user authentication for such e-relations will be applied and tested by the project by means of five pilot projects that will use existing government services in EU Member States. In time however, additional service providers will also become connected to the platform thereby increasing the number of cross-border services available to European users.

Thus in the future, you should be able to start a company, get your tax refund, or obtain your university papers without physical presence; all you will need to access these services is to enter your personal data using your national eID, and the STORK platform will obtain the required guarantee (authentication) from your government. [...]

The role of the STORK platform is to identify a user who is in a session with a service provider, and to send his data to this service. Whilst the service provider may request various data items, the user always controls the data to be sent. The explicit consent of the owner of the data, the user, is always required before his data can be sent to the service provider. [...]

This user centric approach was not taken to satisfy some philosophical preferences, but in line with the legislative requirements of all the various countries involved that oblige concrete measures to be taken to guarantee that a citizen's fundamental rights, such as his privacy, are respected."³⁶

"Most EU countries have already deployed national electronic citizen cards; [...]. Other countries have opted for simpler solutions based on userid and password, sometimes complemented with other identification mechanisms.

The objective of the project is not to replace any existing national infrastructure, but rather to take what is already available and to connect all the various authentication methods with transparency, in such a way that any of these methods will allow users to present their certified personal data to foreign administrations."³⁷

"The project is aware that authentication schemes based on userid and password are weaker than eIDs stored in fully compliant hardware crypto-tokens. Furthermore the eID issuing procedure can be heavier or lighter, which also affects the quality of the identifier.

These two factors have been fully analysed by the STORK project, and divided into 7 elementary factors that form the basis of classification of the foreign identifiers. Service providers can require users to authenticate with any of these 4 levels of the authentication scheme."³⁸

³⁵ STORK: Secure Identity Across Borders linked: <https://www.eid-stork.eu/>

³⁶ STORK at a Glance. STORK. URL:https://www.eid-stork.eu/index.php?option=com_content&task=view&id=186. Accessed: 2011-01-14. (Archived by WebCite at <http://www.webcitation.org/5vjSi19Xf>)

³⁷ STORK at a Glance, Integration in existing eID Infrastructures. STORK

³⁸ STORK at a Glance, Quality of the Identifier. STORK

§4.2 Use Cases

"[...] [T]he STORK platform will be integrated into existing applications and tested in real, live situations. [...]"

1. *Cross-border Authentication Platform for Electronic Services*
A demonstrator showing that cross-border electronic services can operate in a number of Member States [...];
2. *Safer chat*
Promoting the safe use of the Internet by children and young people;
3. *Student mobility*
Facilitating people who want to study abroad in a different Member State;
4. *eDelivery*
Developing cross-border mechanisms for secure online delivery of documents;
5. *Change of Address*
*Assisting EU citizens move and settle in other EU countries;*³⁹

In the context of patient identification, only case 1 "Cross-border Authentication Platform for Electronic Services" is interesting. The general objectives are to demonstrate that

- *"[...] cross-border interoperable services can operate on the principles defined and tested in the course of the STORK project;*
- *[...] the common specifications defined by the STORK project are sufficiently flexible and scalable for the EU interoperability layer to accommodate a broad range of national services;*
- *[...] trust circles defined in the STORK project can operate in practice"*⁴⁰

The objectives in detail are to

- *"[...] test and implement the defined trust framework by operating services requiring different authentication levels;*
- *[...] test with applications (Service Providers) and national eID systems the EU interoperability layer defined and implemented in the course of the STORK project;*
- *[...] connect existing national portals and services participating in the Cross-border authentication platform for electronic services to the EU interoperability layer and the reference architecture models defined in the course of the STORK project;*
- *[...] test that the connections function with a variety of log-in methods and tokens.*
- *[...] assess the ease of use and take-up of cross-border e-ID services*
- *[...] implement an EU portal providing an overall interface to all the services accessible within the Cross-border authentication platform for electronic services."*⁴¹

³⁹ STORK at a Glance, The Pilots and their Integration. STORK

⁴⁰ STORK - Pilot1: Cross border authentication platform - for electronic services. STORK. URL:https://www.eid-stork.eu/index.php?option=com_content&task=view&id=85. Accessed: 2011-01-14. (Archived by WebCite at <http://www.webcitation.org/5vjT4tppE>)

⁴¹ STORK: Stork at a Glance: Pilot1: Cross border authentication platform - for electronic services, https://www.eid-stork.eu/index.php?option=com_content&task=view&id=85 (accessed 06.09.2010)

§4.3 Impact for the Development of a Luxembourgish Patient Card and eHealth Infrastructure

The goal of the project has definitely its target on the interoperability of e-IDs between European Countries. An Impact for the Luxembourg in the context of patient identification only arises, in case of the usage of e-IDs as patient identifiers.

