Smart Open Services for European Patients

Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription

Deliverable: Work Package Document

WP3.6

<Deliverable: D3.6.2 Final identity management specification definition >

June, 25th 2010

Document Version: V1.2 (FINAL)

Work Package Leader: **Martin Hurch / Gottfried Heider**
Beneficiary: **ELGA (Elektronische Gesundheitsakte)**

Table of Content

Document Information

Project name	Smart Open Services – Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription
Author/ person responsible	Gottfried Heider
Document name	WP36_D362 Identity management V1.0.doc
Status	in process | submitted to QA | accepted by QM | **approved**
Dissemination level	PUBLIC

Sub-Project Identification

Work Package	WP3.6
Working Tasks	WT3.6.2
Document Owner	Gottfried Heider

History of Alteration

Version	Date	Type of editing	Editorial
0.1	2009-06-02	First draft for internal review	ELGA
0.2	2009-06-17	First draft with included comments and open issues	ELGA
0.3	2009-06-25	Reordering chapters and paragraphs	ELGA
0.5	2009-07-02	Insert HPRO Document; Processes of necessary changes on nation side	ELGA
0.6	2009-08-06	Insert Chapter 3 intro, Parts 3.3, 3.4, 4.1, 4.2, supplement of Part 4.3, rearrangement 4.3 and chapter 10, intro to chapter 7, rewritten 7.1, insert 7.1.1	NHIC
0.7	2009-08-18	Insert evaluation of questionnaires	FhG ISST, GIP-DMP, ELGA
0.8.4	2009-08-28	Insert new definitions and descriptions	NHIC
0.9.5	2009-09-15	Insert processes and descriptions	NHIC
0.9.6	2009-09-20	Chapter 7 (Parts 7.4-10), Security requirements (to Chapter 8), Annex 16.1., some terms added to glossary	NHIC
0.9.6.1	2009-09-21	Move some parts to Annex II	ELGA
0.9.6.3	2009-09-22	Consolidation of Chapter 7 and Annex I, Part 16.1 was moved to chapter 9, Annex III was added, formal changes	NHIC

Version	Date	Type of editing	Editorial
0.9.6.4	2009-10-02	Consolidation after internal review and included comments	NHIC, ELGA
0.9.7	2009-10-19	Prepared for Quality review	ELGA
0.9.8.1	2009-11-21	Consolidation after Quality review	ELGA
0.9.8.3	2009-11-26	Consolidation after F2F-meeting	NHIC, ELGA
0.9.8.5	2009-12-02	Consolidation after internal review with included comments	NHIC, ELGA
0.9.8.6	2009-12-04	Add Chapter 9 (Open Issues) and 10 (Recommendation/Requirements)	ELGA
0.9.8.7	2009-12-05	Consolidation (Add Annex I)	ELGA
0.9.8.9	2009-12-06	Completion for external review	ELGA
0.9.9.0	2009-12-06	Internal Version	ELGA
0.9.9.1	2009-12-06	Version for external review (QA)	ELGA
0.9.9.2 - 0.9.9.9	2009-12-14 till 2009-09-21	Internal Version after External Review	ELGA
1.0	2009-12-22	Final Document (delivered to TPM)	ELGA
1.01	2010-01-13	Change some words to perfect English – add some comments	ELGA
1.1	2010-03-30	Modification of processes after finalisation of PD3 documents (including Central Services)	ELGA
1.2	2010-06-25	Finishing after Decision from PSB on June, 21st 2010 on Central Services	ELGA

1 Executive Summary

The main functionality of the epSOS LSP environment is the provision of patient health data stored in patient's home country (in epSOS LSP terminology: "patient's country of affiliation" and always seen or referred to as "Country A") to a health care professional providing health service in a foreign country (referred to as "Country B").

According to ISO/IEC CD 24760, "Identity Management" in general relates to the issuance, administration, and use of identities of entities known in a particular domain of applicability.

Therefore "Identity Management" is one of the crucial elements of networked systems, where human users and their roles need to be known and assured. This applies especially in epSOS LSP, where a patient and a "Health Care Provider" build up a trustful relationship. To be able to rely on personal and corresponding health data is one of the most important issues to assure that medical care is done properly and with a set of trustworthy information.

As described in "Annex I" identification is a vital element of epSOS LSP.

> *Proved identification of persons is one of the basic requirements for the access of person related health data on the regional, national and also multinational level in the European context. Such as other requirements (e.g. data protection legislation, security, trust, reimbursement), person identification has an exponential complexity on the bi- or multilateral level. Proper person identification has to be solved both, on a national and a multinational level, before accessing even one set of individual health data cross-border.*
>
> *The challenge is to identify internationally compatible and interoperable solutions on three levels:*
>
> - *Person identification / patient identification,*
> - *Healthcare provider identification incl. identification of persons (health professionals) working in organisations with more than one employee,*
> - *Rights management: definition of rights, definition of rules and procedures for health professionals.*

Based on this description the declared objectives of WP3.6 are to develop processes for:

- Identification and authentication of patient and Healthcare provider
- Authorisation of Healthcare provider
- Patient consent
- Audit Trail

The development of these processes is based on functional requirements of other WPs in the epSOS LSP (mainly WP 3.1 and WP 3.2) and instructions of WP 2.1. National constraints (national security policies and patient privacy policies) are taken in consideration, as well as the right of patients to make autonomous decisions.

The two opposite starting points

- to keep the interference with already installed systems in MSs as less as possible

and on the other hand

- to take into consideration that most of the steps of the designed processes have to be included in national infrastructures

emphasise the complexity of multilateral identity management.

This in mind, the design of the necessary processes for identification and authentication purposes of patients and HCPs supports the participating MSs in creating or easily adapting processes

within their own infrastructures, which are fully compliant with the goals of epSOS LSP. This is achieved by presenting different variants and options for these processes, which are all comparable and equally valid. 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 LSPs for cross border identification and authentication was investigated before the design process within WP 3.6 was started and possible synergies in the future have been analyzed.

The most challenging and complex topic is the bilateral authorisation of HCPs to access patient's health data abroad. Due to the fact that national laws and regulations differ extremely in important points, some final decisions have to be postponed to the piloting phase.

Especially the handling and management of patient consent still raises open questions and issues which need some further investigations, analyses and agreements. This is an ongoing process driven by WP 2.1. Nevertheless WP 3.6 proposes processes and requirements for MSs on a commonly understood and agreed base.

Descriptions of the mentioned processes and their possible variants are presented in the following chapters of this document in more detail.

The outcome of the described processes is listed in chapter 16 ("Annex I Overview about requirements/recommendations and responsibilities") as requirements and recommendations, completed by the appropriate responsibilities.

2 Introduction

2.1 Objectives

Identification and authentication refer to the necessity to establish the identity of patients and healthcare providers as well as for documents and other objects in the care process. *Identification* provides an answer, whether the provided identity information is sufficient to determine the entity or not (recognition of their identity), but does not deal with the validity of identity.

In epSOS LSP, the identity of a patient will always have to be proven (validated) in his[1] country of affiliation, even if this process is initiated abroad in Country B. The process is very similar to the processes in the STORK project (see chapter 5.1 STORK – WP 7.3 (STepS)).

The identification of the Healthcare Professional will always happen in the country of his registration, most likely by referring to a HCP-Registry/Repository (Database). This process is very similar to the one which will be established by the HPRO project (see chapter 5.2 HPRO Card).

The *authentication* is the process of establishing an acceptable level of assurance that a claimed identity of an entity is genuine.

Authorisation is a part of access control. In general, authorisation is a process to assign the proper rights to an identified entity (person, system or process) to do or to use something. In the epSOS LSP environment, authorisation provides access control decision information for some access control mechanisms, controlling access to patient health data and other sensitive data. The access to patient's data in epSOS LSP is governed by epSOS LSP access control policy, based on the need-to-know principle. Active entities (actors) of epSOS LSP are categorised with respect to their tasks and positions in the epSOS LSP environment and standardized sets of privileges are assigned to each category (role).

epSOS LSP will use parts of a Policy-Based Access Control (PBAC) mechanism for the decisions which are not only based on the roles, but also on attributes (e.g. "Purpose of use", "Locality") and additional modified restrictions following from patient consent. Details of the model of "Access Control" will be defined by WP 3.3, WP 3.4 and WP 3.7.

Based on a decision made by PEB (made June, 30th 2009), patients will not have any direct access to the epSOS LSP environment. With respect to this decision the objectives and the scope of WP 3.6 are defined in a proper way.

2.2 Scope of WP 3.6

WP 3.6 is a link of a chain within epSOS LSP and takes the functional requirements of WP 3.1 ("Definition of ePrescription Services") and WP 3.2 ("Definition of Patient Summary Services") as input for the methods and processes mentioned above. On the other hand WP 3.6 defines functional requirements for WP 3.3 ("System Architecture") as well as for WP 3.4 ("Common Components Specification"), but cannot and should not cover all security aspects of epSOS LSP. Security services are mainly covered by WP 3.7 and a proposed Security Policy is part of the deliverables of WP 3.7. This document describes the mission of WP 3.6 as part of this chain and delimits the responsibilities of WP 3.6.

Models for "Integrated Information Security Management Systems" according to ISO/IEC 27001 (and Identity Management is a vital part of these models) can be expressed as a matrix, which uses the columns to address the terms to fulfil (the goals to achieve), and the rows to define the appropriate layers of fulfilment (a short description of the used terms can be found in chapter 12 Glossary).

[1] "He" stands for "he" or "she", "his" stands for "his" or "her", "man/men" stands for "man/men" or "woman"/women" throughout this document

From the perspective of WP 3.6 in epSOS LSP this matrix can be seen as follows (Table 1). It should give an overview of the different responsibilities and tasks of the Work Packages of epSOS LSP and show, which parts of a Security Management System have to be covered by WP 3.6 (blue lined area). Some of the responsibilities and tasks are overlapping or shared with other WPs of epSOS LSP, but they have to be described as a part of Identity Management to understand the whole processes and the interfaces between different systems and infrastructures.

An important interface exists between WP 2.1 and WP 3.6 due to the fact that “Authenticity” and “Confidentiality” are common terms to fulfil of both WPs (see Table 1). To achieve the common goals the issues around “patient consent” (which is a sensitive and complex topic in epSOS LSP) are addressed by WP 2.1 and WP 3.6 together.

Appropriate references to other Work Packages are included in this document, whenever necessary.

	Integrity	Availability	Authenticity	Confidentiality	
Juridical	• MS		• MS • WP 2.1	• MS • WP 2.1	National Security and patient privacy policies
Organisational	• WP 3.1 • WP 3.2	• MS	• MS • WP 2.1	• MS • WP 2.1	Network of trust
Procedural	• WP 3.1 • WP 3.2	• WP 3.3 • WP 3.4	• WP 3.6	• WP 3.6	Processes with respect to security policies
Administrative	• WP 3.5 • WP 3.7	• WP 3.3 • WP 3.4	• MS	• WP 3.6 • WP 3.7	Patient consent Risk management
Technical	• WP 3.5	• WP 3.3 • WP 3.4	• MS • WP 3.7	• WP 3.7	Security services
Physical	• WP 3.7	• WP 3.3 • WP 3.4	• MS • WP 3.3	• WP 3.7	Secured infrastructure and communication

Table 1 - Security model and responsibilities

2.3 Approach of WP 3.6

The requirements laid on epSOS LSP identity management in “Annex I” (taking into account the solutions and restrictions of national eHealth domains of participating MSs) exceed the framework of pure Identity management and need to include selected functions of access management, too. Therefore, the present document (though entitled Identity management) defines the following terms for epSOS LSP:

- Entities (see chapter 3.1 epSOS LSP entities)
- Identity (see chapter 3.2 Identity)
- Domains of applicability (see chapter 3.2 Identity)
- Identity information (see chapter 3.2 Identity)
- Roles (see chapter 3.1 epSOS LSP entities)

The scope for WP 3.6 is to describe the following fundamentals for the epSOS LSP entities HCP, HCPO, patient and health data administrator

- Identification (see chapter 4.1 Identification)
- Authentication (see chapter 4.2 Authentication of actors and 4.3 Authenticity and Integrity of documents)

- Authorisation (see chapter 4.5 Authorisation)

It describes procedural and administrative issues related to a specific security function used for authorisation, namely

- Patient consent (see chapter 3.3 Patient consent)

And finally, it elaborates the requirements on

- Audit trail (see chapter 4.7 Audit Trail and Audit log records)

To achieve the global security goals of the epSOS LSP environment formulated in “Annex I” (Part B 3.6.) access management - controlling the use of system resources and access to sensitive data - is a cornerstone of the epSOS LSP security architecture.

Identification and authentication of entities are the basic security functions of access management and access control.

Various services and components of the epSOS LSP environment require univocal, unambiguous identification and/or reliable authentication of different entities; moreover some transactions associated with identification/authentication take place in systems belonging to the national e-health infrastructures, which are not part (not under direct control) of the epSOS LSP environment. Since the results of identification/authentication are crucial for epSOS LSP fundamental functions WP3.6 has to

- Identify the cases, where identification and authentication are required on both, the national (local or national systems in the national e-Health domain) and the international (in the epSOS LSP environment) levels,
- Assemble the information on identification/authentication solutions used in different MS,
- Identify the restrictions, legal requirements and other relevant factors influencing the use of identification/authentication solutions in MS.

The last task must be solved in cooperation with the legal/juridical experts group of WP 2.1.

3 Terms and Definitions

The use of appropriate security functions in epSOS LSP will be described in more detail in the following chapters of this document. The following explanation of terms (used in this document) is not meant to replace a glossary, but to illustrate some of the more abstract terminology with examples in respect to the epSOS LSP environment.

3.1 epSOS LSP entities

Persons (physical or legal), technical devices, systems, documents, data, etc. are called *entities.* From a functional point of view, entities can be separated into active entities (actors) and passive entities (*actors*).

Actors can perform various activities in the epSOS LSP. This document concentrates on activities directly referring to access control of patient's health data and does not deal with activities concerning the technical systems operations (like national authorities, national NCPs, local systems, etc.). They are out of scope of epSOS LSP and this document. The necessary security requirements for epSOS LSP environment operation are formulated in deliverables of WP 3.7.

3.1.1 Active epSOS LSP entities

Examples for active epSOS LSP entities are patients, HCPs, health data administrators, NCPs and computer systems as part of the epSOS LSP environment. Some entities can be either passive or active depending on the actual situation. This document deals primarily with epSOS LSP active entities (actors).

Formally, *a role* is a special attribute that cannot be used for identification/authentication, but specifies the activities permitted or allowed to an entity in a domain of applicability.

A role in epSOS LSP implies that an entity has or gets a collection of privileges to access or use resources available in the epSOS LSP environment.

3.1.1.1 Medical roles in the EU

"Health care professional" (HCP) means

- Medical doctors,
- Nursing professionals,
- Dental practitioners,
- Midwifery specialists or
- Pharmacists

within the meaning of Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications or another professional exercising activities in the healthcare sector, which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC.

3.1.1.2 Medical roles in epSOS LSP

Agreed between WP 3.5 and WP 3.6 the epSOS LSP will use the following detailed roles[2] for Healthcare Professionals in identification, authentication and authorisation processes. A role in

[2] If necessary, more roles can be used in national e-Health domains but when using epSOS LSP **services,** they must be mapped to epSOS LSP roles

epSOS LSP implies that an entity has or gets a collection of privileges to access or use resources available in the epSOS LSP environment.

- Medical Doctors
    - Generalist medical practitioners
    - Specialist medical practitioners
- Nursing and Midwifery professionals
    - Nursing professionals
    - Midwifery specialists
- Pharmacists

This list of roles can or should be extended after the pilot phase. A special role is used for the organisation of the HCPs (HCPO), but is not used in the processes within this document.

3.1.1.3 Non-medical roles in epSOS LSP

Other important roles in the epSOS LSP are

- Patient
- Medical data administrators and
- NCP

External service providers may be involved in some processes, but they are out of scope of epSOS LSP or WP 3.6

3.2 Identity

An entity can be characterized by its special features (physical appearance, properties, states, status) called *attributes*. A set of entity attributes is called *identity.* A complex entity like a person can have a very large set of attributes. For practical reasons, only particular attributes in collaboration are used as identities. An entity can have various identities. Since an identity contains only some of the attributes of an entity, it is not universal. When an entity is linked with a specific *domain of applicability*, this identity can be identified within that specific domain of applicability, but it may not be sufficient for identifying the entity outside of that specific domain of applicability.

The most important entities of epSOS LSP system are human beings (patients, HCPs, administrators, etc). In a family, every member can be characterized by his appearance, voice, etc. In a small collective like a class, the pupils can be distinguished by their surnames. If there are two pupils with the same surname, the given name can be added to their identities. To identify a person in a large population, other attributes like the date and place of birth, address, etc. must be used to the identity.

The information contained in an identity is called *identity information.*

Example: Daniela Altenberg, born 29.12.1979 in Vienna, Austria, father Gottfried Altenberg (*6.6.1953), mother Elisabeth Altenberg (*6.3.1956, maiden name Eugenie) address of residence Vienna, Castle of Schönbrunn, No 1.)

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.)

There are many non-human entities in the epSOS LSP. The most important of them are documents in electronic form, which are of course always linked to a human entity.

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.

3.3 Patient consent

Patient Consent is the "*freely given specific and informed indication of the patient's wishes by which he signifies his agreement to personal data relating to him being processed*". This definition is laid down in Art 2(h) of the Data Protection Directive (1995/46/EC) referred to herein as DPD[3].

Since health data contain sensitive information[4], both participating countries (A and B) usually have a legislation generally governing the processing of health data (National Security Policies (NSP) and Patient Privacy Policies (PPP) and the cross border transfer of health data in particular (for further information refer to the deliverables of WP 2.1 and chapter 6 Analysis and review of Identity Management in participating MSs). Moreover, every patient has the right to restrict or to permit the access of his health data. The patient's prohibition or permission is called *patient consent.* In the epSOS LSP, patient's consent for the cross border transfer of health data is an important part of the authorisation process. The regarding processes and the interdependencies with the roles mentioned above, are introduced in chapter 4.5 Authorisation and described in detail in chapter 7 epSOS LSP identity management, authentication, authorisation and audit.

Every patient ought to have the possibility, to modify the previous value of his patient consent. Which elements or restrictions will be modifiable by the patient, has to be defined by WP 2.1 in detail. Other important parameters, like duration of validity of patient consent during a treatment process, have to be defined by WP 2.1 as well.

Depending on national laws, patients in epSOS LSP can use Opt-In and Opt-Out consent. The modalities of how this consent is referenced (internally and abroad) and where and how this information is stored, are part of the responsibilities of Country A, the country where the patient is insured (definition of WP 2.1).

The administration of patient consent in Country B has to be done at a Point of Care. In Country A the administration is usually defined by national regulations.

Note: "YES" and/or "NO" in the next chapters mean that consent is "given" or "not given yet".

[3] Given that this is a rather precise formulation which has been further clarified in the recitals of the Directive as well as in subsequent opinions of the Data Protection Working Party, the definition and handling of patient consent is not expected to vary significantly across Member States

[4] Health related data falls under 'special categories of data' which are granted specific protection under article 8 of [Dir95/46/EC]

3.3.1 Patient Consent in epSOS LSP

epSOS LSP patient's consent is a pre-requisite, not for collecting health data for the purposes of providing medical care in the Point of Care (PoC) by a health care professional in country B, but for the purpose of accessing already existing data in the country of residence (Country A). Two processes can be distinguished for which patient consent is needed – one for providing medical service per se, the other for realizing the epSOS LSP "business case" as a specific processing of already existing personal data.

3.3.1.1 Consent for collection and processing of patient's data for medical services, treatment, diagnosis, and similar purposes:

In this process, patient's data are collected and stored in the patient's health record and they are further used for providing health care. Personal data are obtained directly from the patient, or as results of laboratory, diagnostic and other investigations. Patient Consent in this case is regulated by each particular epSOS LSP country and legislation of the country where data is created is applied. This consent does not grant agreement to access to the patient's data from abroad.

3.3.1.2 Consent for the creation of an epSOS LSP summary

In some MS where the epSOS LSP record is created specifically for the purposes of epSOS LSP out of existing stored records, it will be necessary to obtain patient consent locally in Country A for the creation of the epSOS LSP summary

3.3.1.3 Consent for access to patient epSOS LSP patient summary and ePrescription data from abroad

In this processes, the consent is the patient's agreement to make accessible his/her epSOS LSP health data (already existing in his/her medical record, respectively extracted from this record into the medical summary record) to professionals providing care to the patient abroad.

It must be clear that if, for the purpose of providing care in another country, new health data is created, then this process is equivalent to case (a) above and is subject to Country B rules.

3.3.1.4 Principles for Patient Consent

1. The consent will be specific

- Patient consent is acquired for the creation of "epSOS LSP patient data", i.e. Patient Summary (including medication record), if the patient's resident country legislation requires it. This action will take place in Country A, this is therefore a requirement in each Country A associated to the establishment of a PS, which would be needed irrespective of the cross border exchange.

- Patient's consent is also acquired for access to epSOS LSP patient data abroad under the circumstances specified in the project. This is additional consent that should ideally be incorporated, as an opt-in option in the national patient consent procedure and documentation.
- A provision will be made to ensure that if a patient has not provided his consent for access to "patient data" from abroad, he still has the right of his epSOS LSP patient data to be created (for use in country A only).

2. The consent will be freely given.

- The patient has a free choice to participate in the epSOS LSP without any subsequent restrictions or negative influence to receiving all necessary medical treatment or any other medical services.
- Patient may withdraw his consent at any time.

3. The consent will be informed.

- The patient will be informed:
  - On the aims of the epSOS LSP, how his patient data will be used, on his rights and any other circumstances of the processing of his data for the epSOS LSP purposes.
  - That his consent is free without any consequences if the consent will not be given.
  - That the collection and further processing of patient's health data solely for providing medical services, is a subject of legislation of a country in which medical care is provided.

- This information will be drafted as part of Annex II of the FWA and will be localised in each country, preferably as an addendum to the national standard information provided to patients for acquiring consent.
- The information will reside in the epSOS LSP NCP(A) and will, if required, be made available to the patient when he is in country B.

3.3.2 Where is Patient Consent provided

From a legal and regulatory perspective, in a trusted domain environment, consent may be provided in any territory of location within the trusted domain, under auditable, verifiable and conditions conformant to the epSOS LSP Information Governance.
Consent to create the PS is obtained in Country A, as well as a general consent to sharing the record in a putative Country B. That consent is then confirmed, once the patient is in situ in Country B.

3.3.3 Opting IN consent

Opt-In within the context of the epSOS LSP means that (by default) remote access to patient's data from abroad is forbidden, unless the patient explicitly allows it. If a patient assumes, he will need a health service requiring some of his health data during the visit in a foreign country (Country B) and his home country (Country A) is adopting Opt-In policy, he administrates his consent for Country B, before the journey and change the default "NO" to "YES". If a patient does not register his positive consent, NCP A will not provide any health data to the NCP (HCP) of Country B.

3.3.4 Opting OUT consent

The opposite of Opt-In policy is the Opt-Out policy. Opt-Out within the context of the epSOS LSP means that (by default) remote access to patient's data from abroad is allowed, unless the patient explicitly denies it. If a patient is afraid that his health data can be compromised or misused during his stay in a foreign country, he can deny access to his data by replacing the general "YES" by a particular "NO" in the corresponding patient consent for Country B. Without previous denying the remote access to patient's health data from Country B, HCPs from Country B can require at least the patient summary.

Further information on patient consent can be found in the epSOS LSP Concept paper on patient consent.

The processes for modification of patient consent are described in chapter 7.5 Patient consent management.

3.4 Level of trust

Within the epSOS environment HCPs must be able to rely on the authentication of other entities by an Identity Provider (IDP). To establish trust, certain security requirements must be met, depending on the role of the epSOS actor.

The level of trust is based on authentication and the quality of attributes[5] and must encompass all relevant factors that drive these qualities:

- The assurance level of the registration phase, (identity and attribute proofing, credential issuing, quality of the registration authority)
- The assurance level of the electronic authentication phase (like token quality, authentication protocol, platform security)

The relying party has to place sufficient confidence in the authentication and attribute assertions which will be set up by the MS according to the annex “Security Policy” of the pilot site agreement.

REQ 3.6.1 Appropriate values for level of trust and their influence on authentication processes have to be defined by WP 3.7 (together with WP 3.3).

5 In this context of security objectives quality and assurance are used synonymously

4 Basic concepts

This chapter describes the commonly used fundamental processes and how the terms described above are used within them. The epSOS LSP processes (shown in chapter 7 epSOS LSP identity management, authentication, authorisation and audit) are based on the following concepts.

4.1 Identification

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

Examples:

- There are three men in a room (domain of applicability) two doctors: Elisabeth and Daniela Altenberg and a patient, Daniela Altenberg. The identities: doctor, Doctor Altenberg, Daniela Altenberg are not sufficient to recognize the entity doctor Daniela Altenberg (and the identification based on every of these incomplete identities fails).
- Another example of identification: for a large amount of unordered papers, the identification of presented identity information “document in a large manila envelope” means to search the papers and the result of identification will be positive if there was just one such document, otherwise the identification fails.

4.2 Authentication of actors

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.

A*uthentication* 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, which can then be used for authentication to prove that the person with a specific name or national identification number is really a resident of a particular country, and probably even the person holding the passport.
- Issuer of ID cards, service cards, membership certificates (ITIC, ISIC, etc.) - these institutions use the results of other identity authorities for identity management in a specific domain of applicability.
- University. Issuing a diploma, it confirms that the graduate has successfully accomplished a university study and gains a Master of Science title.

Within the epSOS LSP environment existing identity authorities can be used within identification and authentication processes.

4.3 Authenticity and Integrity of documents

Other important kind of nonhuman entities (objects) within epSOS LSP which ought to be distinguished are documents. The authenticity (genuineness) of a document is guaranteed by its issuer/producer (e.g. Hospital Information Systems (HIS), CIS (Clinical Information Systems), who uses various protective measures to minimize the probability of forgery or modification (like digital signatures).

Many important epSOS LSP documents will exist only in electronic form. Authentication of such documents means the verification of the *document's origin* (who created the document and/or who sent this document).

The responsibility for technical issues for the authenticity of an epSOS LSP document and the responsibilities for administrative and technical issues for the integrity of the documents, belong to WP 3.7.

The authenticity of technical devices is important for the security of epSOS LSP system, but it is out of scope of this document and ought to be analyzed together with other security topics/issues of epSOS LSP[6].

4.4 Identification and authentication of other epSOS LSP entities

Patient health data is created, stored and processed (totally or mainly) apart from the epSOS LSP environment – in various systems of national (e-Health) domains. The sources of medical and other necessary information (e.g. the list of patient, HCPs, etc.) in national domains are called *repositories or databases*. The national domains of MS will be connected to the epSOS LSP system by *National contact points* (NCPs**),** which will serve as interfaces (gates or proxies). (See Figure 1) Since all epSOS LSP communication among HCPs from different countries will run through NCPs, every NCP must be able to prove his identity and to validate the identity of his partner (another NCP**),** before engaging data exchange and sending the required data.

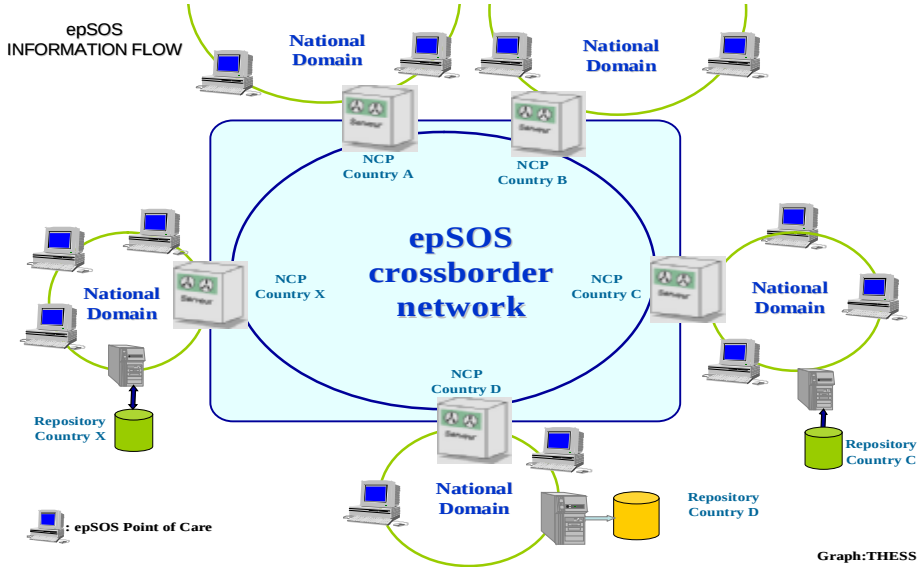

Figure 1 - The epSOS LSP system global topology (taken over from WP3.7, reference: [2])

Successful authentication of epSOS LSP entities means that epSOS LSP actors (patients, HCPs) can rely on documents they are receiving and can also trust the identities of other epSOS LSP partners, human and non human alike (e.g. NCP, HCPO).

[6] The security requirements on epSOS LSP identified by WP 3.6., which are to be analyzed or fulfilled by other WPs or national domains, are summarized in chapters 8 and 9.

4.5 Authorisation

Since the “need-to-know” principle is one of the cornerstones of epSOS LSP, an actor is only able to access the epSOS LSP services and resources that are required for the completion of his duties. To enforce this, a temporarily approved set of privileges (determining the services or sources an actor can use) is allocated to the authenticated actor. This process is called *authorisation*.

4.6 Health data transfer

The epSOS LSP services defined by WP 3.1 and 3.2 include the transfer of sets of agreed data, particularly, a *patient summary*, that includes also a *medication summary* and data related to the *ePrescription* (prescription and dispensation). Most of the data included in those sets correspond to health data and therefore these documents are referred to as health data.

Utilising epSOS LSP services to access health data is contingent on successful identification and authentication of the health care professional, the identification of the patient, the fact that the epSOS LSP system “knows” the appropriate documents and the requestor is assigned to a role which is authorised to gain access to epSOS LSP. The second authorisation factor is patient consent, which determines which role or roles of HCPs in Country B may have access to patient’s health data and what portion of the health data can be retrieved from Country A.

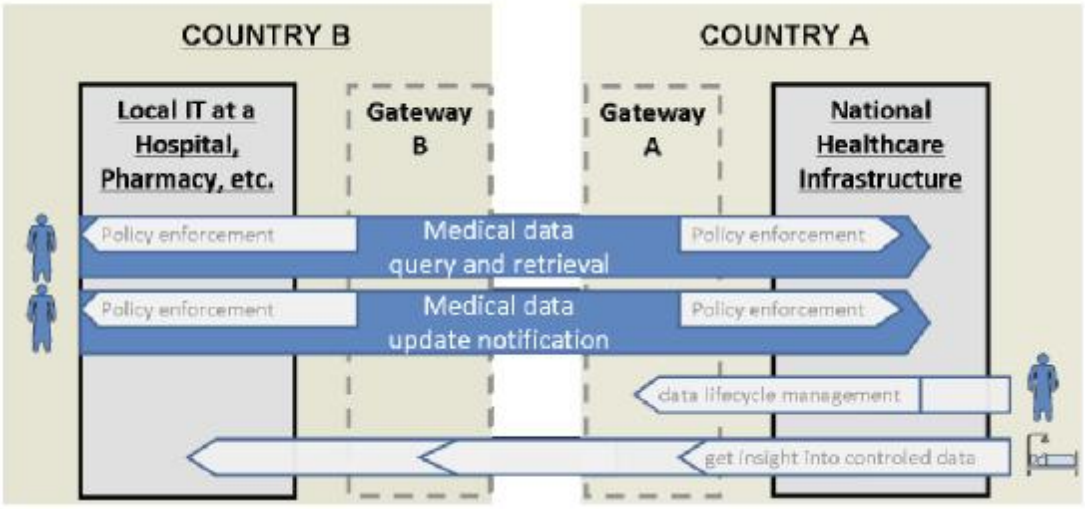

Figure 2 - The flow of health data (taken over from WP3.3, reference:[3])

4.7 Audit Trail and Audit log records

Health data processed by epSOS LSP contains sensitive information, the protection of which is required by EU legislation, national laws, and epSOS LSP security policy. Besides of various security functions of epSOS LSP system designed for information protection in general and the protection of health data in particular, “Annex I” required accountability based on auditing. For every transaction (requesting, sending, processing, receiving sensitive information) or security relevant event (authentication and/or authentication change of epSOS LSP system parameters), identity management transactions, etc. a record describes who has done what and when. Such records are called *audit logs* and provide useful evidence for a potential investigation of security incidents, which can take place in epSOS LSP system.

WP 3.6 defines audit record events for HCP and patient authentication. In particular, it defines when audit log entries are created. WP 3.7 defines all other security relevant audit log entries and the requirements for the data collection infrastructure.

The formal definitions of the above mentioned and other important terms can be found in the Glossary (Chapter 12).

5 Interdependencies to other EU-Projects

In parallel to epSOS LSP WP 3.6 other EU-Projects are working on related issues. In joint workshops of WP 3.6 and members of the following mentioned EU-Projects, common issues and reusable parts were identified. Due to the fact that these projects are at comparable stages (before or just starting piloting phase), it can be assumed that some processes defined by these projects will help epSOS LSP in the future. Right now, estimations about timeframes or schedules cannot be proposed.

Some other projects with similar content, without any assessment from WP 3.6, are listed in chapter17 Annex II Additional EU Projects

5.1 STORK – WP 7.3 (STepS)

Link: http://www.eid-stork.eu

STORK aims to develop, test and validate common specifications and its reference implementations to identify and authenticate citizens from EU member states, using electronic identity (eID) methods already available in the individual countries.

These methods *inter alia* include

- Smart cards
- Username / password combinations
- “Mobile TAN” (one-time access code sent to user’s mobile phone via SMS)

Two interoperability models and their combinations are investigated and piloted: Pan-European Proxy Services (PEPS) are central eID proxies, provided by Member States for their citizens. The second model is the middleware model, where a middleware couples the eID with the service provider. It is a Member State’s decision, which model to implement.

The concept of “Pan European Proxy Services” (PEPS) maps to the epSOS LSP concept of National Contact Point.

In the individual MS where eID methods are already available, STORK can be used to authenticate users for the use of cases involving / giving / revoking consent and defining / deleting / modifying privacy policies. In these cases, epSOS LSP can probably use identifiers linked to health insurance (e.g. those defined by EHIC), because this data management is an administrative process and is not health-related.

Concerning the remaining use case requires to authenticate the patient (access to the patient’s own patient summary), nevertheless the restriction that in some countries it is forbidden to use insurance-related identifiers to access health-related data (like the patient summary) needs to be taken into account.

If an insurance number is used for identification, it has to be considered that more than one single person can have the same numbers in some countries (e.g.: children have the insurance number of their parents). In such situations another database has to be used for univocal identification.

STORK defines “quality assurance levels” that are defined depending on the eID token and issuance processes. E.g. a smart card will yield a higher level compared to username-passwords. The service provider defines a minimum security level that is needed for a particular service. For "harmless" services lower levels might be sufficient, whereas eID with low levels may be denied access for sensitive services.

These security levels could be used to give better protection to sensitive parts in epSOS LSP. E.g. updating data could require a different security level than reading them.

5.1.1 General positioning of STORK and epSOS LSP

STORK	epSOS LSP
The basic use case in STORK is to authenticate a citizen in his country of affiliation to a relying party in country B. The citizen's unique identifier may be used by the relying party to access related data. Authorization is not within the scope of STORK.	epSOS LSP use cases do not require the relying party in country A to know the identity of an HCP/HCPO in country B, but to rely on the assertion of a particular role. (Obviously the identity is recorded for audit purposes). Identification and authentication is an issue of the national infrastructure. epSOS LSP relying parties acquire roles needed for the authorization from the IdP.
Although not limited to, the pilot use cases imply a focus on Browser-based clients as described with the SAML Web-Browser SSO use case.	epSOS LSP use cases are from the class of messaging/document exchange, like described in the OASIS Webservice Security profile. There is no direct interaction between clients and service providers, but NCPs act as reverse proxies, opposed to the Web-SSO-model.
Depending on the model, the circle of trust (CoT) is either hierarchical (PEPS on MS-level and national) or flat with the middleware approach.	The CoT is strictly hierarchical, with the NCPs forming the epSOS LSP-level CoT and MS with the HCP on the national level.
Defined by the application's requirements, there are 4 different assurance levels for the authentication quality, based on the factors of registration and authentication phase.	Trust levels can be taken over from STORK, but will be tuned to the capabilities of the epSOS LSP actors of the MS participating in the LSP.

5.1.2 Possible synergies between STORK and epSOS LSP WP 3.6

The only process where synergies could be identified, is when a patient has to be identified and authenticated abroad and uses an eID (see chapter 7.3.2.2 Identification and authentication of a patient with a unique identifier).

Excerpt of a document of STORK

Patient Country A – PoC (eID)

> *The eID cross-border identification case fits the STORK process models well. As STORK distinguishes two models "middleware" (used by Austria and Germany) and a "Pan-European Proxy Service (PEPS)" (used by other member states), synergies with both models are discussed:*
>
> - *PEPS: The epSOS LSP process flows are basically the same as the STORK PEPS authentication flows. A difference that is given is that the STORK PEPS model assumed that actual authentication of the citizen (patient) is carried out by the Identity Provider in Country A.*
> - *Middleware: The STORK Middleware model assumes a so-called "virtual IDP" installation at the "Country B" PEPS. The IDP carried out the authentication of the citizen. Assuming such a V-IDP at NCP B, the process flow is the same.*

Further collaboration between STORK and epSOS LSP has to be investigated in the piloting phases of epSOS LSP.

5.2 HPRO Card

Link: http://www.hprocard.eu

HPRO Card is a project to study authentication of HCPs. The HCP authentication is based - first - on the HCP registration by the competent authorities (as defined by the Directive 2005/36/EC) and on certified data by Certification Authorities in each MS.

HCP may be

- a doctor of medicine,
- a nurse responsible of general care,
- a dental practitioner,
- a midwife or
- a pharmacist

within the meaning of Directive 2005/36/EC. The HCP must be related to at least one HCPO or to a Health Authority belonging to the country that could univocally identify him or her.

In its current version, already existing national professional identity cards of HCPs will be equipped with a uniform backside layout, which states (in English and the local language) the profession and the contact data of the competent authority which issued the card. The contact data can be used to inquire at the authority, if the professional is well registered and isn't under sanction in his own country.

HPRO Card can give epSOS LSP valuable input on the organizational structure of the competent **authorities,** which control the activities of HCPs in the individual member states.

5.2.1 Smart cards

For existing HCP professional chip cards, the verification of the card's validity and the authentication process will be provided through classic electronic certificate usages. 9 countries are already equipped with such cards: Austria (pharmacists and doctors in contract with social insurance), France (all professions), Germany (doctors), Hungary (doctors), Italy (Lombardy: all professions), The Netherlands (all professions), Slovenia (all professions), Spain (3 regions: doctors), Sweden (all professions).

Some countries have concrete short term projects: Belgium (pharmacists), Finland (all professions), Hungary (all professions), Ireland (pharmacists), Slovakia (all professions), Spain (pharmacists) and Switzerland (doctors).

HPRO Card has received a lot of answers from the different existing certification authorities through a questionnaire where epSOS LSP specific questions were added. The overall data will be provided to epSOS LSP as soon as the countries will have expressed their consent for this sharing.

5.2.2 Possible synergies between HPRO Card and epSOS LSP WP 3.6

Processes where synergies could be identified are when a HCP has to be identified and authenticated in Country B.

Further collaboration between HPRO Card and epSOS LSP has to be investigated in the piloting phases of epSOS LSP.

5.3 NETC@RDS

Link: http://www.netcards.eu

NETC@RDS is particularly interesting, because it is more mature than the other projects.

The aim of NETC@RDS is to verify, if an EU citizen is insured in the country of origin. This is not directly related to epSOS LSP, but epSOS LSP can reuse some parts and processes that are used to identify the patient:

- The European Health Insurance Card (EHIC). Currently this is a human-readable card (not a smartcard). However, a specification for a corresponding smartcard has been drafted and will be implemented in the near future. epSOS LSP can use it in follow-up projects.
  The current version of the EHIC can be very valuable, but for identification processes which can be used EU-wide the EHIC number must be a combined data set ("Personal identification number of card holder", “Issuing state ID number" and "Identification number of the institution") to be definitely unique.
- A software package which enables HCPs in Country B to read national health-insurance smartcards from Country A. This obviously works only for citizens whose country of origin uses smartcards, and only if HCPs in Country B use card readers. However, the number of countries basing their health insurance systems on smartcards is continually growing, so this solution will become more common and important in the future.
- The input data structure of a web service to check the patient’s insurance status. Again, the web service itself is of little value for epSOS LSP, but the input data structure which identifies the patient has been agreed by many EU member states and should be sufficient for epSOS LSP.

As mentioned in chapter 5.1 STORK – WP 7.3 (STepS)**,** an obstacle to reuse results from NETC@RDS is the restriction to link insurance- and health-related data. This might be solved by using an irreversibly encrypted EHIC identifier directly in epSOS LSP. However, it has to be checked if this satisfies the legislation in all member states. If this is the case, the usage of NETC@RDS web service or at least its input data structures, combined with the card reader software, to identify patients could be valuable for epSOS LSP.