The requirements for setting up the infrastructure are similar to those of the epSOS initiative. This is one reason, why both initiatives try to cooperate (see §5 "STepS - Connecting STORK and epSOS").

§5 STepS - Connecting STORK and epSOS

"STepS, the cooperation model between STORK and epSOS, is based on the assumption that these two pilot projects have overlapping infrastructural requirements. The challenge is to connect the projects in a synergetic way despite continuous concrete work being done in each project independently.

Within eHealth, eID comes laden with a number of security and trust issues. epSOS concentrates on the Public Health Sector, where the mechanisms and tools for personal identification in many member states are comparable, and in some cases are connected to identification in the eGovernment sector.

STepS' role is to define similarities and divert requirements of both sectors, to find out how far a synergetic development of eID will go and how can be secured for the future that sectoral progress is not going into different directions. STepS integrates the progress and outcomes developed and tested in STORK into epSOS with the goal of easing cross-border eHealth relations. Additionally, information which is not addressed by or necessary to STORK but needed in epSOS (e.g. specifications addressing different health service providers, authentication systems) will be developed independently within epSOS. [...]

STORK provides a common interoperability platform that integrates different solutions. Using STepS, the initial idea of setting up a pan-European eID system is expanded to include the eHealth requirements and specifications contained in epSOS.

epSOS and STORK based on the results in the projects so far decided to have STepS field tests, dealing with different concrete aspects of eID in the health sector.

At present a survey of all member states referring to six field test scenarios has been started:

- 1. PEPS and NCP co-location: STORK's PEPS (Pan-European Proxy Services) and epSOS' NCP (National Contact Points) are based on similar concepts. Augmenting epSOS' NCPs with STORK's modules may provide enhanced functions.*
- 2. Attribute transfer for health care provider (HCP) roles: STORK defines the protocols for attribute transfer. These protocols could be used in connection with epSOS' National Contact Points to have roles authorized online by competent authorities.*
- 3. HCP identification: Several member states involved in STORK or epSOS issue Health Care Professional cards (e.g. for general practitioners, dentists or pharmacists). A limited field test on integrating HCP cards into STORK for HCP identification in epSOS could be performed.*
- 4. Electronic patient consent: Patients are required to give consent prior to data being accessed or transferred. Depending on their national situation, this consent can be either implicit or explicit. For explicit consent, electronically signed patient consent can be field-tested for those member states where eID is based on signature cards.*
- 5. Patient access to electronic health records (EHR): Patient online access is not currently available in epSOS. Such access could be field-tested using STORK, since citizens using their eID to access their information online STORK's goal.*
- 6. Signature verification for ePrescription: Electronic prescriptions carry electronic signatures for the purposes of data origin authentication. Establishing a field test in this area however would*

have to take into account, that signature validation in cross-border environments still has to overcome some hurdles."⁴²

⁴² STepS (STORK-epsOS): Press Information, 5th EU-eGovernment Conference "Teaming up for eUnion". pp2-3. STORK. 2009-11-16. URL:http://www.epsos.eu/fileadmin/content/pdf/STePS_Malmö_final.doc. Accessed: 2011-01-14. (Archived by WebCite at <http://www.webcitation.org/5vjTReGCU>)

§6 Cards in a Nutshell

The following tables give an overview about patient cards, social security cards and citizen cards.