5.4 PEPPOL

Link: http://www.peppol.eu

PEPPOL is a Large Scale Project in the area of eProcurement and it includes within its scope a cross-border validation service for eSignatures. As such, PEPPOL might be interesting for epSOS LSP to the extent that documents will need to be electronically signed and signatures will need to be verified across countries.

Regarding eSignatures, PEPPOL sets up a registry server where trusted Validation Authorities (at least one in each country) are listed. Each Validation Authority in one country is responsible to support/validate a number of national Certificate Authorities (CAs).

In functional terms regarding service support, PEPPOL offers two validation models:

- Scenario A - Remote validation. The receiving country sends a request to the Registry in order to discover the appropriate Validation Authority in the originating country. It then sends a validation request to that Authority and receives back an assertion.
- Scenario B: Local validation: The originating country’s application asks the Local Validation Authority to supply an assertion that the signature is valid and legitimate. Then it sends the assertion to the receiving country, where it is trusted because it originates from a trusted Validation Authority

Apart from eSignatures, PEPPOL's core architecture of trusted service points may be of relevance to epSOS LSP definitions of NCPs. This is mostly a WP3.3/3.4 and WP3.7 issue although some architectural aspects such as authentication tokens etc. may be directly relevant to WP3.6

5.5 SPOCS

SPOCS is the Large Scale Project which is starting in 2009 and is concerned with the implementation of the Services Directive. Given that the HCPs are not part of the Directive's scope, it is perceived that SPOCS would not offer to epSOS LSP any added value regarding HCPs over what HPRO is doing.

6 Analysis and review of Identity Management in participating MSs

In order to provide a highly-integrated and smooth operating technical architecture / infrastructure, while constantly applying adequate security and monitoring means, the current situation, national requirements, and specific capabilities of the participating Member States have been determined by several questionnaires within this working package.

The individual answers by a representative of each Member State have been collected, preliminary analysed and were subsequently compiled into a comprehensive overview of what aspects are to be addressed by the technical, security, and architectural working groups.

This document presents the concrete results of the answered questionnaires and acts as the foundation for the respective security and architectural decisions taken for epSOS LSP. The individual requirements and constraints for each Member State were derived, compared to each other, and eventually generalised to facilitate a secure and legitimate cross-border communication.

The answered questionnaires for each Member State are also provided for reference purposes as an appendix to this document.

6.1 National Security Policy Specifics

The National Security Policy (NSP) is an umbrella security policy, which is applied to all access requests communicated through the specific national infrastructure. It determines what actors may access what information in what context. The questionnaire indicates that almost all Member States operate a NSP within their national infrastructures.

All Member States restrict any health data disclosure exclusively to HCP. Any potential exceptions for special actors, such as supervisory authorities and appointed specialists (e. g. quality control, financial/administrative/medical auditors, etc.) are out of scope of epSOS LSP.

Many Member States restrict the disclosure of medical information even further by regulating data access to certain types of medical personnel. This regulation is usually implemented by communicating not only identities of HCP but also their currently assigned roles. Referring to the answers of the questionnaire, the roles are based on functional aspects, such as the job title and the organisation of labour. Exemplary access regulations are:

- DE: physician, pharmacist, dentist, psychotherapist (with the option of delegating data access to their appointed assisting personnel)
- ES: physician, pharmacist, nurse
- FR: physician, pharmacist

6.1.1 Member State-specific Characteristics

Some Member States are imposing additional restrictions on any data disclosure attempt. In contrast to the rather coarse-grained role-based access operated by most national infrastructures, those countries base access decisions on more detailed or specific roles and treatment locations.

Member State(-s) affected	Constraint
AT	The access control decision requires the provision of additional attributes of the HCP, such as “GP”, “”Psychiatrics”, etc.
DK	The access control decision may also consider the organisational unit of the HCP.
NL	Only GP’s (and assistants with mandate) may have access to Patient summary. Pharmacists, specialists, GP’s (and assistants with mandate) may request dispensed

	drug data[7].

Table 2 - National security policy specifics

6.2 Patient Privacy Policy Specifics

Constraints and restrictions, which were put in place by the patient, are considered to build the Patient Privacy Policy (PPP). Almost all Member States grant the patients the right to impose further restrictions (additionally to those already defined by the patient consent and the National Security Policy) onto their health data, such as restricting who may access, when, or in what situation:

- opt-in[8] / opt-out[9] certain HCP roles: IT, DK, AT, ES, FR (by patient consent), (NL)
- opt-in / opt-out certain countries: CZ, IT, SK, ES, DK, AT, DE (by consent)
- opt-in / opt-out certain document parts: IT, SK, DK, AT, ES

The Member States, which do not implement specific PPP, usually implement the (resulting) technical authorisation through a health card. In this case, the patient may decide on his own whom he would like to authorise by passing over the health card.

Almost all Member States operate (or currently design) procedures for “breaking glass scenarios” in which an emergency data access is required. An emergency access may override the usual policy application and therefore may grant access to an HCP who was not explicitly authorised to access the health data. This may also apply to a part or all of data, which was hidden by the patient (with the exception of DE and SE). Due to the inconsistencies towards the hiding/revealing capabilities of health data, the access control decision for emergency access (with or without revealing hidden data) is to be fully performed at Country A based on the information provided by Country B.

Almost all Member States – but FR and SE for the epSOS LSP pilots – grant the patients the right to hide medical information. The concrete extent of the data hiding capabilities differs:

- exclusive (full) data hiding capabilities for all HCPs: ES, IT, SK, CZ,, AT
- conditionally (partial) data hiding for certain HCPs: AT
- a combination of both data hiding paradigms: DE, DK, AT

When health data is specifically hidden by the patient, most Member States do not indicate the existence of any hidden data. Data hiding is only announced in DK.

6.2.1 Member State-specific Characteristics

Member State(-s) affected	Constraint
FR, SE, AT	Although data hiding capabilities originally exist for those Member States, they are not granted during the epSOS LSP pilots.
IT	IT distinguishes between data hidden by the patient and data hidden by national law.
DE, SE, AT	Even an emergency data request may not reveal any hidden health data.

Table 3 - Patient privacy policy specifics

6.3 Patient Consent Specifics

The concrete design regarding the appropriate reflection of the patient consent as the legal foundation for any legitimate processing of health data within or when using the epSOS LSP

[7] This constraint describes the current situation (2009) in NL. In future steps authorisation for PS is based on the actual role of a HCP
[8] opt-in: inclusion of the aspect needs to be explicitly authorised by the patient and is declined by default
[9] opt-out: inclusion of the aspect is authorised by default and must be removed explicitly by the patient

services, has been a constant issue for discussion. In order to facilitate the design of secure and smooth operating technical solutions, the questionnaire compiled a set of questions regarding the individual composition and configuration of patient consents.

Almost all Member States require the patient to specifically state their agreement to the initiation of any epSOS LSP service prior to any service operation or health data processing. Those Member States also require the patients to explicitly manifest their agreement (based on an expression through “free will”) by a signed declaration, either by wet signature (common ink signature) or by a digital signature (if already provided and fully supported by a Member State). Since the majority of Member States use a wet-signature-based (paper based) approach to collect the patient consent, the specific and full contents of those consent documents may not be processed digitally, however their existence can.

Most member States have legal procedures and constraints in place, which define what information must be declared / included in the patient’s consent and how the consent document is processed, stored, and archived.

Spain is using a different approach regarding the patient consent. Indeed, consenting to the access of health data is assumed implicitly, whenever the patient is seeking for care at a point of care that belongs to the public National Health System. Therefore no additional technical or organisational means are implemented to register or archive this patient consent.

Many Member States allow the patient to add additional constraints into the consent document, such as restrictions on which country may access, what HCP may process what data, and when data processing is allowed.

All Member States assume and demand up to some degree, that a patient consent is given at a Point of Care. Although most Member States assume, that the patient consent is generally given in the “country of affiliation” of the patient, no Member State reported this as a concrete legal requirement. Prospectively, a patient consent for the epSOS LSP services may be given in any participating country.

Naturally, all countries fully respect the requirements as stated in the European Data Protection Directive regarding the “informed” character of the patient consent. It is also possible for the patient, to withdraw the consent at any time.

6.3.1 Member State-specific Characteristics

Member State(-s) affected	Constraint
AT	In contrast to the other Member States, more than one consent document may exist.
AT, DE, DK, SE	The consent may define further restrictions, such as document types, time validity, certain persons, groups, data types, and restrictions what countries may access.
DK	The consent may be stated orally by the patient, however must be properly documented by the HCP.
ES	Implicit consent whenever a patient seeks health care.
IT	Whenever Italy acts as Country B, the HCP must explicitly prove the existence of a valid patient consent.

Table 4 - **Patient consent specifics**

7 epSOS LSP identity management, authentication, authorisation and audit

7.1 Introduction

Identification and authentication as well as authorisation are not only necessary security functions of the epSOS LSP environment explicitly defined in Annex I, but their successful completion is the explicit precondition of various other security functions, as mentioned in chapter 4 of this document. Without unambiguous identification of a patient, necessary documents of a specific patient can hardly be found. Without strong authentication of HCPs the privacy of patient data cannot be guaranteed and the audit log cannot help to maintain the accountability in the epSOS LSP environment. Requirements on identification and authentication explicitly defined in various epSOS LSP documents (the deliverables of WPs) covered both identification and authentication in the epSOS LSP environment and in national domains, too. This part of the document is based on specifications of epSOS LSP environment, on analysis of national solutions and restrictions (technical and legal); it contains the short description of identified cases (where identification or authentication is requested/needed) and provides analysis and the rationale of the possible solutions. This document concentrates on identification (and authentication) issues in the epSOS LSP environment *per se.* Other important identity management topics, which are located outside of the intrinsic epSOS LSP environment – in national domains – are discussed in chapter 9 Requirements/Recommendations for National Sites of this document.
Since identity management is a part of access management, consisting of:

- Identity management,
- Privilege management,
- User authentication management,
- Control, Traceability, Monitoring, and Review of user access,

this document briefly mentions the relevant relations between the parts of access management and, especially, formulate the requirements on other security functions.

Chapter 7.2 defines the scope of Identity management in the epSOS LSP environment and in national domains.

Chapter 7.3 identifies basic scenarios and describes the possible solutions of epSOS LSP entities identification and authentication.

Chapter 7.4 deals with authorisation. The authorisation in epSOS LSP is based on roles and patient consent.

Chapter 7.5 is devoted to patient consent. It describes both default solutions (Opt-In and Opt-Out) and various scenarios on how to modify previous patient consent.

Chapter 7.6 concentrates on logging; namely on creating and processing audit log entries in epSOS LSP.

7.2 Identity management responsibilities

Identity Management in general relates to the issuance, administration, and use of identities of entities known in a particular domain of applicability, which is in this case the epSOS LSP environment (together with national eHealth domains of MS participating in this project). The epSOS LSP environment is a set of National Contact Points communicating by means of public networks. NCPs are interfaces or proxies between national eHealth domains (for detailed specifications of NCPs refer to the deliverables of WP 3.3, WP 3.4 and WP 3.7). These national eHealth domains are not under direct control of epSOS LSP but WP 3.6 defines requirements and recommendations for them (see Chapter 9 Requirements/Recommendations for National Sites).

Patient data and identities of patients, HCPs, HCPOs are placed in registries, repositories or databases in national domains and most of data processing takes place there. Therefore it must be distinguished between processes running in the intrinsic epSOS LSP environment and the

processes running partially or totally outside the intrinsic epSOS LSP environment within the national domains.

The intrinsic epSOS LSP identity confirming and forwarding covers the following points

- Management of selected identity datasets and/or identifiers
  - of single persons (HCP, patient)
  - of a group of persons (legal entity of healthcare providers, e.g. HCPO)
  - of single documents (patient consent)
- Management of outgoing requests for validation of provided identities within the "Circle of Trust"
- Management of incoming requests and responses to such requests
- A secure, trustworthy, and reliable acknowledgement and vouching for the correctness of information provided by the national infrastructure and the HCPs

National authorities and institutions from national domains will provide

- The accurate management of identities lifecycle, from the creation of identifiers of entities until they terminate,
- The accurate management of identity assurance, authentication of the identity information, and the assessment of the required level of risk assurance for collecting and using identity information (named "trust level" in the following descriptions),
- The accurate management of identity information at the level of the relevant identity authorities and
- The accurate management of local systems and/or services which support the "Circle of Trust" (NCP) [10]

REQ 3.6.2 The national authorities must run identity registers and provide necessary information to authorised epSOS LSP actors.

epSOS LSP and authorities/participants from national domains will together provide identification and authentication services.

7.3 Identification and authentication of epSOS LSP entities

7.3.1 Identification and authentication of HCP

A HCP is one of the key players in the epSOS LSP environment. He communicates with the patient, proofs patient's identity against the identifier(s) provided by the patient, manages the communication with the epSOS LSP environment (e.g. entering data for the patient authentication process) and he requests access to patient's health data. To guarantee the privacy of patient data and the security of epSOS LSP transactions, reliable identification and authentication of HCP is unconditionally required.

The identification and authentication of a HCP takes place in the national eHealth domain of Country B (and is influenced by Country B legislation, standards and by HCPOs technical equipment and organizational rules) the principal steps of the identification and authentication procedures could be common for all MS participating in epSOS LSP project.

Entity	HCP
Identity	To be specified by MS

[10] NCPs need not to store information of HCPs, HCPOs and patients; it can retrieve information from national authorities (repositories, registers) and other services.

Identifier	Card, HCP personal code – see questionnaires
Identity authority	National organizations issuing ID cards for HCPs Certification authorities, issuing public key certificates and attribute assertion
Identity provider	• National organizations providing identities for entities by registering and distributing identifiers for entities.
Domain of applicability	MS of epSOS LSP
Claimant	HCP
Identity verifier	National domain
Relying party	NCP
Dependencies	Prerequisite of authentication

Table 5 - Identification and authentication of a HCP

The following parts of this chapter describe the variant processes of HCP identification, authentication and authorisation for epSOS LSP. These processes are completely under the responsibility of the MSs. The different variants are examples for the fundamental functionalities needed for a successful authorisation of a HCP for requesting health data from Country A.

For HCPs identification and authentication, the mechanisms and tokens considered in STORK Project and HPRO Card Project can be utilized.

7.3.1.1 Identification and authentication of a HCP with a unique identifier

This process describes how a HCP identifies and authenticates himself for epSOS LSP in his country (Country B**),** using a unique identifier. This unique identifier (e.g. stored on a smart card or a similar authentication token) is issued by a national authority in Country B. All other attributes linked to the identifier of the HCP are stored in the national infrastructure of Country B (e.g. national registry).

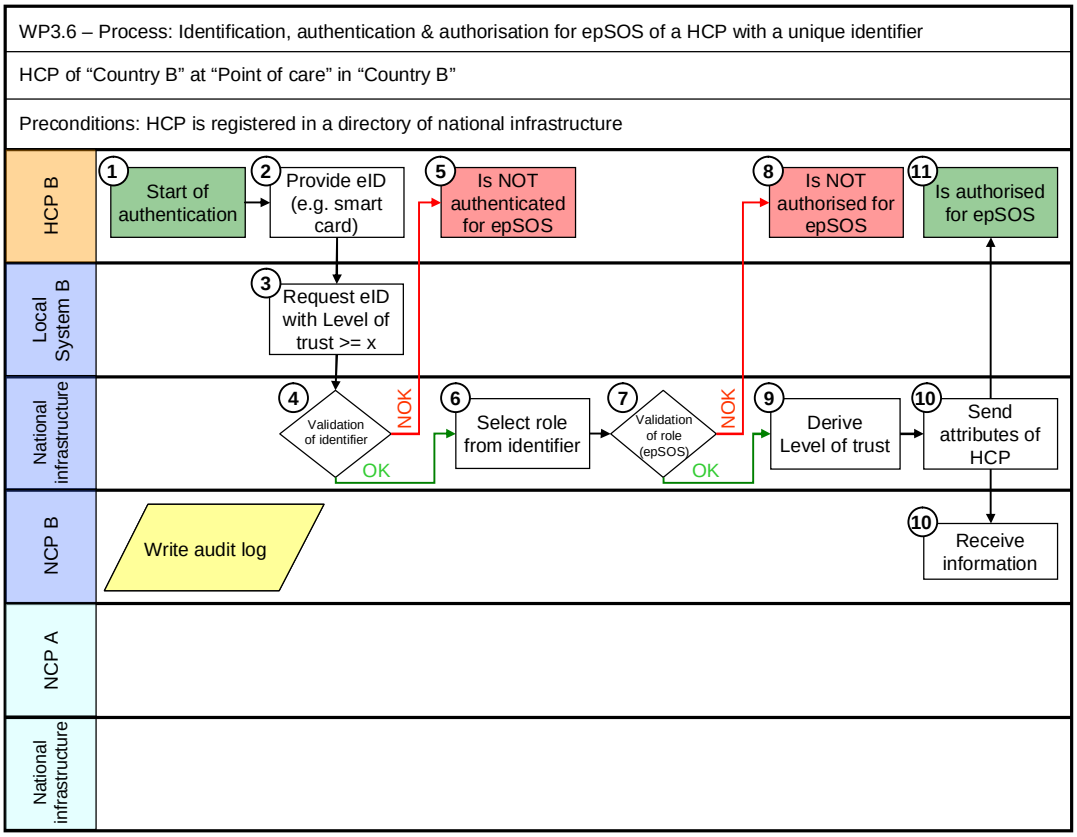

Figure 3 - Process of identification, authentication & authorisation for epSOS LSP of a HCP with a unique ID

The process in the above flow diagram (figure 3) consists of the following steps:

1. HCP is situated at a local system at a PoC in Country B, wants to identify and authenticate himself and wants to be authorised for epSOS LSP. This is the start of the identification and authentication process.
2. HCP owns a unique identifier (e.g. located on a (smart) card electronically readable or a human readable one) and provides it for identification and authentication purposes.
3. The identification and authentication method sets a request for identification with a level of trust not less than "x" (value of "x" has to be analysed by WP 3.7 and will be defined by national authorities, with respect to national legislation (see REQ 3.6.1)).
4. The provided unique identifier of the HCP is checked by the national infrastructure (e.g. validated by an appropriate verification service in Country B).

   One of the following results is returned:

   a. HCP is authenticated for the epSOS LSP environment (continue with step 6) or
   b. HCP is not authenticated for using the epSOS LSP environment.
5. If the HCP is not authenticated for the epSOS LSP environment an appropriate message is returned and the process is finished.
6. The national infrastructure selects the actual role of the HCP (see 3.1.1.2 Medical roles in epSOS LSP) out of the provided identifiers.
7. The actual role is checked against the predefined roles for epSOS LSP.

   One of the following results is returned:

   a. HCP's actual role is authorised for the epSOS LSP environment (continue with step 9) or
   b. HCP's actual role is not authorised for using the epSOS LSP environment.

8. If the actual role of the HCP is not authorised for the epSOS LSP environment, an appropriate message is returned and the process is finished.
9. The national infrastructure derives a value for the evaluated level of trust, based on the authentication method used.
10. This value must be kept - together with some of the extracted information from the identifier - for further processing. All the selected attributes of the HCP are sent to the NCP B for further processing in other processes.
11. The message about the successful authorisation is sent to the local system of the HCP. The process is finished.

7.3.1.2 Identification and authentication of a HCP using an internet portal

This process (not part of epSOS – but installed in some MS) describes the identification and authentication of a HCP for epSOS in his country (Country B) using an internet portal. A HCP has at his disposal identification, authentication and authorisation data or he can use a unique identifier as described before. These data are issued by a national authority (Country B) and are stored in the national infrastructure (national registry in Country B). The process of a HCP identification and authentication can be performed at any system (anywhere) in Country B (for details, see picture and descriptions below).

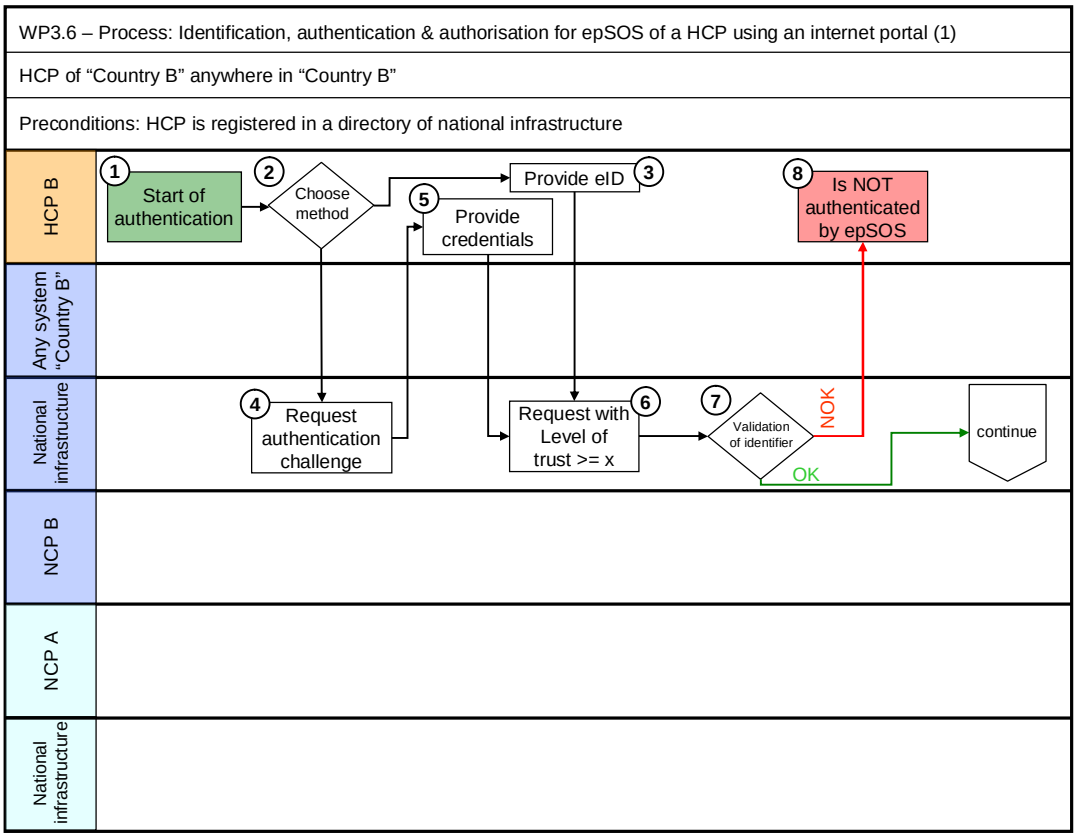

Figure 4 - Process of identification, authentication & authorisation for epSOS LSP of a HCP using an internet portal

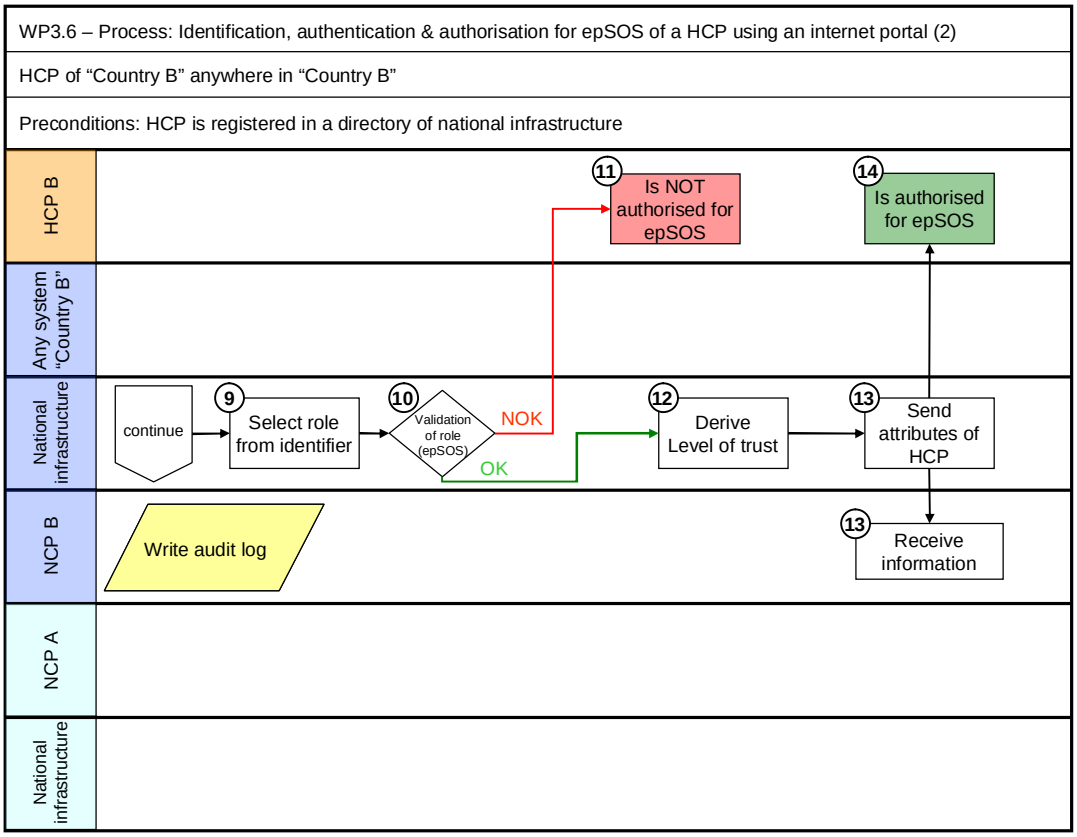

Figure 5 - Process of identification, authentication & authorisation for epSOS LSP of a HCP using an internet portal (cont)

The process in the above flow diagram (figures 4 and 5) consists of the following steps:

1. HCP is situated at any system in Country B, wants to identify and authenticate himself within the national infrastructure and wants to be authorised for the usage of the epSOS LSP environment using an internet portal solution provided by the MS. This is the start of the process.
2. HCP may be able to choose which identification and authentication method should be used: either the internet portal solution requests HCP‘s
    a. unique ID (continue with step 3) or
    b. logon data (continue with step 4)
3. HCP owns a unique identifier (refer to the process in chapter 7.3.1.1 Identification and authentication of a HCP with a unique identifier) and provides it for identification and authentication purposes (continue with step 6).
4. The internet portal solution is requesting an authentication challenge from the HCP.
5. The HCP responds to the authentication challenge as required by the authentication mechanism offered by the internet portal solution.
6. Both identification and authentication methods set a request for identification with a level of trust not less than “x” (value of “x” has to be analysed by WP 3.7 and will be defined by national authorities with respect to national legislation (see REQ 3.6.1)).
7. The entered credentials of the HCP are checked by the internet portal solution. A unique identifier of the HCP is authenticated (validated) by an appropriate verification service in Country B.

One of the following results is returned:

a. HCP is authenticated by the internet portal (continue with step 9) or

b. HCP is not successfully authenticated by the internet portal.

8. In the case that HCP's authentication fails the process is finished.
9. HCP is authenticated and authorised for using the internet portal. The portal solution provides the necessary information (authentication method and actual role) to the national infrastructure. The role of the HCP is selected from the attributes.
10. The actual role of the HCP is checked against the authorisation data stored in a national registry. One of the following results is returned:

    a. HCP is authorised for epSOS LSP (continue with step 12) or

    b. HCP is not authorised for epSOS LSP.

11. In the case that HCP's authorisation by epSOS LSP fails, the HCP receives an appropriate message and the process is finished.
12. The national infrastructure derives a value for the evaluated level of trust based on the authentication method used. This value must be kept - together with some of the extracted information from the identifier - for further processing.
13. All the selected attributes of the HCP are sent to the NCP B for further processing in other processes.
14. The message about the successful authorisation is sent to the local system of the HCP. The process is finished.

7.3.1.3 Identification and authentication of a HCP using a local system

The difference to the above described process is that this process of a HCP's identification and authentication is performed in two sub processes on different epSOS LSP environment layers. The first part of the process provides identification, authentication and authorisation of a HCP for and within a local system; the second part of the process provides identification, authentication and authorization of a HCP for the epSOS LSP environment within the national infrastructure.

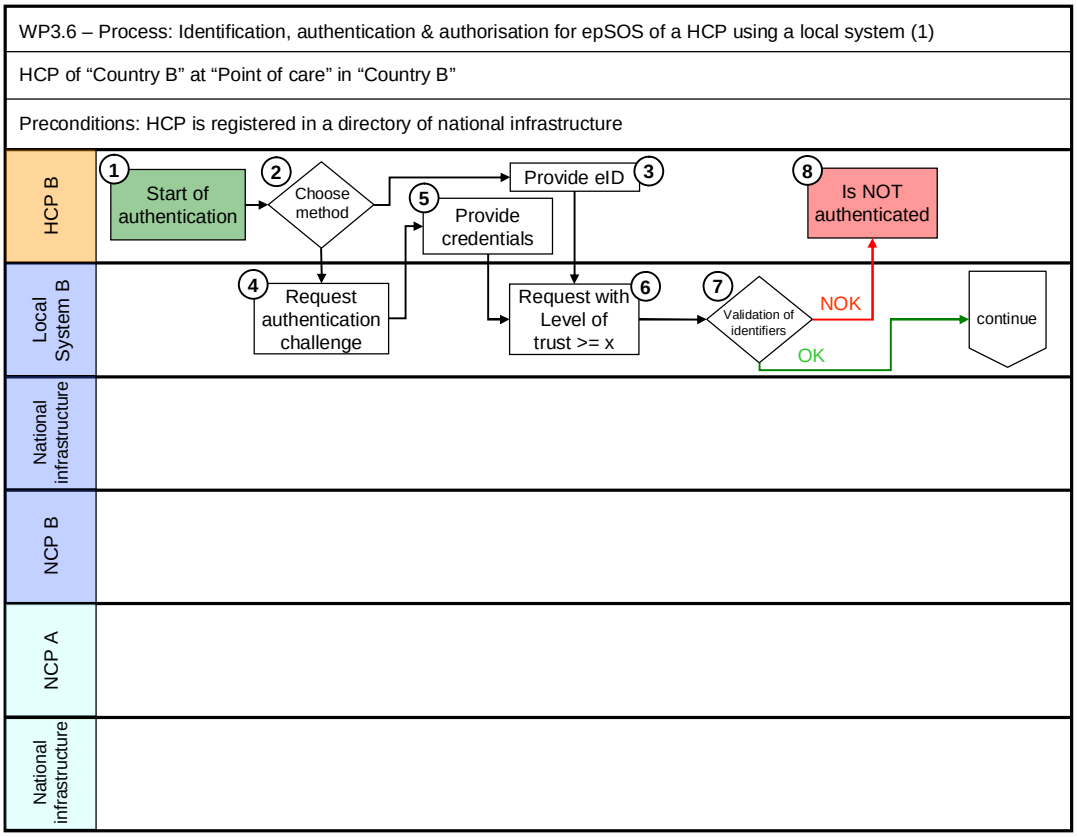

Figure 6 - Process of identification, authentication & authorisation for epSOS LSP of a HCP using a local system

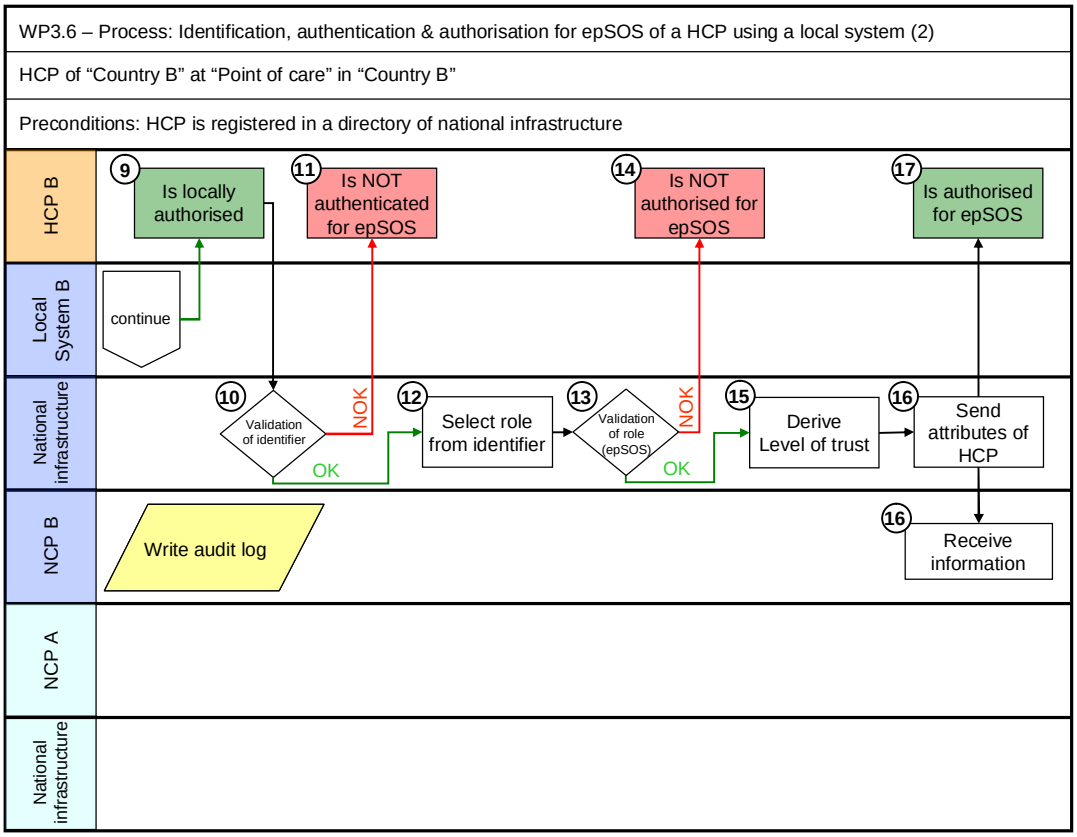

Figure 7 - Process of identification, authentication & authorisation for epSOS LSP of a HCP using a local system (cont)

The process in the above flow diagram (figures 6 and 7) consists of the following steps:

1. HCP is situated at a local system in the Point of Care in Country B, wants to identify and authenticate himself for using the local system and wants to be authorised for the usage of the epSOS LSP environment. This is the start of the process.
2. HCP may be able to choose which identification and authentication method should be used: either the local system requests HCP‘s
    a. ID (continue with step 3) or
    b. logon data (continue with step 4)
3. HCP owns a unique identifier (refer to the process in chapter 7.3.1.1 Identification and authentication of a HCP with a unique identifier) and provides it for identification and authentication purposes (continue with step 6).
4. The local system is requesting an authentication challenge from the HCP.
5. The HCP responds to the authentication challenge as required by the authentication mechanism offered by the local system.
6. Both identification and authentication methods set a request for identification with a level of trust not less than “x” (value of “x” has to be analysed by WP 3.7 and will be defined by national authorities with respect to national legislation (see REQ 3.6.1)).
7. The entered credentials of the HCP are checked by the local system. A unique identifier of the HCP is authenticated (validated) by an appropriate verification service.

    One of the following results is returned:
    a. HCP is authenticated and authorized by the local system (continue with step 9) or
    b. HCP is not successfully authenticated by the local system.
8. In the case that HCP’s authentication fails the process is finished.
9. HCP is authenticated and authorised for using the local system. The local system provides the identifier information to the national infrastructure.
10. The credentials of the HCP are checked against the authentication data stored in a national registry. One of the following results is returned:
    a. HCP is authenticated for epSOS LSP (continue with step 12) or
    b. HCP is not successfully authenticated for epSOS LSP.
11. In the case that HCP’s authentication for epSOS LSP fails the HCP receives an appropriate message and the process is finished.
12. The actual role of the HCP is selected from the provided attributes.
13. The actual role of the HCP is checked against the authorisation data stored in a national registry. One of the following results is returned:
    c. HCP is authorised for epSOS LSP (continue with step 12) or
    d. HCP is not authorised for epSOS LSP.
14. In the case that HCP’s authorisation by epSOS LSP fails the HCP receives an appropriate message and the process is finished.
15. The national infrastructure derives a value for the evaluated level of trust based on the authentication method used. This value must be kept - together with some of the extracted information from the identifier - for further processing.

16. This value must be kept - together with some of the extracted information from the identifier - for further processing. All the selected attributes of the HCP are sent to the NCP B for further processing in other processes.
17. The message about the successful authorisation is sent to the local system of the HCP. The process is finished.

7.3.1.4 Messages that can occur within the HCP processes

As already mentioned in the preconditions of the above described processes the HCP must be registered in a national directory which is a part of the national infrastructure of Country B (for details refer to chapters 9.1 HCP Identification/Authentication and 9.4 Storage of HCPs, HCPOs Identifiers on a National Base - "Directory" for HCPs).

Regarding the single process steps the following (error) messages could show up:

- "The validation of HCP's identifier or identification and authentication data was not successfully completed."
- "The expected Level of trust is higher than the offered one."
- "The actual role of the HCP is not authorised for epSOS."

7.3.2 Identification and authentication of a patient

Patients are other key actors of epSOS LSP. They enter into many relations with other epSOS LSP 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 HCP in Country B;
- When the patient wants to administrate his own patient consent (in Country B it only can be done by a HCP at PoC);
- 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 LSP 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 epSOS LSP but some MS have implemented such solutions.

REQ 3.6.3 At least one of these possible methods to identify and authenticate patients abroad MUST be installed and maintained by a participating MS.

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.

7.3.2.1 Identification and authentication of children

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.

7.3.2.2 Identification and authentication of a patient with a unique identifier

This process describes the case in which a patient of Country A identifies and authenticates himself for epSOS LSP at a PoC 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 LSP (for details, see picture and descriptions below).

If an eID is used, it is a precondition for this process that the system at PoC in Country B must have the capability to deal with an eID (e.g. read a “foreign” smart card) of Country A.

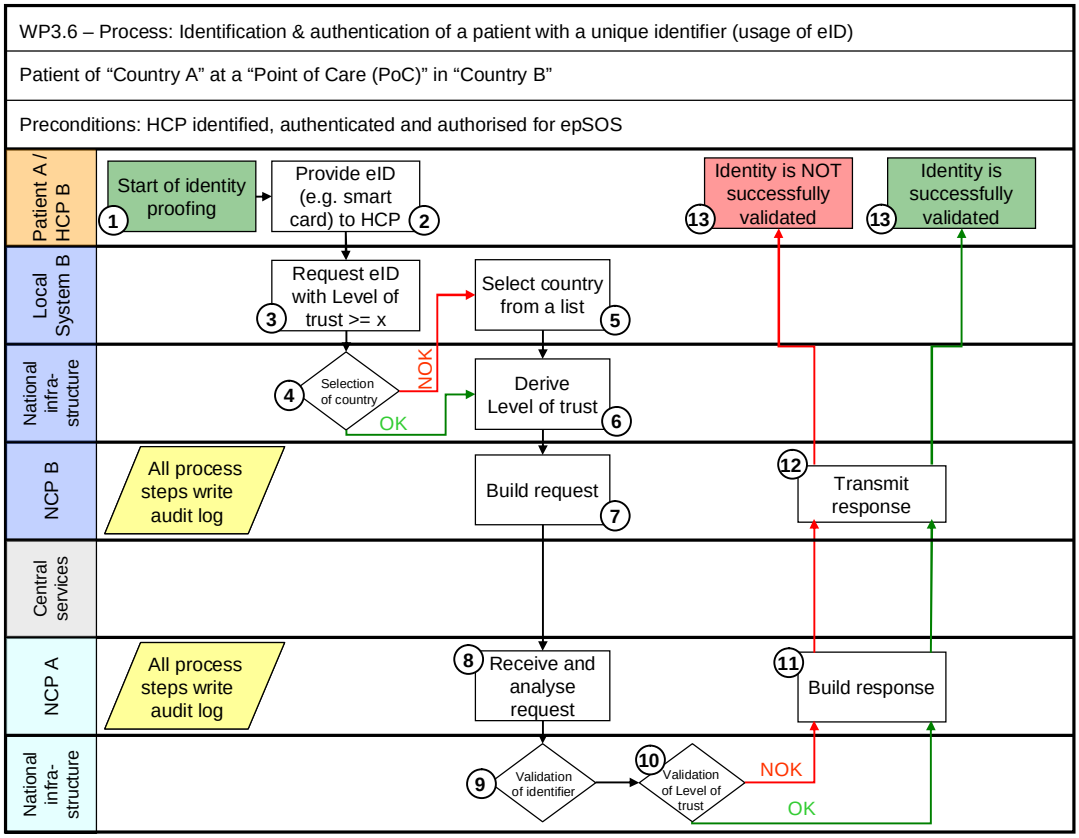

Figure 8 - Process of identification and authentication and authorisation of a patient with a unique identifier

The process is depicted in flow diagram in Figure 8 and consists of the next steps:

1. Patient is situated at the PoC in Country B and wants to be identified and authenticated for epSOS LSP. As a precondition, the patient has to show a trustworthy document (e.g. driving license, passport) as a primary identifier to the HCP. This is the start of the identification and authentication process. The first step in this process may include the revalidation of the authorization of the HCP for epSOS LSP.
2. Patient possesses a unique identifier (e.g. eID located on a smart card) and provides it for identification and authentication process in epSOS LSP.
3. Patient provides the unique identifier to the HCP (at PoC) and the HCP uses this unique identifier with request for identification with trust level not less than “x” (value of “x” has to be analysed by WP 3.7 and will be defined by national authorities with respect to national legislation (see REQ 3.6.1)).