§6.1 Special Patient/Insurance/Social Security Cards

§6.1a Germany⁴³

Name	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
eGK Elektronische Gesundheitskarte	<p>European Recto: E111</p> <p>Obligatorily Data</p> <ul style="list-style-type: none"> - Information about the insurance - Administrative data - Electronic Prescription (eRezept) <p>Facultative Data</p> <ul style="list-style-type: none"> - Emergency data: (chronic diseases, implants, vaccinations, blood group), - Declaration about organ donor - Vaccination card, - Maternity protection pass (Mutterschutzpass) <p>Functionalities</p> <ul style="list-style-type: none"> - Identification - Electronic Signature - Medication documentation (Arzneimitteldokumentation) - Electronic doctors letter (Arztbrief) - Electronic patient record (EPA) 	<p>Global consents vs. partial and/or individual consents</p> <p>Card + PIN</p>	<p>Security Module Card</p> <p>Micro-processor</p> <p>32 KB - 63 KB</p>	<p>Standardisation of data makes problems</p> <p>Recommendation not to use Internet for the communication</p> <p>Patient might block information on certain levels</p> <p>Synchronisation of data in a reserved part for the electronic patient record</p>

§6.1b France⁴⁴

Name	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
Carte Vitale	<p>Data</p> <ul style="list-style-type: none"> - INSEE number - Name, last name - Insurance data mode of insurance health insurance security social - Biometric ID - Emergency data - 4 signed prescriptions - Last transaction of treatment - Information about additional insurances 		<p>Smartcard</p> <p>128KB ROM 32 KB EEPROM 5 KB RAM</p>	

⁴³ Telemedizin Führer Deutschland 2006; <http://www.dimdi.de/static/de/ehealth/karte/>; <http://www.die-gesundheitskarte.de>; <http://www.gematik.de>

⁴⁴ GIE CPS: <http://www.gip-cps.fr>; GIE Sesam-Vitale: <http://www.sesam-vitale.fr>

	Functionalities <ul style="list-style-type: none"> - Identify the social insured person - Electronic transmission of the sheets of care 			
--	--	--	--	--

§6.1c Austria⁴⁵

Name	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
e-Card	European Recto: E111 Obligatorily Data <ul style="list-style-type: none"> - Administrative data - Information about the insurance - Sickness certificate (Krankenschein, Krankenkassenscheck) Functionalities <ul style="list-style-type: none"> - Identification - Automatic approval of prescriptions from medical superintendent - Electronic Prescription (elektronische Rezept), - Electronic letter of referral (eÜberweisung/Zuweisung); - Electronic results (eBefundübermittlung) - Medical data - Emergency data - Disease management 		Micro-processor card LAN Card reader might be connected directly to the net	Could be wide towards a citizen card with the introduction of the national electronic signature.

§6.1d Italy⁴⁶

Name	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
Carta Regionale dei Servizi CRS	European Recto: E111 <ul style="list-style-type: none"> - Identification data - Administrative data - Emergency data - Possibility to store electronic signature Functionalities <ul style="list-style-type: none"> - Identification - Authentication - Access to the service for the public administration - Certification of the presents of the patient 	Written consent of the citizen for the treatment of information managed by the network SISS. Consent implies some measures (Informativa) Citizens might make data "invisible" and only accessible be giving the PIN.	Chip card 32 KB Netlink Specification for the storage of emergency data	Special terminals in the hospitals and pharmacies might be used to consult historic examinations and medical reports, medication, treatments and hospitalisation

⁴⁵ Telemedizin Führer Deutschland 2006 (Sonderausgabe Modellegionen, Projekte und Initiativen zur elektronischen Gesundheitskarte in Deutschland und Europa); <http://www.chipkarte.at>

⁴⁶ Carta Regionale dei Servizi: <http://www.crs.lombardia.it>; Netlink project: <http://www.sesam-vitale.fr/netlink>

§6.1e Suisse⁴⁷

Card Type	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
Carta Sanitaria	<p>Data</p> <ul style="list-style-type: none"> - Name - Address - Contacts in case of urgency - Insurance <p>Important Medical Data</p> <ul style="list-style-type: none"> - Allergies - Blood group - Vaccinations - Pharmacological therapy - List of principal health problems - Donner of organs <p>Medical Record</p> <ul style="list-style-type: none"> - Diagnostics - List of radiographies - Laboratory results - Identification - Authentication - Storage of information 	<p>The patients</p> <ul style="list-style-type: none"> - decides about the data stored on card - chooses the level of protection of the data - Decides who is able to access the data <p>Level 1: Free access to the data</p> <p>Level 2: Access limited to health professionals</p> <p>Level 3: Data is protected unless the patient enters his PIN</p>		<p>Intermediate results of the University of Lausanne:</p> <p>Patients</p> <ol style="list-style-type: none"> 1. are very interested 2. have fears about the abuse that could be made of data stored on the card 3. are willing to co-finance the card <p>Storage of data on the card and in servers</p>