4. The national infrastructure in Country B should be able to (based on the unique identifier) either automatically select the home country of the foreign patient (continue with step 6) or present a form for the selection of patient's home country manually (continue with step 5).
5. Selection of patient's home country from a list is done manually on local system by the HCP.
6. The national infrastructure derives a value for the evaluated level of trust based on the authentication method used.
7. The identifier information is transmitted to the NCP B. The NCP B builds the request and maps it into a predefined format for Country A. The request is transferred to NCP A for starting the authentication of a patient. NCP B writes a record into audit log[11]. The new layer of Central Services is not actively involved in this process.
8. NCP A receives and analyses the request (e.g. checks the completeness) from NCP B and writes a record into audit log.
9. Then NCP A confirms to NCP B reception of the request and writes a record into audit log. NCP B receives the confirmation from the NCP A and writes a record into audit log. *Note: These steps appear redundant but they are necessary for trouble shooting if some transactions seem to be lost.*
10. The transferred unique identifier of the patient is validated by the identity verification service in Country A.
11. The level of trust is checked not to be less than a predefined value.

    One of the following results is returned to NCP A:

    a. Patient is authenticated for epSOS LSP or
    b. Patient is not successfully authenticated for epSOS LSP.
12. NCP A receives the result of the authentication step from the national infrastructure and writes a record into audit log. Then NCP A builds the response and maps it into the predefined format for Country B. The response to the request for authentication is transferred to NCP B. The transmission is logged in the audit log.
13. The NCP B receives the response from NCP A and writes a record into audit log. Then NCP B transmits the result of the authentication process in Country A to the local system of the HCP and writes a record into audit log.
14. HCP and patient receive the result of authentication:

    a. Either patient is authenticated for epSOS LSP or
    b. Patient is not successfully authenticated for epSOS LSP.

7.3.2.3 Identification and authentication of a patient with demographic data

This process describes the case of a patient of Country A, who wants to be identified and authenticated for epSOS LSP in Country B at the PoC 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) (for details, see pictures and descriptions below).

Minimum data elements for searching a patient:

- Surname
- Given Name
- Date of birth (YYYYMMDD)

[11] The audit log in this and in the following cases will contain information relevant for the particular event, see chapter 7.6

- 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 MS, can be added (e.g. address)

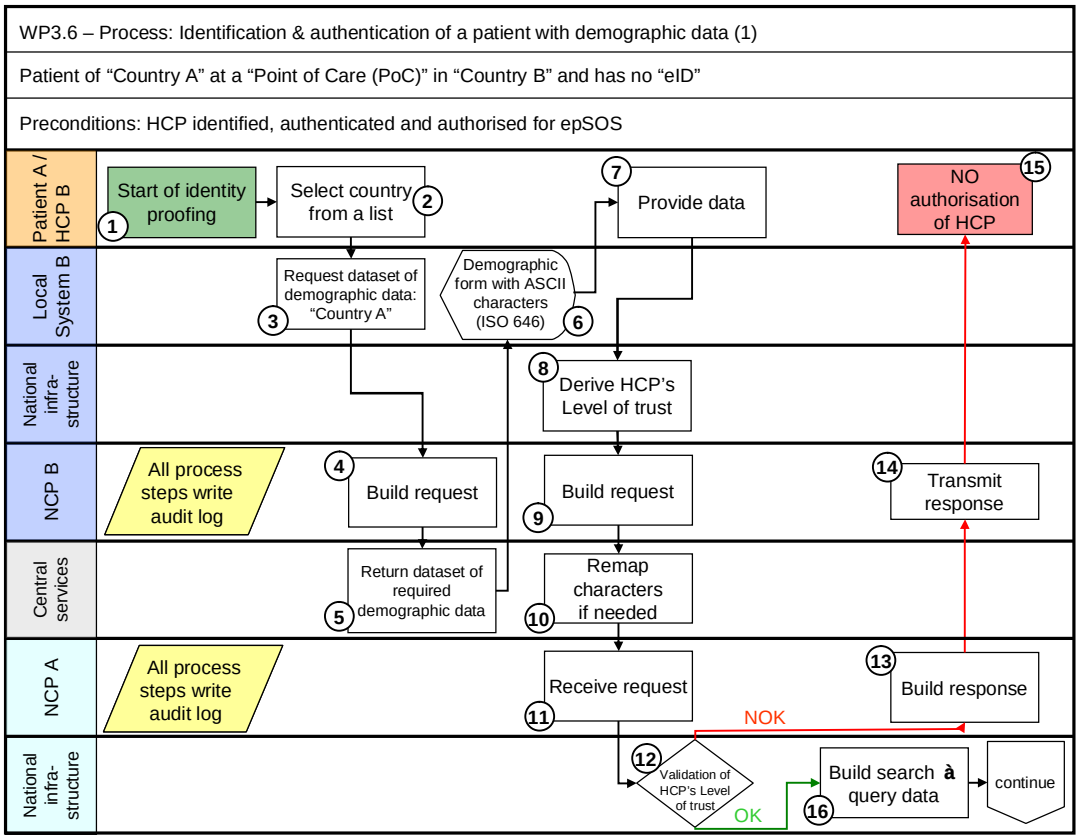

Figure 9 - Process of identification and authentication of a patient with demographic data

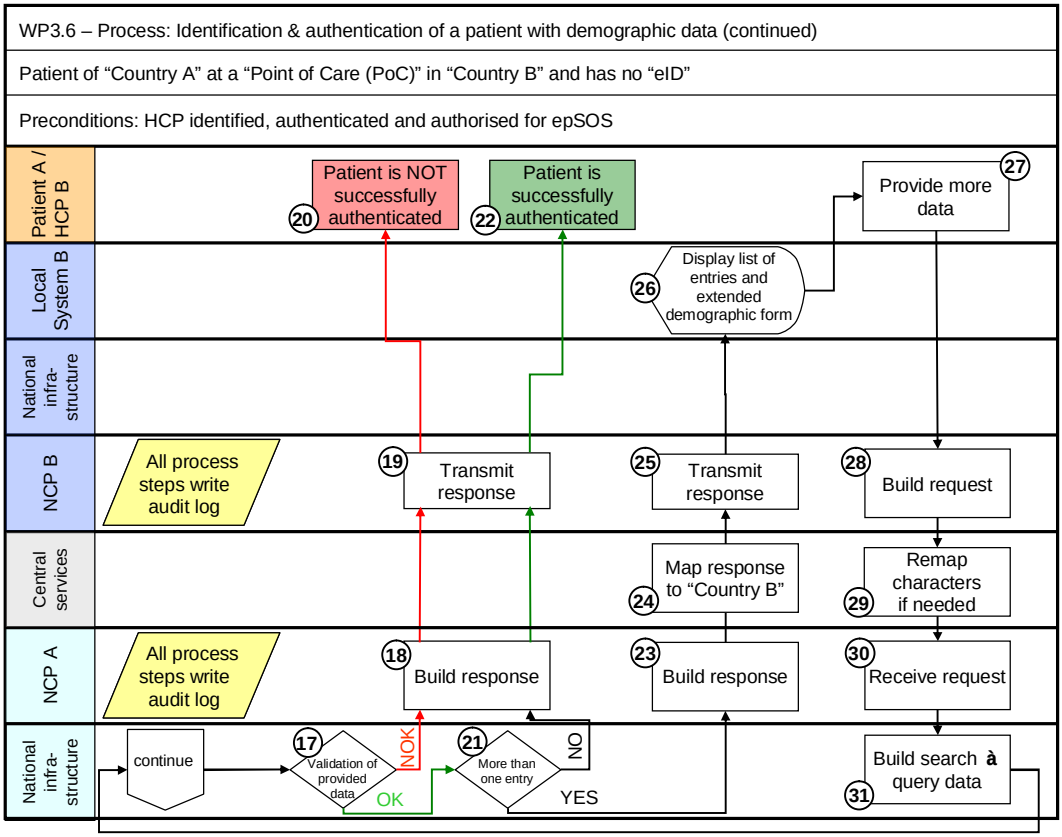

Figure 10 - Process of identification and authentication of a patient with demographic data (cont)

The process is depicted in flow diagram in Figure 9 and Figure 10 and consists of the next steps:

1. The patient is situated in Country B at the PoC and wants to be identified and authenticated. As a precondition, the patient has to show a trustworthy document (e.g. driving license, passport) as an identifier to the HCP. This is the starting point of the identification and authentication process. The first step in this process includes the revalidation of the authorization of the HCP for epSOS LSP.
2. The patient tells the HCP the name of "his country of affiliation" (Country A) and based on this information, the HCP makes the selection of the appropriate country from a list, provided by the local system.
3. Then the local system (at PoC) requests from the NCP B the required dataset of demographic data for Country A.
4. NCP B receives the request from the local system and writes a record into audit log. Then the NCP B builds the request and sends it to the Central Services layer.

   Note: 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 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.
5. Then the appropriate part of the Central Services returns the required dataset of demographic data for Country A to the local system at PoC and writes this event into audit log.

Note: Of course this is not done in a direct way (Central Services send back the information to NCP B and NCP B sends the information to the local system) these is just drawn in a short way to make the picture easier to read.

6. The local system displays the form to enter the appropriate demographic data (e.g. for French patients just one filed to enter the ID or for German patients the required fields to enter a pseudonym and a TAN). If used the fields for “Surname” and “Given name” must be appropriately adapted in length and format (e.g. name prefix for ES and NL). This form uses ASCII characters (as defined by ISO 646) for entering demographic data to avoid misspelling errors raised by “foreign” characters. The permission of how to use “wildcards” (replacing characters by a single character e.g. “?”, “*”) must be defined by each MS.
7. Patient provides the appropriate demographic data to the HCP, who enters them into the local system at PoC, exactly as written in the patient’s document or printed on an identification card.
8. The national infrastructure derives a value for the evaluated level of trust based on the authentication method used by the HCP. This value is sent to NCP B together with patient’s demographic data.
9. The NCP B receives data from local system and writes this event into audit log. Then the NCP B builds the request and hands it over to Central Services.
10. Central Services map it into the predefined format for Country A. The request for patient authentication is transmitted to NCP A and the transmission is recorded into audit log.
11. NCP A receives the request from NCP B and remaps characters (if needed). NCP A writes a record into audit log. NCP A sends the received identification and authentication data to the national infrastructure and writes a record into audit log.
12. The national infrastructure compares the value of the level of trust of the HCP in Country B with the predefined value.

    One of the following results is returned:

    a. The received value is below the defined minimum or
    b. The received value is equal to or higher than the defined minimum (continue with step 16).

13. Then NCP A builds a response, maps it into the predefined format for Country B and transmits the response to NCP B. NCP A writes this event into audit log.
14. NCP B sends the response to the local system of the HCP.
15. The local system at the PoC displays an appropriate message and the process is finished.
16. The national infrastructure takes the identification and authentication data and builds a request for search. Number of returned data records of this query is limited.

    Note: The limitation of returned data is an assumption and has to be defined by Country A. If there are more matches than this limit, the “quality” or the number of entered identification and authentication data can be seen as inaccurate and more data values are necessary to decrease the number of possible matches.

17. The national infrastructure performs a search (trying to validate identification and authentication data – credentials) against stored data in a national registry.

    One of the following results is returned:

    a. Validation of credentials is successful (at least one entry in the national registry conforms to the received demographic data) (continue with step 21) or

b. Validation of credentials is not successful (no entry in the national registry conforms to the received identification and authentication data) **à** patient is not authenticated.

18. NCP A receives an appropriate message from the national infrastructure and writes a record into audit log. Then NCP A builds the response, maps it into the predefined format for Country B and transmits the response to NCP B. NCP A writes this event into audit log.
19. NCP B receives the response from NCP A and writes a record into audit log. Then NCP B transmits the response to the system where HCP wants to authenticate the patient and writes this event into audit log.
20. HCP receives the message about failed authentication of the patient. The process is finished.
21. If just one entry in the national registry conforms to the received identification and authentication data of the patient, the patient is successfully authenticated and all unprotected demographic data will be returned to NCP A. Using the same algorithms as describes in steps 18 and 19 the national infrastructure sends back the data to the HCP in Country B.

    If more than one entry in the national registry conforms to the received identification and authentication data, the patient is not yet successfully authenticated and more identification and authentication data values are required (the process continues with step 23).
22. HCP confirms the authentication of the patient based on the returned demographic data and the process is finished.
23. Country A decides what will be returned to Country B.
    a. Option 1: The national infrastructure of Country A sends the list of matching entries to NCP A, limited by the national rules.
    b. Option 2: No demographic data will be returned but a predefined value that Country B can derive that there are more matches than just one. This would support patient's privacy and prevent the HCP from selecting the wrong patient record from the list of available matches.

    Regardless of which option is used, the NCP A writes a record (NOT the data content!) into audit log. Then NCP A builds the response, maps it into the predefined format for Country B and transmits the response to NCP B. NCP A writes this event into audit log.
24. The Central Services layer of NCP B receives the response from NCP A, remaps or translates the response if needed and writes this event into audit log.
25. Then NCP B transmits the response to the local system of the HCP at PoC.
26. The local system at PoC receives the response of Country A and displays the (probably extended) demographic form again.
27. Now the HCP has 2 options:
    a. If Country A sent back a list of matching entries (step 23, Option 1), he can select the specific record that matches the person which is standing in front of him based on additional identifiers (e.g. Passport) or
    b. Enter more identification and authentication data of the patient and send the data to NCP B.
28. The NCP B receives data items from the local system of the HCP. Then NCP B builds the request again and hands it over to Central Service.
29. Central Services map it into the predefined format for Country A and transmits the requests to the NCP A again. NCP A writes a record into audit log.

30. The NCP A receives the request from NCP B and writes an event into audit log. Then NCP A sends the identification and authentication data to the national infrastructure.
31. The national infrastructure takes over the identification and authentication data and processes the search algorithm again. Number of query data is still limited (as defined by Country A). Continue with step 17.

REQ 3.6.4 The permission how to use “wildcards” (replacing characters by a single character e.g. “?”, “*”) must be defined by each MS.

REQ 3.6.5 The procedures of how to handle “more than one” matches in identification and authentication processes of patients must be defined by each MS.

7.3.2.4 Messages that can occur within the patients processes

As already mentioned in the preconditions of the above described processes the patient must be registered in a national directory which is a part of the national infrastructure of Country A.

Regarding the single process steps the following (error) messages could show up:

- “No information about Country A is available neither in Country B nor in epSOS.”
- “Connection to Country A failed. Identification, authentication and authorisation of a patient is not available.”
- “The expected Level of trust of patient’s identification, authentication and authorisation in Country A is higher than the offered one.”
- “The expected Level of trust of the HCP is higher than the offered one.”
- “The offered eID or identification and authentication data of the patient could not be found in Country A.”
- “The offered identification and authentication data return more matches than allowed in Country A.”

7.4 Authorisation

Authorisation is a part of access management and the outcome is an attribute (role). In general, authorisation is a process to assign the proper rights to an identified entity (person, system or process) to do or to use something. In epSOS LSP environment, authorisation provides access control decision information for some access control mechanisms, controlling access to a patient’s health data and other sensitive data. The access to patient’s data in epSOS LSP is governed by epSOS LSP access control policy, based on the need-to-know principle. Active entities (actors) of epSOS LSP are categorised with respect to their tasks and positions in epSOS LSP environment and standardized sets of privileges are assigned to each role (category). Most activities require as a necessary prerequisite successful authentication of both participating parties and methods of authentication were described in previous parts of this chapter. Having assigned roles to entities, successful authentication enables to link an entity with a role (attribute) and thus in many cases it serves as an authorisation. Nevertheless, the cross-border access to patient’s data requires additional authorisation, based on patient consent. (The management of patient consent is described in part 7.5 Patient consent management)

In this part the epSOS LSP actors are described and activities associated to them.

7.4.1 epSOS LSP actors and responsibilities

The following table summarizes the relevant activities of actors belonging to epSOS LSP roles (assuming the basic scenario – HCP from Country B needs patient’s health documents from patient’s home Country A).

Actor	Action	Necessary preconditions	Other directly

			involved actors
HCP B	Requests services from Country A	• Successful identification, authentication and authorization of HCP in Country B • Successful identification and authentication of the patient by Country A	National Infrastructure B NCP B NCP A
Patient	Gives, revokes or modifies patient consent	• Successful identification and authentication of the patient at PoC	HCP (A or B) NCP A NCP B
	Requests check and provision of audit log concerning the accesses to his health data	• Successful authorization of HCP and authentication of the patient at PoC	NCP A Health data administrator
NCP B	Requests services from Country A	• Successful identification and authorization of NCP A • Authentication of the patient	NCP A
NCP A	Responds to service requests of NCP B	• Successful identification and authentication of NCP B • Authentication of the patient • Authorisation of HCP/O	NCP A Identity authority managing the databases of patients, HCPs, HCPOs
HCPO or other external service provider	Provides required information to NCP	• Mutual successful authentication of both parties • Patient consent • positive authorisation	NCP A HCO or other external service provider
Health data administrators	Administrate systems processing data and provide some services (e.g. excerption of audit logs)	• Successful identification of health data administrators • Authentication of health data administrators • Assigning the role of health data administrators	NCP or HCO

Table 6 - epSOS LSP actors and responsibilities

7.4.2 Management of epSOS LSP actors

epSOS LSP is based on distributed systems and many functions will be executed by actors within national domains. The epSOS LSP role management depends strongly on cooperation with national authorities, operators of local systems..

7.4.2.1 NCP

NCPs occupy the highest position in epSOS LSP and there is no epSOS LSP entity authorised to assign an entity the role of a NCP. The management of the NCP role must follow the following schema[12]:

1. epSOS LSP project defines the initial requirements for NCPs
2. NCPs of MSs participating in epSOS LSP pilot project will be founding NCPs of epSOS LSP

[12] The schema describes one possible technical solution and does not deal with legal, political, economic and procedural aspects

3. Founding NCPs review the initial requirements, set the criteria for NCP and introduce control mechanisms (e.g. security audit); the cooperation among NCPs must conform to general multilateral agreement (least security and interoperability inevitable requirements) and more advanced bilateral agreements.
4. Enrolment of a new NCP into epSOS LSP must be based on candidate NCP accreditation by existing NCPs and signing multilateral agreement,
5. Since every NCP must prepare, approve and implement security policy compliant with epSOS LSP security policy, every NCP will regularly (and if it would be necessary) undergo a security audit. The results of security audit are the necessary conditions for retaining the status of NCP.
6. Since the security problems of one NCP can jeopardize the others, the cooperation with a problematic NCP can be interrupted (on bilateral basis) or the activities that insecure NCP in epSOS LSP can be suspended.

The secure communication among NCPs (identification, authentication and encryption/decryption) can be supported by PKI.

Detailed descriptions of the issues of NCPs are included in the deliverables of WP3.3 and WP3.4.

7.4.2.2 HCPO

In every MS involved in epSOS LSP a national authority or a group of regional authorities must exist, able to define/manage HCPOs from its domain, participating in epSOS LSP. NCP will communicate with the respective national authority to keep the actual list of HCPO. epSOS LSP project (WP 3.6) would define the minimal set of information necessary for unambiguous identification of HCPO.

7.4.2.3 HCP

HCPs identities will be managed in national domains. A national authority will maintain the list of all HCPs in its domain and provide it to its national NCP. HCPO will provide NCP the roles assigned to its HCP (if necessary). epSOS LSP project (WP 3.6) would define the minimal set of information necessary for unambiguous identification of HCP.

7.4.2.4 Patients

epSOS LSP project WP 3.2 required the minimal set of necessary information for identification of a patient.

7.4.2.5 Health data administrator

A health data administrator is primarily responsible for running systems which exchange health data on NCP. The second responsibility covers the support of patients whenever they want an extract of audit log data.

Health data administrators are working for or in behalf of national authorities and from an epSOS LSP point of view the standard professional and security requirements fully suffice for this role.

REQ 3.6.6 Installation of a health data administrator in each MS with defined mission.

7.5 Patient consent management

Patient's health record can contain very sensitive data**,** where every kind of compromise can harm the patient. The privacy of patient data must be adequately protected.

The patient may decide to selectively allow any processing of health data within his patient consent. This selection has to be done in Country A – if patient is giving consent in Country B the consent no selection can be done.

It is agreed in epSOS LSP that explicit consent is necessary, except in an emergency case.

Different Options:

- Give/Revoke consent prior to country A for country B
- Give/Revoke consent in country B for country B with information "paper"
- Confirm Consent in Country B if Country A requires
- In possible further iterations of epSOS LSP a patient should be able to give/revoke consent anywhere in Country A

The descriptions suppose the existence of a national entity in Country A responsible for administration of patient consent (i.e. storage, management of changes, providing information on patient consent to authorised entities, etc.) This entity should be a repository which can be a part of the NCP. This document concerns to the national domain.

The document is always stored in his country of origin (Country A). Consent has to be given at a Point of Care. In the event of a patient seeking treatment in Country B, the Healthcare Provider will hand over an information "paper" to the Patient in the language of Country B and in the language of the patient (Country A). This "paper" will assure that consent is indeed "informed." In case of emergency implicit consent is assumed (depends on national law of Country A) and authorization for treatment is given to HCPs.

REQ 3.6.7 Implementing of Give/Revoke consent in Country B for Country B

REQ 3.6.8 Confirm consent in Country B for a patient from Country A if Country A requires

REQ 3.6.9 Different Data Set Entries in Audit Log File of Country A (see processes)

REQ 3.6.10 Different Data Set Entries in Audit Log File of Country B (see processes)

7.5.1 Processes for patient consent management

The following describes four basic processes for patient consent management:

7.5.1.1 Patient gives/revokes consent in Country A at PoC for Country B

This process describes the case in which a patient is situated at PoC in his Country A and gives/revokes patient's consent prior to Country B. A patient is already identified and authenticated and a HCP is also already identified, authenticated and authorised. Based on the request of a patient, a HCP at PoC carries out a modification of the patient's consent in national infrastructure (national repository in Country A). The consent modification can be "printed" and "signed" as evidence.

Highlights of this process:

- Consent is given/revoked prior to Country A for Country B

- Patient can give/revoke his consent for different Country B's
- Attributes of Consent:
    - Valid from Date (YYYYMMDD)
    - Valid to Date (YYYYMMDD)
    - Days (NNN)
- Consent Document is stored in Country A
- Consent is valid for whole Country B

This process describes Give/Revoke Consent in Country A for Country B

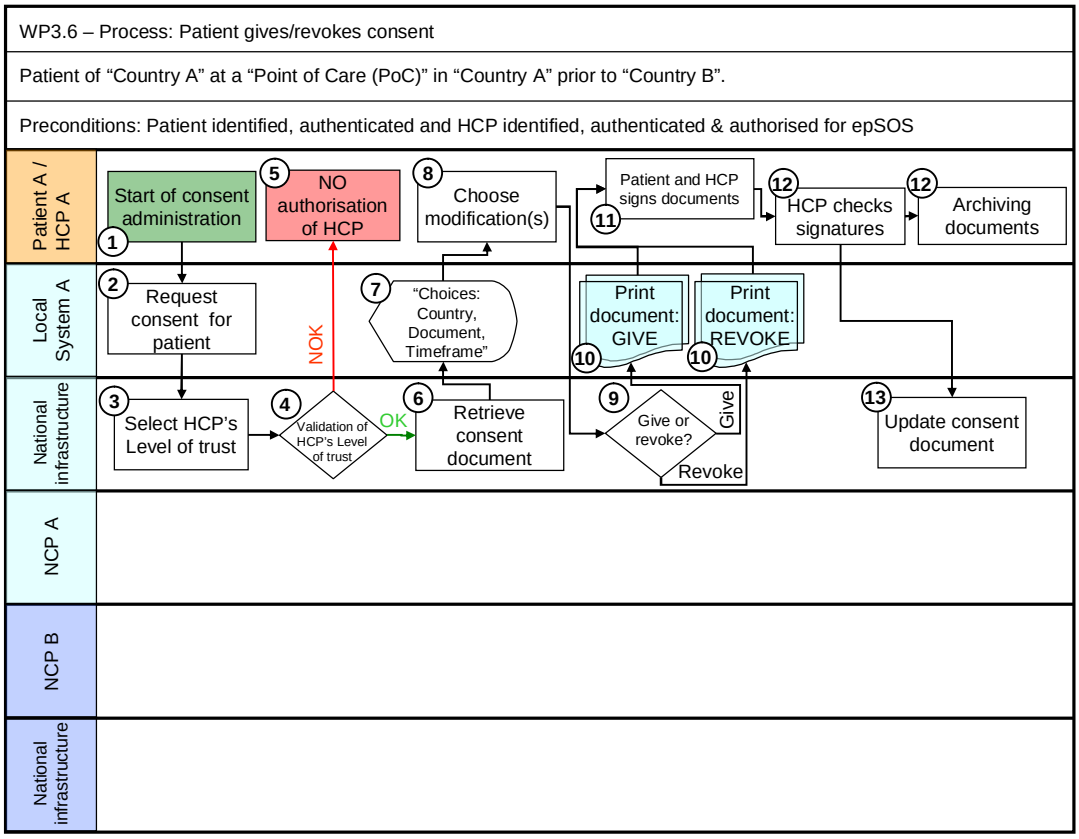

Figure 11 - Process of patient gives/revokes consent at PoC in Country A

The process is depicted in flow diagram in Figure 11 and consists of the following steps:

1. Patient is situated at PoC in Country A – start of consent management. Precondition for this process is that HCP is authenticated and authorized for epSOS LSP (including check of role) and the patient is authenticated.
2. HCP uses local system at PoC, makes a connection to national infrastructure (national repository) and requests consent for patient.
3. Level of trust from HCP will be selected.
4. The selected trust level will be checked and if not less than necessary, the process continues with step 6.

5. HCP is not authorized to change consents. An in formation will be written in the audit log record and the process is finished.
6. On this request the national infrastructure retrieves a consent document
7. Choose country, document and timeframe from national repository and send document to local system.
8. HCP inserts patient's choice of consent document modification(s) and sends modified consent document back to national infrastructure.
9. The national infrastructure checks the validity of either opt-in policy or opt-out policy of modification(s) and sends to local system either document „Patient gives consent" or document „Patient revokes consent".
10. On local system the document is printed out twice (one for patient and one for HCP).
11. The printed documents (informed consent documents) must be signed by the patient and by HCP.
12. HCP checks signature of patient (e.g. comparing with patient's passport) and archives one copy of document as an evidence of consent modification.
13. HCP confirms the modification(s) to national infrastructure and updates the patient's consent document in national repository. The process is finished.

Steps 11 to 13 are recommendations for documentation purposes in Country A and depend on national law of Country A as well as the will of HCP and patient.

7.5.1.2 Patient gives/revokes consent in Country B for Country B

This process describes the case in which a patient of Country A is situated at PoC in Country B and gives/revokes patient's consent. A patient is already identified and authenticated and a HCP is also already identified, authenticated and authorised for epSOS LSP and the level of trust is checked. At PoC, a HCP on patient's request executes the modification of patient's consent in national infrastructure in Country A (national repository in Country A). As evidence the consent modification document is "printed out" and the document is signed by HCP and by the patient. How to furnish proof in the future is an open issue (for details, see pictures and descriptions below).

Highlights of this process:

- Consent is given/revoked on demand in Country B for Country B
- Consent can be given/revoked only for Country B where he is staying
- Attributes of Consent:
    - Valid from Date (YYYYMMDD)
    - Valid to Date (YYYYMMDD)
    - Days (NNN)
- Consent Document is stored in Country A
- An information has to be signed (either signing of paper, digital signature, …)
- Consent is valid for whole Country B

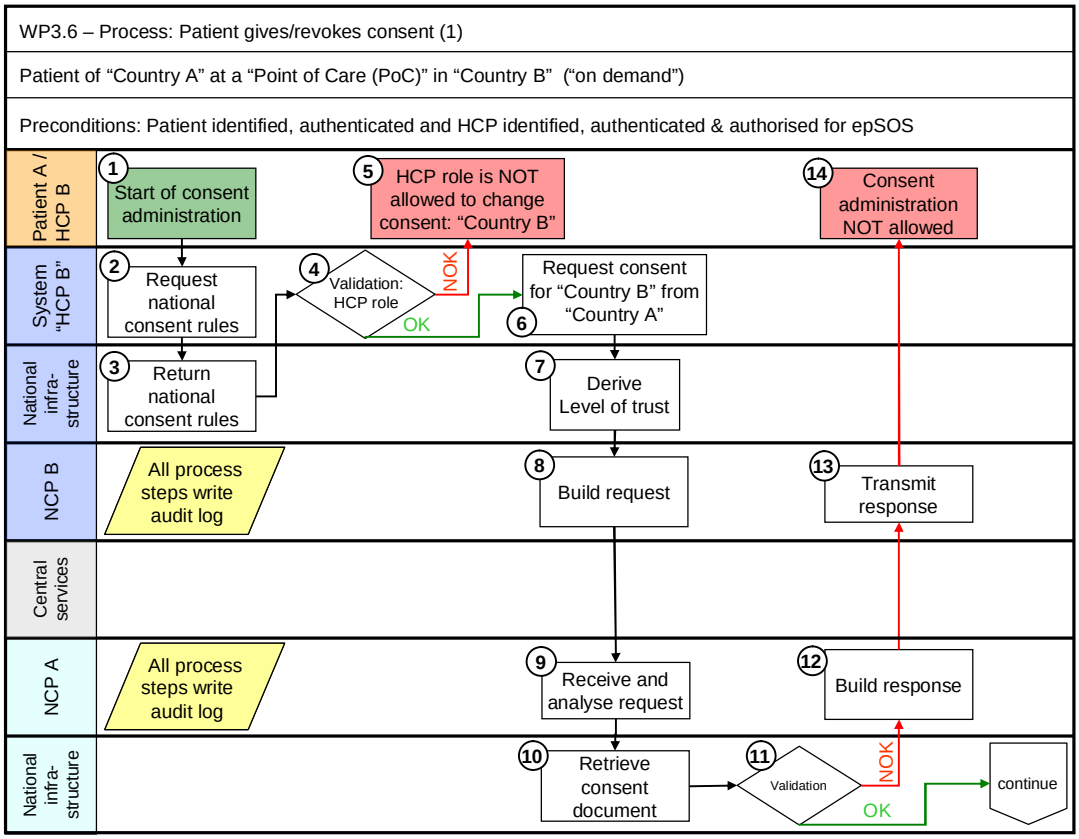

Figure 12 - Process of patient gives/revokes consent in Country B at PoC

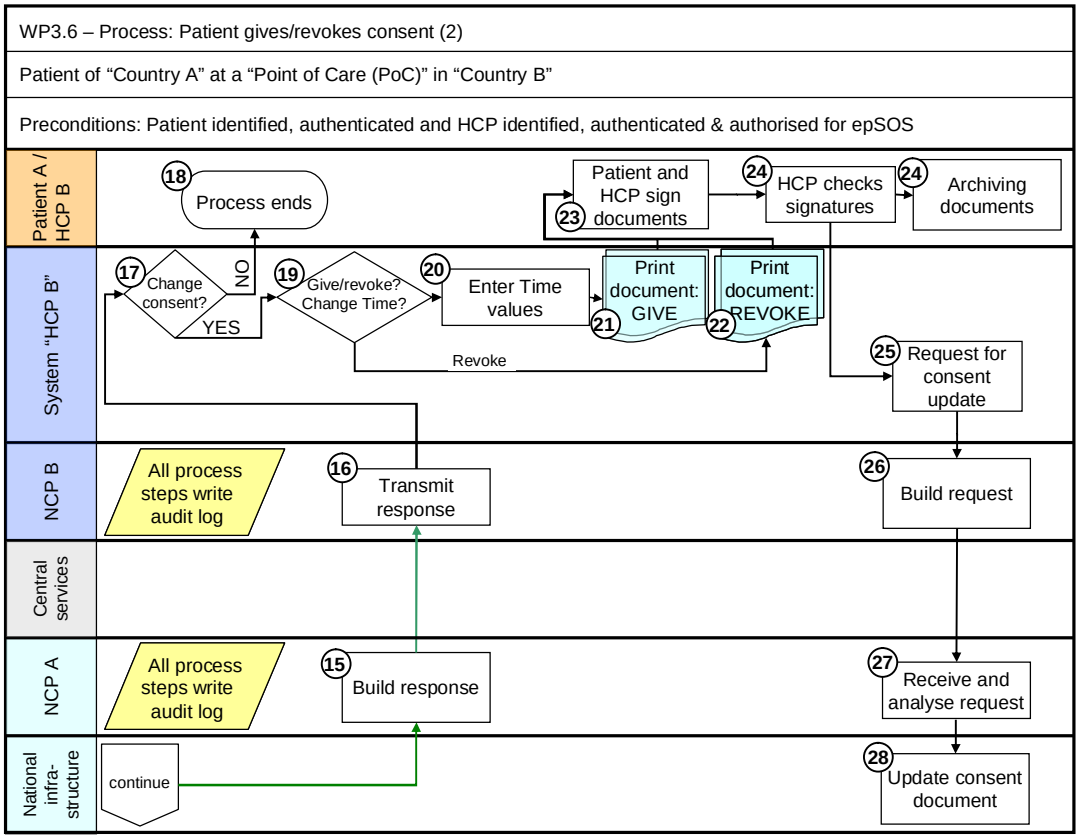

Figure 13 - Process of patient gives/revokes consent in Country B at PoC (cont)

The process is depicted in flow diagrams in Figure 12 and Figure 13 and consists of the following steps:

1. Patient is situated at the PoC in Country B and asks HCP for modification of patient's consent – start of consent management.
2. HCP's local system requests national infrastructure (Country B) for national consent rules.
3. National infrastructure in Country B returns on request the national consent rules to the HCP system.
4. The HCP system then checks the validity of the actual role of the HCP to change the patient's consent in Country B.

   One of the following results is returned:

   a. OK (actual role is allowed) (continue on step 6) or

   b. NOK (continue on step 5).
5. HCP's actual role is not allowed to change the patient's consent in Country B – process is finished.
6. HCP's system makes a request for consent for Country B from Country A and sends this request to NCP B.
7. Select the level of trust from Country B for the decision if Country A is trusting Country B in this process (level of trust is defined by WP 3.7).
8. The NCP B receives the request from HCP system and writes a record into audit log. Then NCP B builds the request, maps it into the predefined format for Country A and transmits the request for consent to NCP A. NCP B writes a record into audit log.
9. NCP A receives and analyses the request from NCP B and writes an audit log.
10. NCP A sends a request for the consent document to the national infrastructure of Country A and writes an audit log. The actual consent document from national infrastructure of Country A will be retrieved to check the actual status of consent for Country B.
11. The national infrastructure in Country A checks (in the national repository) the status of patient consent for Country B and prepares the consent document. In addition to that, the level of trust and the actual role of HCP B will be checked.

    One of the following results is returned:

    a. patient consent for Country B is NO - Country B is not allowed – national infrastructure prepares document „Patient gives consent" (continue on step 15) or

    b. patient consent for Country B is YES - Country B is allowed – national infrastructure prepares document „Patient revokes consent" (continue on step 15) or

    c. level of trust is below the required value of Country A or actual role of HCP B is not allowed to manage patient's consent (continue on step 12)
12. NCP A builds the response, maps it into the predefined format for Country B and sends it to NCP B. NCP A writes an audit log.
13. NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HCP's system and writes an audit log.
14. HCP and patient receive the result of consent for Country B and the process ends.
15. NCP A builds the response, maps it into the predefined format for Country B and sends it to NCP B. NCP A writes an audit log.
16. NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HCP's system and writes an audit log.

17. HCP and patient receive information on patient's consent status for Country B. If the patient does not want to change the consent (patient decides not to change anything) continue with step 18 else with step 19.
18. Process ends and the information about this will be added to audit logs in Country A and Country B.
19. Depending on consent details (as a result) of step 11 (Consent was given or not) the process will continue.
    a. If consent was given in Country A prior to Country B or in Country B for Country B, the patient can decide if he likes to change the time parameters (proceed with step 20) or to revoke the consent (continue with step 22).
    b. If consent was revoked or not given in Country A prior to Country B or in Country B for Country B, proceed with step 20
20. Enter date parameters
    a. Date Valid From (YYYYMMDD)
    b. Date Valid To (YYYYMMDD)
    c. Days (NNN)
21. In the case that status of patient's consent in Country B either was "NO" or patient wanted to change the timeframe, HCP systems receives document "Patient gives consent" and document is "printed out" in languages of patient and of HCP.
22. In the case that status of patient's consent in Country B was "YES" and the patient wants to revoke the consent, HCP systems receives document "Patient revokes consent" and document is "printed out" in languages of patient and of HCP.
23. Patient and HCP sign documents.
24. HCP checks signatures with identity cards (e.g. Passport, Driving Licence, etc.) and requests for consent update. The request is sent to NCP B. HCP can archive one copy of document (depends on the law of Country B). The patient gets a signed copy of the physical document in his language.
25. HCP's system sends the request for consent update to NCP B.
26. NCP B builds the request (or maps it to Country A) for NCP A for consent update and writes an audit log. If the patient wants to revoke his consent and the consent was prior confirmed by the patient (for details see next process description) this confirmation is deleted.
27. NCP A receives and analyses the request from NCP B and writes an audit log. If the patient wants to revoke his consent and the consent was prior confirmed by the patient this confirmation is deleted. NCP A sends a request for consent update to national infrastructure in Country A (national registry in Country A) and writes an audit log.
28. The national infrastructure in Country A updates (in national registry) the patient's consent document. The process is finished.

7.5.1.3 Confirm Consent in Country B if Country A requires

This process is necessary for some MS within epSOS LSP to confirm the consent which was either given prior to Country A for Country B or in Country B for Country B (this is a precondition for this process).

If Country A requires confirmation then this process is needed every time (for each treatment), because no information about requested HCP will be stored and date parameters are not valid (see Chapter 8.1.4 (Validation of Confirmation of Patient Consent)).

The outcome is a precondition for receiving health data to Country B from Country A, if this process is required.

Highlights of this process:

- Confirmation of given consent
- No information has to be signed
- Valid Date (From-To) of confirmation is still open (see Chapter 8.1.4 (Validation of Confirmation of Patient Consent))

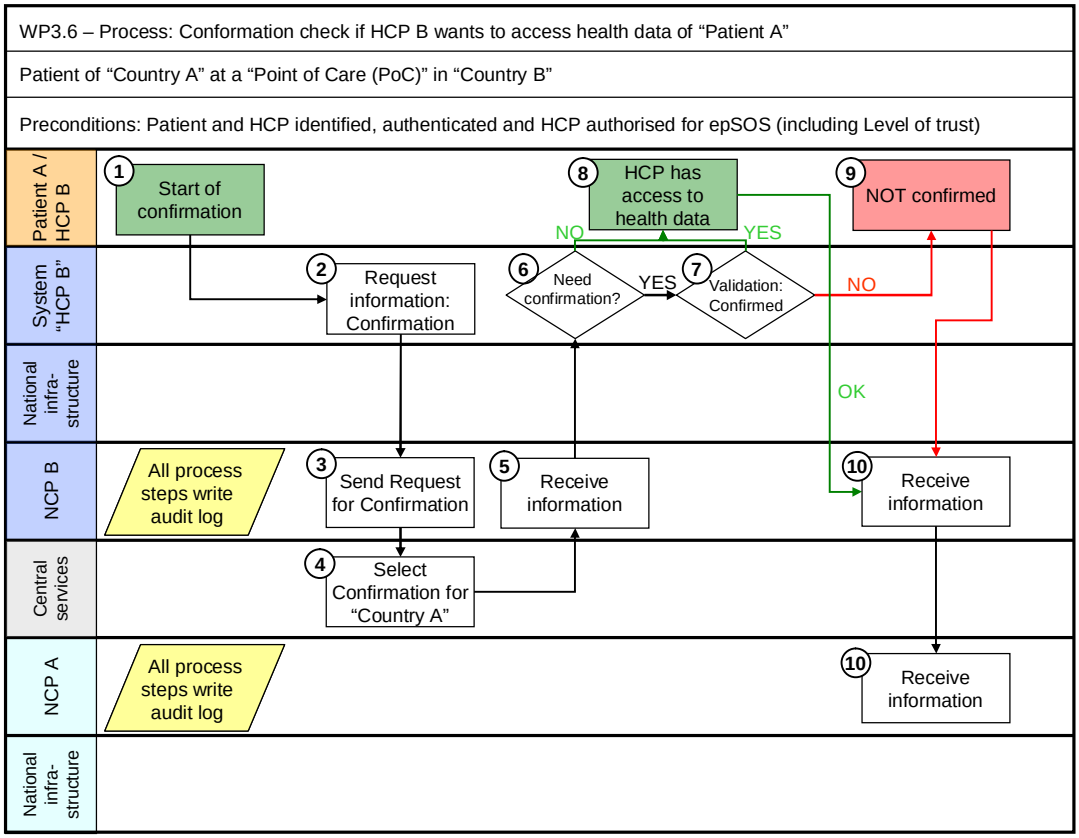

Figure 14 – Confirm Consent in Country B

The process is depicted in flow diagrams in Figure 14 consists of the following steps:

1. Patient is situated at the PoC in Country B and asks HCP for confirmation of his consent.
2. HCP requests via his local system the NCP B for information if confirming consent is required for Country A.
3. NCP B receives the request and hands it over to Central Services. This step will be logged in the audit log of Country B with the identifiers of HCP B and the patient of Country A.
4. The Central Services layer receives the request and selects the confirmation flag for Country A.
5. NCP B receives the appropriate information about the confirmation flag.
6. If patient must not give a confirmation, the process continues with step 8 else proceeds with step 7.