§6.1f Belgium⁴⁸

Name	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
Carte SIS Système d'Identité Social	<p>Data</p> <ul style="list-style-type: none"> - Social security number - Name, initial second name, last name - Birth date - Gender - Validity period of the card - Card number (also printed on the card) <p>Functionalities</p> <ul style="list-style-type: none"> - Identify the social insured person - To provide the data under electronic format 	<p>"Public" data can be read but not modified (data identification schemes Basic National Registry of Persons)</p> <p>"Protected" data can be read only by using one key stored on the card of health professional (SAM).</p>	<p>Chip card</p> <p>1 KB</p>	<p>It is possible that the information stored on the SIS card is integrated into the electronic identity card Belgian (Belgium e-ID card)</p>

⁴⁷ Telemedizin Führer Deutschland 2006 (Sonderausgabe Modellegionen, Projekte und Initiativen zur elektronischen Gesundheitskarte in Deutschlands und Europa); <http://www.retesan.ch>

⁴⁸ Institut National d'Assurance Maladie - Invalidité (INAMI): <http://inami.fgov.be>; Banque Carrefour de la Sécurité Sociale (BCSS): <http://ksz-bcss.fgov.be/>

§6.1g Slovenia⁴⁹

Name	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
Health Insurance Card (2 nd Version) HIC Card	<p>Data Visible on the card</p> <ul style="list-style-type: none"> - Health insurance number - Card number - Name, last name - Date of Birth <p>On the chip</p> <ul style="list-style-type: none"> - Address - Gender - Health insurance data - Data concerning the usually consulted doctors (general practitioners, podiatrists, gynecologists, dentists) <p>Functionalities The HIC Card is the single document in force for the identification and the implementation of the rights to the health insurance deriving from the obligatory and voluntary health insurance. It is also used as access key to the proposed services by the means of a network of terminals in self-service.</p> <ul style="list-style-type: none"> - Data of medical assistances technical (prosthesis, wheel chairs, ...) - Relative data with the allergies and vaccination - Voluntary engagement to donor organs - Electronic prescription 	<p>The health professionals can only reach the data stored on the HIC by using their HPC card and a suitable reader</p> <p>The holders of a HPC cards are divided into several groups, each group having a HPC card with distinct key and, consequently, different rights of accessing the data within the HIC</p> <p>The network terminal self-service is used to update online HIC, services, adding new applications and functions to the card (HIC new files, change access rights) and the communication of information.</p>	<p>JavaCard Smartcard 72 KB</p>	

⁴⁹ Health Insurance Institute of Slovenia: <http://www.zzzs.si>

S6.1h Republic of China (coll. Taiwan)⁵⁰

Name	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
National Health Insurance Card	<p>Personal Data:</p> <ul style="list-style-type: none"> - Name - Gender - Date of Birth - Photo - Patient Identifier - Card number, - Date of creation <p>Treatments and others:</p> <ul style="list-style-type: none"> - Allergies - Drugs, - Long lasting prescriptions - Vaccinations - Donation of organs - Pregnancy <p>Insurance Data:</p> <ul style="list-style-type: none"> - Validity period of the card - Number of consultations and admissions - Entire amount of the medical treatment 	PIN code to protect the personal data	<p>Chip card</p> <p>Java technology</p> <p>32 KB</p>	<p>A NHI IC card places at the disposal of the patient a quota of 6 consultations (18 for the children of less than 6 years, 12 for patients of more than 70 years).</p> <p>When these 6 consultations were carried out, the patient must reload the card to again have a quota of 6 consultations</p> <p>To reload his card and to have 6 consultations again, the patient must use kiosk available in the agencies of the "Office of National Health Insurance" or the readers installed in the hospitals</p> <p>The recharging of the card is however possible only if the patient regulated all the expenses well.</p>

S6.1i Québec

Name	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
	<p>Administrative Data</p> <ul style="list-style-type: none"> - Name - Address - Contacts in case of urgency <p>Important Medical Data</p> <ul style="list-style-type: none"> - Allergies, - Blood group - Donor of organs - Vaccinations - Pharmacological Therapy - Wearing of prostheses - List of principal health problems - Medication <p>Functionalities</p> <ul style="list-style-type: none"> - Identification - Authentication - Assumption of costs / insurance 	<p>The patient may express its consent for a specified period and specifically target one or more participants or all members of the nursing team of one or more service organizations.</p> <p>In an emergency situation, a proper authorized participant can consult the summary of health information of the person in difficulty, as this is currently the case in any emergency.</p>	<p>Micro processor card</p>	

⁵⁰ Bureau of National Health Insurance Taiwan: <http://www.nhi.gov.tw>; Consortium TECO / GD: <http://www.gdai.com>

§6.2 Citizen Cards

For citizen cards the STORK initiative has created an overview, which presents some properties in more detail.⁵¹

§6.2a Italy⁵²

Card Type	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
e-ID Card	<p>Data</p> <ul style="list-style-type: none"> - Name, last name - Gender - Size - Nationality - Birthday - Unique identification number - Address - Tax number - Validity period of the card - Authentication keys - The chip could in the long term also contain given health data, which its holder will authorize to record there. - Optional recording of the digital fingerprints <p>Functionalities</p> <ul style="list-style-type: none"> - Identification - Authentication - Electronic signature - Access to public services, national or local - Health card - Payment card - Vote registration card 	The detention of the identity card is not obligatory.	<p>Card hydride: Microprocess or card</p> <p>Laser tape card (optical card)</p>	<p>The laser tape has vocation 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>

⁵¹ T. Zefferer, STORK Work Item 3.3.5 - Smartcard eID Comparison

⁵² <http://www.innovazione.gov.it/ita/egovernment/infrastrutture/cie.shtml>; Carta Identitta Electronica: <http://www.cartaidentita.it/cie/reader/index.html>

§6.2b Finland⁵³

Name	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
e-ID Card	<p>Data</p> <ul style="list-style-type: none"> - Identification certificate - Name, last name - Unique identifier - Signature certificate <p>Health Insurance Card (optional)</p> <ul style="list-style-type: none"> - Data of the health insurance <p>Functionalities</p> <ul style="list-style-type: none"> - Identification - Authentication - Electronic signature - Access to 50 online-services - Verify the data in the "Population Information System" (contains data of all Finnish citizens and foreigners living in Finland) 	PIN code	Chip card	<p>In March 2006, practically 85,000 Finnish citizens had a valid e-ID cards.</p> <p>16,400 of these people integrated their data of insurance health on the electronic identity 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>

§6.2c Belgium⁵⁴

Name	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
e-ID Card	<p>Data</p> <ul style="list-style-type: none"> - Name, Last Name - Date and place of birth - Photo - Card number - Identification number of the Registre National de la population - Issuing Commune - Type of card - Language - Emission and expiration date of the card - No biometric data for the moment, even if in the long term the card can be able to integrate these data - Electronic certificate <p>Function</p> <ul style="list-style-type: none"> - Authentication - Identification - Electronic signature <p>Functionalities</p> <ul style="list-style-type: none"> - To ask official documents and to fill of the forms 	<p>The regulations provide that each holder of an electronic identity card can access and view at any time the data stored on the card at the municipality in which it is registered in the population</p> <p>Functions with a PIN</p> <p>Except legal requirement or lawful, the consultation of the data of identification of the electronic identity card will have to be carried out with the authorization express of its holder</p>	<p>Chip card</p> <p>Java technology</p>	<p>In June 2005, 725,000 Belgian citizens had an electronic identity card. From here the end of 2009.8 million cards (Belgian population unit) will be distributed</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>

⁵³ Population Register Centre: <http://www.vaestorekisterikeskus.fi>; FINEID.FI: <http://www.fineid.fi>

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

§6.2d Estonia⁵⁵

Name	Type of Data stored on the Card Functionalities	Patient Consents	Technology	Comments
e-ID Card	<p>Data</p> <ul style="list-style-type: none"> - Name, last name - Date and place of birth - Nationality - Others - Signing certificates - Authentication certificate with Name Identifier - Government eMail <p>Functionalities</p> <ul style="list-style-type: none"> - Identification - Authentication - Electronic signature - Social security card - Access to the medical record - Access to the national online services 	PIN code	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>

⁵⁵ Estonian ID card: <http://www.id.ee/>