7. If confirmation is necessary, it has to be given explicitly. The patient has to say “Yes” (HCP will tick a box and patient will confirm it).
8. HCP has access to health data by patient’s confirmed consent. The process continues with step 10.
9. If the confirmation was not positive the HCP will not have any access to patient’s health data.
10. NCP B and NCP A will receive either a positive or a negative result of confirmation. The result will be stored in an audit log record and is an important parameter for the process “request health data”.

7.5.1.4 Patient gives/revokes consent in Country B for Country B including confirmation

This process describes a combination of the processes designed in chapter 7.5.1.2 (Patient gives/revokes consent in Country B for Country B) and chapter 7.5.1.3 (Confirm Consent in Country B if Country A requires).

The main advantage of this process is to reduce the number of transactions between Country B and Country A and to save performance.

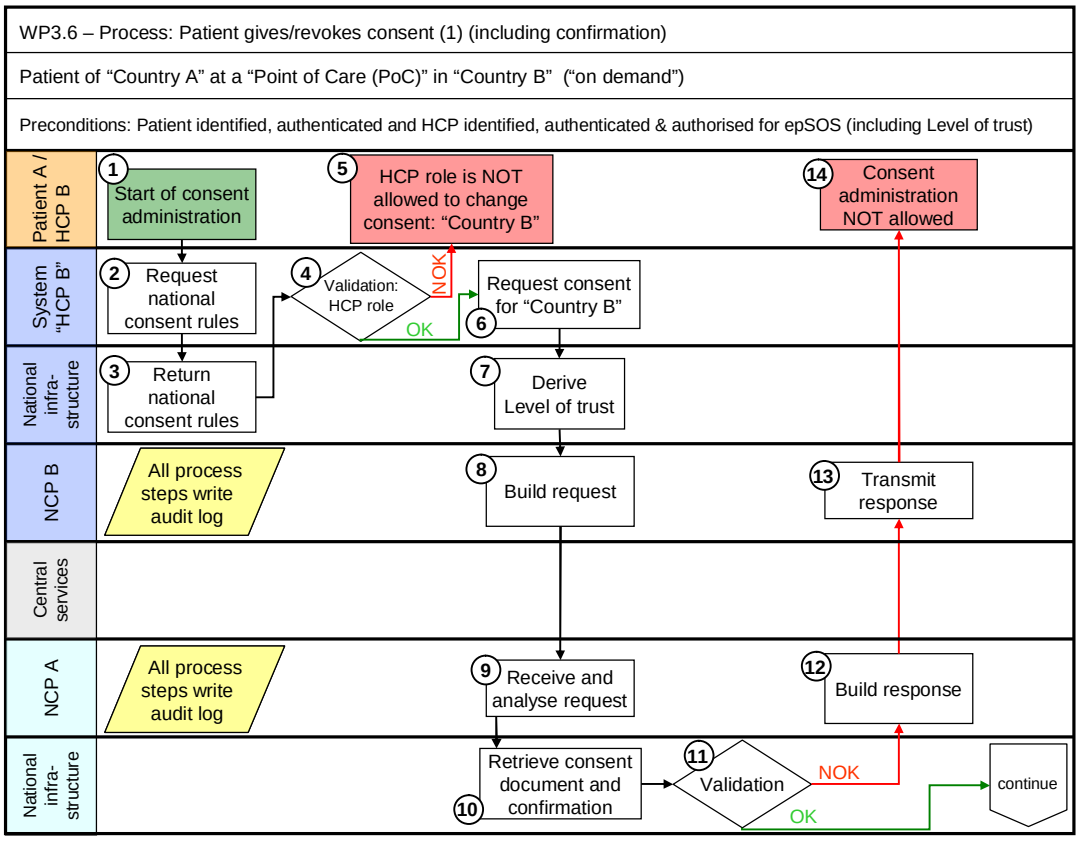

Figure 15 – Giving/revoking consent including confirmation

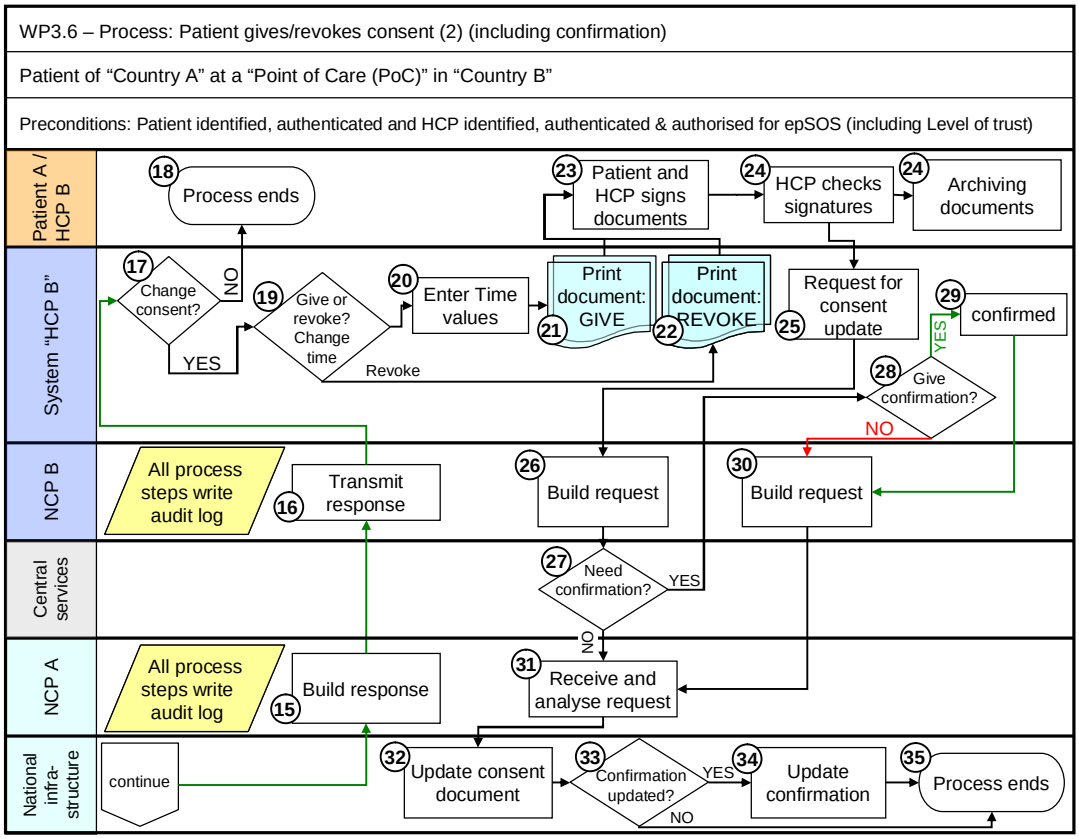

Figure 16 – Giving/revoking consent including confirmation (cont)

The process is depicted in flow diagrams in Figure 15 and Figure 16 and consists of the following steps:

1. Patient is situated at the PoC in Country B and asks HCP for modification of patient's consent – start of consent management.
2. HCP's local system requests national infrastructure (Country B) for national consent rules.
3. National infrastructure in Country B returns on request the national consent rules to the HCP system.
4. The HCP system then checks the validity of the actual role of the HCP to change the patient's consent in Country B.

   One of the following results is returned:

   a. OK (actual role is allowed) (continue on step 6) or

   b. NOK (continue on step 5).
5. HCP's actual role is not allowed to change the patient's consent in Country B – process is finished.
6. HCP's system makes a request for consent for Country B from Country A and sends this request to NCP B.
7. Select the level of trust from Country B for the decision if Country A is trusting Country B in this process (level of trust is defined by WP 3.7).
8. The NCP B receives the request from HCP system and writes a record into audit log. Then NCP B builds the request, maps it into the predefined format for Country A and transmits the request for consent to NCP A. NCP B writes a record into audit log.
9. NCP A receives and analyses the request from NCP B and writes an audit log.

10. NCP A sends a request for the consent document to the national infrastructure of Country A and writes an audit log. The actual consent document from national infrastructure of Country A will be retrieved to check the actual status of consent for Country B.
11. The national infrastructure in Country A checks (in the national repository) the status of patient consent for Country B and prepares the consent document. In addition to that, the level of trust and the actual role of HCP B will be checked.

    One of the following results is returned:

    a. patient consent for Country B is NO - Country B is not allowed – national infrastructure prepares document „Patient gives consent“ (continue on step 15) or

    b. patient consent for Country B is YES - Country B is allowed – national infrastructure prepares document „Patient revokes consent“ (continue on step 15) or

    c. level of trust is below the required value of Country A or actual role of HCP B is not allowed to manage patient's consent (continue on step 12)
12. NCP A builds the response, maps it into the predefined format for Country B and sends it to NCP B. NCP A writes an audit log.
13. NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HCP's system and writes an audit log.
14. HCP and patient receive the result of consent for Country B and the process ends.
15. NCP A builds the response, maps it into the predefined format for Country B and sends it to NCP B. NCP A writes an audit log.
16. NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HCP's system and writes an audit log.
17. HCP and patient receive information on patient's consent status for Country B. If the patient does not want to change the consent (patient decides not to change anything) continue with step 18 else with step 19.
18. Process ends and the information about this will be added to audit logs in Country A and Country B.
19. Depending on consent details (as a result) of step 11 (Consent was given or not) the process will continue.

    a. If consent was given in Country A prior to Country B or in Country B for Country B, the patient can decide if he likes to change the time parameters (proceed with step 20) or to revoke the consent (continue with step 22).

    b. If consent was revoked or not given in Country A prior to Country B or in Country B for Country B, proceed with step 20
20. Enter date parameters

    a. Date Valid From (YYYYMMDD)

    b. Date Valid To (YYYYMMDD)

    c. Days (NNN)
21. In the case that status of patient's consent in Country B either was "NO" or patient wanted to change the timeframe, HCP systems receives document "Patient gives consent" and document is "printed out" in languages of patient and of HCP.
22. In the case that status of patient's consent in Country B was "YES" and the patient wants to revoke the consent, HCP systems receives document "Patient revokes consent" and document is "printed out" in languages of patient and of HCP.
23. Patient and HCP sign documents.

24. HCP checks signatures with identity cards (e.g. Passport, Driving Licence, etc.) and requests for consent update. The request is sent to NCP B. HCP can archive one copy of document (depends on the law of Country B). The patient gets a signed copy of the physical document in his language.
25. HCP's system builds and sends the request for consent update to NCP B.
26. NCP B receives the request and hands it over to Central Services. This step will be logged in the audit log of Country B with the identifiers of HCP B and the patient of Country A.
27. The Central Services layer receives the request and selects the confirmation flag for Country A.

    One of the following results is returned:

    a. If patient must not give a confirmation, the process continues with step 31 or
    b. the confirmation is required

28. If confirmation is necessary, it has to be given explicitly. The patient has to say "Yes" (HCP will tick a box and patient will confirm it).

    One of the following results is returned:

    a. The patient confirms the consent.
    b. The confirmation is not positive, and the process continues with step 30.

29. Consent management process is explicitly confirmed by the patient.
30. NCP B builds the request (or maps it to Country A) for NCP A for consent update and writes an audit log. If the patient wants to revoke his consent and the consent was prior confirmed by the patient (for details see previous process description) this confirmation is deleted.
31. NCP A receives and analyses the request from NCP B and writes an audit log. If the patient wants to revoke his consent and the consent was prior confirmed by the patient this confirmation is deleted.
32. NCP A sends a request for consent update to national infrastructure in Country A (national registry in Country A) and writes an audit log.
33. If the existing confirmation state is not updated the process continues with step 35.
34. The national infrastructure in Country A updates (in national registry) the patient's consent document and confirmation state.
35. Process is finished.

7.5.1.5 Messages that can occur within the consent management processes

As already mentioned in the preconditions of the above described processes the patient and the HCP must be successfully authorised by the appropriate processes.

Regarding the single process steps the following (error) messages could show up additionally to the already described ones:

- "No consent document available for this patient."
- "Connection to Country A failed. Consent document and management processes are not available."
- "Country B is not allowed to manage any consent of Country A."
- "The entered timeframe is not valid or lies in the past."

7.5.2 Change of patient consent

Patient consent is one of the key security measures enforcing the privacy of patient's data and the only one, which is under control of the patient, but can only be done at Point of Care.

Patient may and can modify the default or previous value of his patient consent. The changes of default or previous values of patient consent require identification and strong authentication of patient and other participating entities, too. Any patient can change the former decision on approving/denying access to his health data from abroad personally in the corresponding patient consent registry of his home Country A, following the standard procedure guaranteeing the security and legal validity of the change. If a patient wants to change his previous decision at another place in Country A or B, the procedure has to guarantee, that the same level of security as the procedure of consent revocation in patient consent registry is achieved. Otherwise neither the patient consent registry in his home country nor the NCP A could accept the validity of the consent revocation.

7.5.3 Remote management of patient consent

This chapter describes either how a patient can handle the consent for himself (future possibility) or from HCP (part of the pilot) based on a Web Solution.

.

There are at least two possible scenarios for remote management of patient consent:

- Direct access to patient consent registry
- Changes at a point of care

Patient consent will be stored and administered in a patient consent registry in Country A, which will define procedures for patient consent changes. Everybody, who is authorised to change patient consent of a patient, must strictly follow these procedures. This concerns both, on-site and remote access patient consent changes. If national patient consent registry offers an option of remote access by means of Internet, the patient who is willing to change his actual patient consent must

- Authenticate himself to the registry
- Fulfil the change of consent form

If the patient consent registry does not provide patients the service of direct remote management of their patient consents by means of Internet, it can provide remote access to authorised epSOS LSP entities (e.g. points of care (PoCs). This service reduces the risk of unauthorised access to change patient consent from the Internet, but the following security requirements are still valid and these security problems persist:

- Strong Authentication of HCP (toward NCP B)
- Authorisation of HCP by patient to change his consent
- Strong authentication of the patient: Identity proofing of the patient according to legal requirements (e.g. check Passport)
- Connecting to national patient consent registry (this includes the connection HCP-NCP B-NCP A-registry)
- Confirmation of patients modified consent
- Audit logs (patient consent registry, NCP A, NCP B)
- There must be an agreement between NCP A and national patient consent registry on this service and NCP B must provide authentication service of PoCs.

7.5.4 Patient consent and authorisation

Country A administrates patient's health data (in a central repository or in a distributed form in local HCP (HCPO) systems). The only way to gain access to patient's data from Country B is to gain them from NCP A. To minimize the amount of data processing, the check of patient consent and of the Country A restrictions sending health data abroad, will be done by NCP A or patient's health data provider(s) before the data are processed by semantic service provider of NCP A. The communication protocol governing data transfer among NCP A, NCP B and patient's data providers depends on organization of NCP and the way patient's health data is organized in Country A.

7.6 Audit Trail

Because of security, legal and safety reason all relevant activities in the epSOS LSP environment must be written into audit log. This inevitable requirement should be applied for all NCPs and services/processes.

Generally, the audit trails are managed by administrators of information system (NCP).

REQ 3.6.11 Patient in epSOS LSP has a right to know who accessed his health data and when and in which cases patient gives/revoked consent. All data are stored in national infrastructure in his country (Country A). On patient's demand, the administrator provides patient with audit data that concerns the access to his health data or his patient's consent document.

7.6.1 Audit logging

An audit trail (log) is a record of the events occurring within an epSOS LSP environment (collection of individual NCPs information systems and networks). Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a NCP system or network. The logs, among the other useful goals, serve for recording the actions of users, and providing data useful for investigating malicious activity. Logs have evolved to contain information related to many different types of events occurring within networks and systems. Within an NCP, many logs contain records related to computer security; common examples of these computer security logs are audit logs that track user authentication attempts and security device logs that record possible attacks.

The ISO/IEC 27002:2005 standard formulates general requirement posed to audit logs as: audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period (has to be defined from WP 2.1) to assist in future investigations and access control monitoring.

REQ 3.6.12 Definition must be done from national site under national law.

The general structure of audit log includes (not restricted to):

- **User** IDs;
- **Dates**, times, and details of key events, e.g. log-on and log-off;
- **Terminal** identity (either terminal-ID in a hospital or IP number) or location if possible;

- **Records** of successful and rejected system access attempts;
- **Records** of successful and rejected data and other resource access attempts;
- **Changes** to system configuration;
- **Use** of privileges;
- **Use** of system utilities and applications;
- **Files** accessed and the kind of access;
- **Network** addresses and protocols;
- **Alarms** raised by the access control system;
- **Activation** and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

The audit logs may contain sensitive personal data. Appropriate privacy, integrity and availability protection measures should be taken. A standard option in protecting audits logs is performing their on-line back up on a log server. In this case, the audit logs are stored at two places, at the servers of their creation and at the dedicated log server.

In the processes of identification and authentication of epSOS LSP entities (described in chapter 7.3) the explicit requirements for writing audit logs by NCP are posed. Following the required items of audit log format for both cases of identification and authentication of epSOS LSP entities are given.

Identification and authentication of a HCP
- The audit log written by NCP B should contain these items:
  - Time reference
  - ID of HCP and provider of ID
  - Authorisation request
  - Attributes of HCP (role, specialisation) and provider of attributes

Identification and authentication of a patient
This process supposes the successful identification, authentication and authorisation of HCP for epSOS LSP.
- The audit log written by NCP should contain these items:
  - Time reference
  - ID of patient and provider of ID
  - Other country NCP
  - Type and/or transaction data (identification data, confirmation of transfer, result of identification, etc.)
  - Inbound NCP and outbound NCP
  - ID of epSOS LSP session

In the process of patient consent management the explicit requirements for writing audit logs by NCP are posed. This process supposes the successful identification, authentication and authorisation of HCP for epSOS LSP and the successful identification and authentication of patient.

Following the required items of audit log are given. The audit log written by NCP should contain these items:
- Time reference
- ID of patient and HCP
- Other country NCP

- Type and/or transaction data (patient consent for Country B, result if validation allowed, consent update, confirmation of transfer, etc.)
- Inbound NCP and outbound NCP
- ID of epSOS LSP session

7.6.2 Auditing Process

REQ 3.6.13 Audit process has to be described by WP 3.7
REQ 3.6.14 Audit Log has to be encrypted – is part of WP 3.7

8 Closed Open issues

8.1 Patient consent

Patient consent was discussed in different Work Packages and different Task Forces.

8.1.1 Attributes for Patient Consent

- Valid-From and Valid-To or days for the validity of the consent
- Are any other attributes needed?
  - WP 3.6 is open to handle other attributes too

-

8.1.2 Location for give/revoke Consent

- In Country B only given/revoke Consent can be done for Country B

8.1.3 Information Paper

The information paper is a document which describes the rights of a Patient and all the information needed for the patient to decide if he wants to give consent.

- Will be handed over to the patient at Point of Care in Country B in the language of Country B and in the language of Country A
- PoC has to be handle this information paper
- Information paper in different languages will be stored on a Central Server
- Content of Information paper was defined by WP 1.2

8.1.4 Validation of Confirmation of Patient Consent

- Confirmation is valid till Patient is changing the PoC (Point of Care)
  - Patient is an inpatient or staying as outpatient in the same hospital or hospital organization
  - If Patient is changing the hospital or Hospital organization then a new Confirmation is necessary

8.1.5 Requirements

REQ 3.6.15 The patient consent paper document and attached informational material for epSOS LSP must be based on an epSOS LSP-specific template sketching its layout and contents with as little Member State-specific modifications as possible.

REQ 3.6.16 The external representation of the consent must be available in the language of the patient's country of affiliation.

8.2 Roles

WP 3.6 defines different roles used in epSOS LSP. Only those roles define the rights of HCPs and HCPOs (see Chapter 3.1.1 (Active epSOS LSP entities)

Those rights are necessary for access to health data via epSOS LSP (Patient Summary, e-Prescription data and e-Dispensed medicine data).

The roles can be different in the MS and therefore WP 3.5 (Semantic) will translate (transcode or -map) them.

REQ 3.6.17 The roles have to be defined in each MS and will be matched to epSOS LSP Roles (mapping is defined in WP 3.5).

8.3 Levels of Trust

See Chapter 3.4 Level of trust

Has to be defined in each MS and must be defined as a requirement in WP 2.1 and WP 3.7.

NCP A and NCP B are technical as well as organisational within a circle of trust. NCP A knows explicitly and implicitly the location of NCB B. NCP B is the only regulatory authoritative entity that may legally broker a trust relationship for any HCP of Country B. Therefore, the location of NCP B and the HCP of Country B must always be equal.

REQ 3.6.18 For each operation that makes use of an identifier, risk assessment must define the minimum accuracy required. For each identifier used by epSOS LSP the guaranteed accuracy must be defined for all states of the lifecycle of this identifier. NCPs must only accept identifiers for health data processing if the maximum guaranteed accuracy is higher than the minimum required accuracy.

8.4 Necessary Implementation at National Site

As described in chapter 9 (Requirements/Recommendations for National Sites) MS have to implement processes and workflows for Patient identification & authentication, HCP identification, authentication and authorization, patient consent and audit trail.

8.5 Tests

Before Piloting phase the National Solution has to be tested:

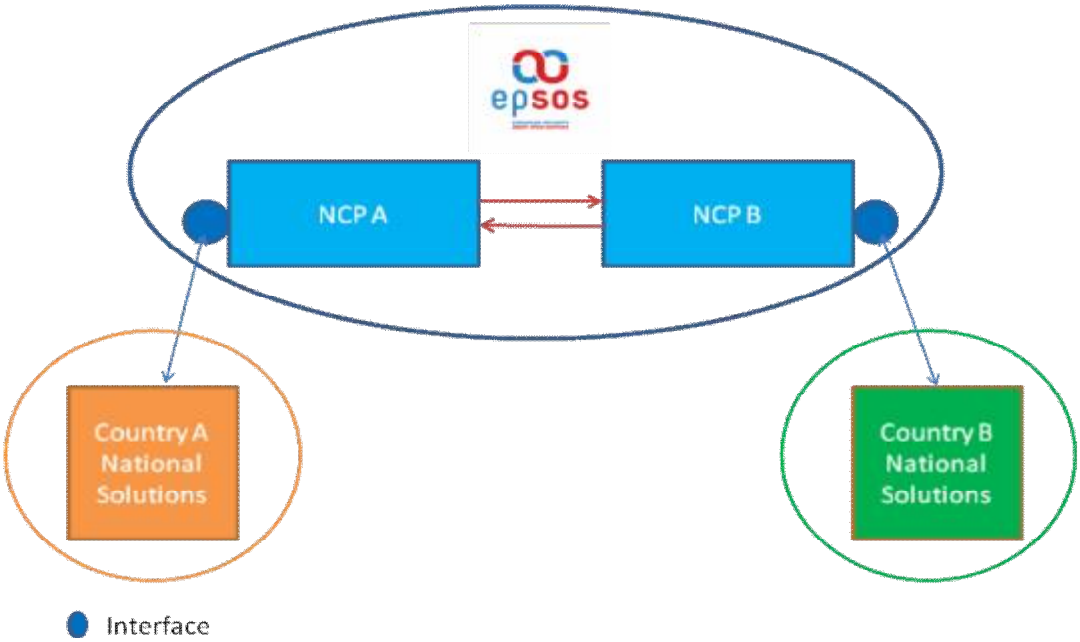

Figure 17 - Responsibility for Test and Implementation

epSOS LSP has the responsibility for the tests between NCPs and defined interfaces (blue ellipse).

MS have the responsibilities to test their solutions as sender and as receiver.

- Interface test from National Solution of Country A to NCP A
- Interface test from NCP B to National Solution in Country B
- Interface test from National Solution of Country B to NCP B
- Interface test from NCP A to National Solution in Country A
- The tests will be described in WP 3.8, 3.9, 3.10 and 4.2 a/b

REQ 3.6.19 Test cases and Test plans must be defined.

8.6 Implementation on National Site

REQ 3.6.20 epSOS LSP has the responsibility to implement all services and functions for NCP A and NCP B. Additionally, the interfaces between the NCPs and the regarding national infrastructures of the MS have to be defined and analyzed.

The MSs have to develop their own solution National implementations/solutions are out of scope in epSOS LSP.

See table of chapter 8.5 (Tests)

Detailed descriptions of the requirements can be found in chapter 9 (Requirements/Recommendations for National Sites).

8.7 Identification/Authentication based on eID

The information about the implementation and operation of smartcard-based patient identification & authentication is rather limited. The technical and architectural means of the epSOS LSP specifications, as well as the procedural and organisational requirements of WP 3.6, 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 LSP specifications may need to be aligned accordingly.

In order to fully enable the epSOS LSP 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.

8.8 ASCII Characters (ISO 646)

For the epSOS LSP piloting phase, only ACII Characters (ISO 646) will be used. The need of considering other characters as a fundamental requirement is fairly low. However, since Member States which may join the epSOS LSP project may not easily substitute their non ASCII characters. Future specification should refer problem to other projects.

REQ 3.6.21 For the pilot phase epSOS LSP should use only ASCII characters (ISO 646). This is very similar to the English alphabet.

8.9 Confirmation

Some MS needs a confirmation at HCP site from the patient. This process is described in Chapter 7.5.1.3 Confirm Consent in Country B if Country A requires and Chapter 7.5.1.4 Patient gives/revokes consent in Country B for Country B including confirmation.

REQ 3.6.22 An additional transaction has to be defined from WP 3.4 to check in Country A from Country B if confirmation is necessary or not.

9 Requirements/Recommendations for National Sites

This chapter describes which services/processes has/can be implemented in the MS.

Some services and/or processes are defined as requirements (REQ) (must be implemented in each MS which participating in epSOS LSP and the other as Recommendations (REC)).

9.1 HCP Identification/Authentication

Precondition for a HCP to have access to epSOS LSP is to be stored in a HCP "Directory" with defined data elements and their roles (see Chapter 3.1.1.2 Medical roles in epSOS LSP).

Outcome of the processes are always the Level of Trust and the Roles of a HCP.

Different options are described in the following subchapters, but one of the 3 options must be implemented.

9.1.1 Process with a unique Identifier

The process in chapter 7.3.1.1 (Identification and authentication of a HCP with a unique identifier) describes the case in which a HCP identifies and authenticates himself for epSOS LSP in his country (Country B) using a unique identifier.

REC 3.6.1 Every MS should use this method whenever technically feasible to support the security issues within epSOS LSP as good as possible.

9.1.2 Process via Internet portal

This process describes how a HCP identifies and authenticates himself for epSOS LSP in his country using Internet portal services. This can be done either by eID, Identifiers or with UserID / Password.

See chapter 7.3.1.2 (Identification and authentication of a HCP using an internet portal**).**

This process should be used if such services are implemented yet.

REC 3.6.2 This process should be used if such services are implemented in a Member state now.

9.1.3 Process within an existing implementation in Hospitals or GP's (local systems)

The process in chapter 7.3.1.3 (Identification and authentication of a HCP using a local system) describes the process of HCP Authentication and Identification for epSOS LSP in his country (Country B) at a PoC via local system.

REC 3.6.3 Hospital Information System or Systems installed by GP's should use the advantage of the service to start identification, authentication and authorisation process of a HCP within an implemented system e.g. if Single Sign-On is installed! The authentication can be done either by eID, unique Identifiers or UserID/Password.

9.2 Patient Identification/Authentication

Patient is another key actor of epSOS LSP. He enters into many relations with other epSOS LSP entities and in all cases he cannot act as an anonymous person. The patient needs to identify and authenticate himself in three cases:

- When he needs a health service and he visits a HCP in Country B.
- When he wants to manage his patient consent.

Outcome of the processes are the Level of Trust and the authentication of a patient.

Different options are described in the following subchapters, but Option 1 must be implemented and Option 2 can be, too.

9.2.1 Process with demographic data

The process in chapter 7.3.2.3 (Identification and authentication of a patient with demographic data) describes identification and authentication of a patient from Country A for epSOS LSP in Country B at the PoC without having an eID.

Because not all of the MS have installed eIDs, the recommendation of WP 3.6 for patient identification is to use at least the following values for demographic data (described data elements in Chapter 3.2 (Identity) are the minimum!)

Each Member State can extent the necessary demographics for better identification! Example: In The Netherlands, some names have a prefix and it's not clearly defined, if this is part of the name or a separate data element. The Netherlands can add this prefix for searching Dutch people in Country B. The Definition of the variables has to be stored on NCP A.

REQ 3.6.23 Any participating MS must establish organisational procedures and technical processes to allow the identification and authentication of its citizens by the usage of demographic data in an electronically format from abroad.

REQ 3.6.24 If a MS needs more than the minimum data elements to search for a patient, the additional data elements have to be stored on NCP A.

9.2.2 Process with unique identifiers

The process in chapter 7.3.2.2 (Identification and authentication of a patient with a unique identifier) describes the case in which a patient of Country A identifies and authenticates himself for epSOS LSP in Country B at the PoC. A patient possesses a unique identifier (e.g. eID stored on smart card or a similar authenticated token) issued by a national authority in Country A.

REC 3.6.4 Every MS should use this method whenever technical feasible to support the security issues and data privacy within epSOS LSP as good as possible.

9.3 Patient Gives/Revokes Consent

Three basic processes for patient consent management are worked out:

- Patient gives/revokes a consent at PoC prior in Country A for Country B

- Patient gives/revokes consent in Country B for Country B
- Patient confirms consent in Country B if Country A requires
- In further possible iterations of epSOS LSP**,** a patient should be able to give/revoke consent anywhere in Country A

REQ 3.6.25 The existence of a patient consent and its current location[13] must be determinable within the epSOS LSP environment.

REQ 3.6.26 Every participating Member State must design, adopt, and operate procedures to enable their assigned patients (country of affiliation) to execute their right of withdrawing their consents at any time, even from abroad.

REQ 3.6.27 Every Member State must implement organisational procedures to enable the patients to execute their granted right of self-disclosure.

REQ 3.6.28 Patients must not be forced to state their consent for the epSOS LSP services in Country A as well, when they are consenting to grant health data access for Country B. The epSOS LSP data access and exchange means regarding a full consented Country B can be independent of the consent of Country A.

REQ 3.6.29 Any patient consent must be given for specific and named countries only. Furthermore, any patient's consent must be given for a Country and not particular organisations / practices within a country.

9.3.1 Patient gives/revokes a Consent prior in Country A for Country B

The process in chapter 7.5.1.2 (Patient gives/revokes consent in Country A at PoC for Country B) describes the case in which a patient is situated at PoC in his Country A and gives/revokes patient's consent for Country B.

REC 3.6.5 Every participating MS should establish organisational procedures and technical processes to allow the modification of patient's consent in an electronically way in Country A for Country B.

9.3.2 Patient gives/revokes Consent in Country B for Country B

The process in chapter 7.5.1.2 (Patient gives/revokes consent in Country B for Country B) describes the case in which a patient of Country A is situated at PoC in Country B and gives/revokes patient's consent.

REQ 3.6.30 Every participating MS must establish organisational procedures and technical processes to allow the modification of patient's consent in an electronically way from abroad.

[13] The location determination may be implemented exclusively by organisational procedures and is only invoked on an on-demand basis.

9.3.3 Patient from Country A confirms consent in Country B when required from Country B

The process in chapter 7.5.1.3 (Confirm Consent in Country B if Country A requires) describes the case in which a patient of Country A is situated at PoC in Country B and confirms his consent for receiving health data.

REQ 3.6.31 Some MS (e.g. Germany, France) need a confirmation of the consent which was given prior to Country B in Country A or a confirmation on demand in Country B for Country B. Every participating MS must establish organisational procedures and technical processes to allow the modification of patient's consent in an electronically way from abroad.

9.3.4 Patient in Country B gives/revokes consent from Country A confirms consent in Country B when required from Country B

The process in chapter 7.5.1.4 (Patient gives/revokes consent in Country B for Country B including confirmation) describes the case in which a patient of Country A is situated at PoC in Country B and gives/revokes patient's consent and confirms his consent for receiving health data.

This process is a combination of patient gives consent for Country B in Country B and the confirmation of this consent.

REC 3.6.6 Every participating MS should establish organisational procedures and technical processes to allow this combined process.

9.4 Storage of HCPs, HCPOs Identifiers on a National Base - "Directory" for HCPs

In the identification/authentication process of each HCP/HCPO it will be checked if appropriate validation data and attributes are stored in a Directory -> Precondition of epSOS LSP Circle of Trust.

Additional to identification/authentication, this Directory is needed for the authorization process, because the role within epSOS LSP is one of the necessary data elements as an attribute.

Some MS are identifying only HCPOs and not the specific HCP. Nonetheless, the name or the Identifier of the HCP must be stored in the audit log and sent from Country B to Country A in case of a request.

HCP-"Directory" for Identification and Authorisation must be part of Test- and Pilot phase. Data Elements of the "Directory", defined in the next chapter, will be used for Identification (e.g. Identification number, Name of HCP/HCPO)" and the other one for the Audit Log (e.g. organisation, address)

The following subchapter (Chapter 9.4.1) describes the minimum information which has to be fulfilled from all MS.

9.4.1 Content of the Directory

Data Element	Mandatory	Description
Identification Number	Yes	Unique Number of the HCP/HCPO – individual in each MS
Name of HCP/HCPO	Yes	HCP : Name of HCP HCPO: Name of Legal Entity
Organization	No	Name of Legal Entity if HCP is working in an organization
Address	No	Street; ZIP Code; Town; Country

Phone Number 1	Yes	Mobile Phone, other Phone
Phone Number 2	No	Mobile Phone, other Phone
Fax Number	No	
eMail Account	No	If available : Mandatory and Minimum
Profession – Code	Yes	Code of the Profession
Profession – Text	No	Text
Specialist - Code	No	Code
Specialist – Text	No	Text
Roles for National Implementations	No	Max. 10 different Roles if needed
HCP - Roles	Yes	HCP roles (maximal 3 different Roles)
Country Code	No	Code of MS – necessary for Identification process
Valid From	Yes	Identification Number is Valid From : YYYYMMDD Necessary for Logical Delete Function
Valid Till	Yes	Identification Number is Valid To : YYYYMMDD Necessary for Logical Delete Function
Free Text	No	Free Text

Table 7 – Content of HCP Directory

REQ 3.6.32 Every participating MS must establish organisational procedures and technical processes to allow identification, authentication and authorisation processes of HCPs on a centrally managed directory, which contains the appropriate attributes for all HCPs authorised to use epSOS LSP.

9.4.2 Processes for HCP Directory

9.4.2.1 Design and implementation

The existence of this Directory is a precondition for Test- and Pilot phases within MS. Country A needs – if it receives a request from Country B - the mandatory data elements within the valid dates to check the role and store the information in the audit log (except Valid From, Valid Till).

9.4.2.2 Additional functions

For management of entries within the Directory additional functions are necessary:

- Add HCP's
  - Add new HCPs/HCPOs in the Directory
- Modify HCP's
  - Modify some information including roles
  - In this case the data elements "valid from" and "valid to" should also be changed
- Remove HCP's
  - Recommendation: 2 Functions:
    - § Logical
      - Change of Valid Till (e.g. retirement, change of profession, etc)

§ Physical

- Depends on national law (e.g. after 30 years)

-

9.5 Patient requests an extract of audit log in Country A

This process describes the necessary steps, if a patient wants to know who accessed his health data and when. The patient has to visit the health data administrator of the national infrastructure and to identify and authenticate himself. The authorisation of the administrator is done by signing (either wet signature or digitally) a form by the patient.

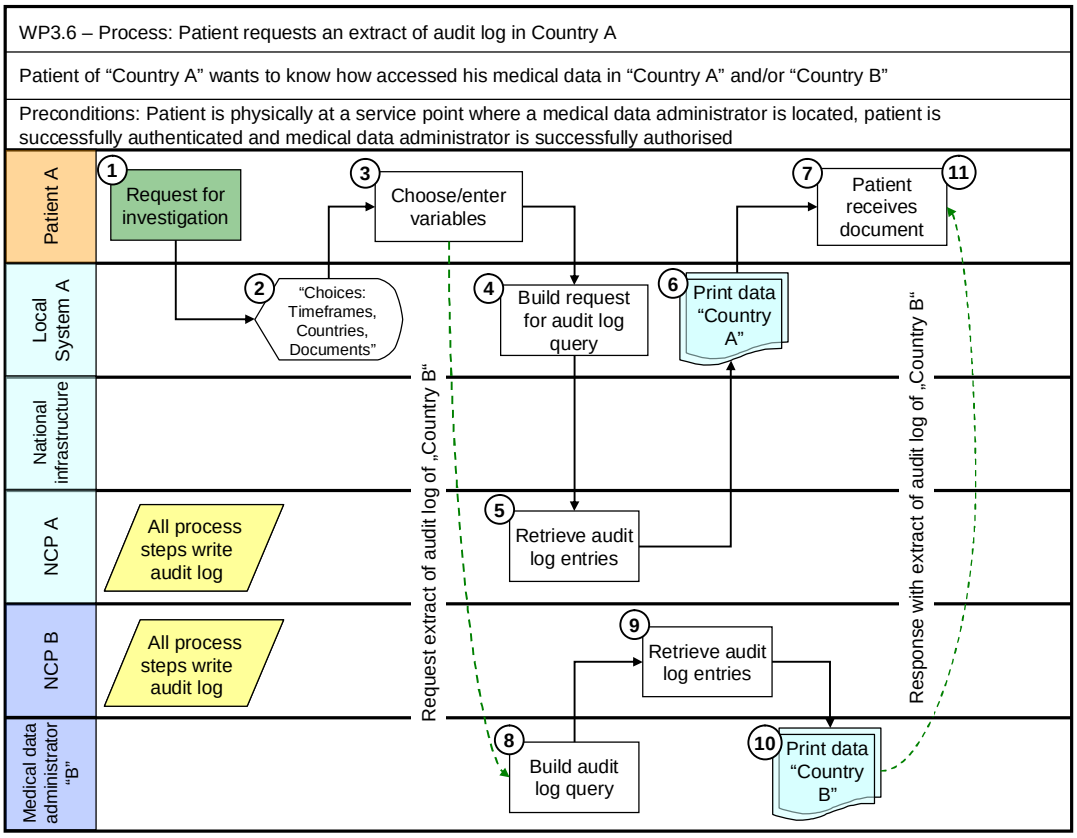

Figure 18 - Process of patient request for an extract of audit log

The process is depicted in flow diagram in Figure 18 and consists of the following steps:

1. Patient is situated at a service point in Country A and demands an extract of audit logs from the health data administrator, for investigating who accessed his health data and for what reason. Precondition is the identification, authentication and authorisation of health data administrator which is in respect not part of epSOS LSP.
2. The health data administrator starts an appropriate application, which collects the parameters for the data extract. Valid parameters can be
    a. Countries (a list of countries to which patient's consent is available)
    b. Documents (a list of available medical documents, including patient consent)
    c. Timeframe (to limit the range of possible date/time)
3. According to patient's statements the health data administrator enters data values.
4. The local system builds a request for a data query and sends this request to NCP A.
5. NCP A performs the query and extracts the corresponding data of the audit log. The resulting data entries are formatted in an appropriate way so that they are ready for

printing and sent back to the requesting local system. The information will be written in Audit records.

6. The local system initiates the print out of received data.
7. The health data administrator hands over the print out to the patient and the patient can check the access attempts to his health data.
8. In case the patient is concerned about the usage of his health data in Country B and wants a complete excerpt of the audit log regarding a singular treatment process in Country B, a request for additional information can be sent to Country B. The way this request is transmitted to Country B (green dotted line) depends on the possible functionalities of both countries and can be done either electronically or by mail. Similar to Country A the query for audit data is built in the local system of the health data administrator of Country B and sent to NCP B.
9. NCP B performs the query and sends data – in a printable format – back to the local system of the health data administrator. The information will be written in Audit records.
10. Like in step 6, the local system prints this data.
11. The health data administrator is responsible for sending the data back to the patient.

REQ 3.6.33 Any participating country must build an organisation and establish process, which can perform the extraction of audit logs based on the values provided by the patient.

9.6 Process "HCP accessing health data of a patient" (with given consent)

All health data of a patient that can be accessed by the means of epSOS LSP are managed within the existing national infrastructures. It is assumed that all data of a patient is indexed with a patient identifier ("index key") that is issued and managed by the national infrastructure. If a patient has data within multiple national infrastructures, these might be indexed by different patient identifiers.

In order to access data or in order to assign new data to a patient, the respective identifier of the patient that is used as an index key within the national infrastructure must be known by NCP A which initiates the respective data access operation. If data is accessed from another country (Country B) the NCP of this country must be aware of a patient identifier that allows NCP A the unique mapping of this identifier onto the data indexing identifier.

REQ 3.6.34 Mapping of any data is Part of WP 3.5

This recommended process describes the case in which a HCP at PoC in Country B wants to access the health data of a patient of Country A. A patient is situated at PoC and is already identified and authenticated and a HCP is also already identified, authenticated and authorised for epSOS LSP and the level of trust from County A was accepted in Country B.

An access attempt to medical information of a patient is caused by three conditions: Country B is allowed for access to health data, accessed data are of allowed type and timeframe for consent is valid. Fulfilling these conditions, the national infrastructure in Country A retrieves health data from national registry and sends requested health data to a HCP in Country B (for details, see pictures and descriptions below).

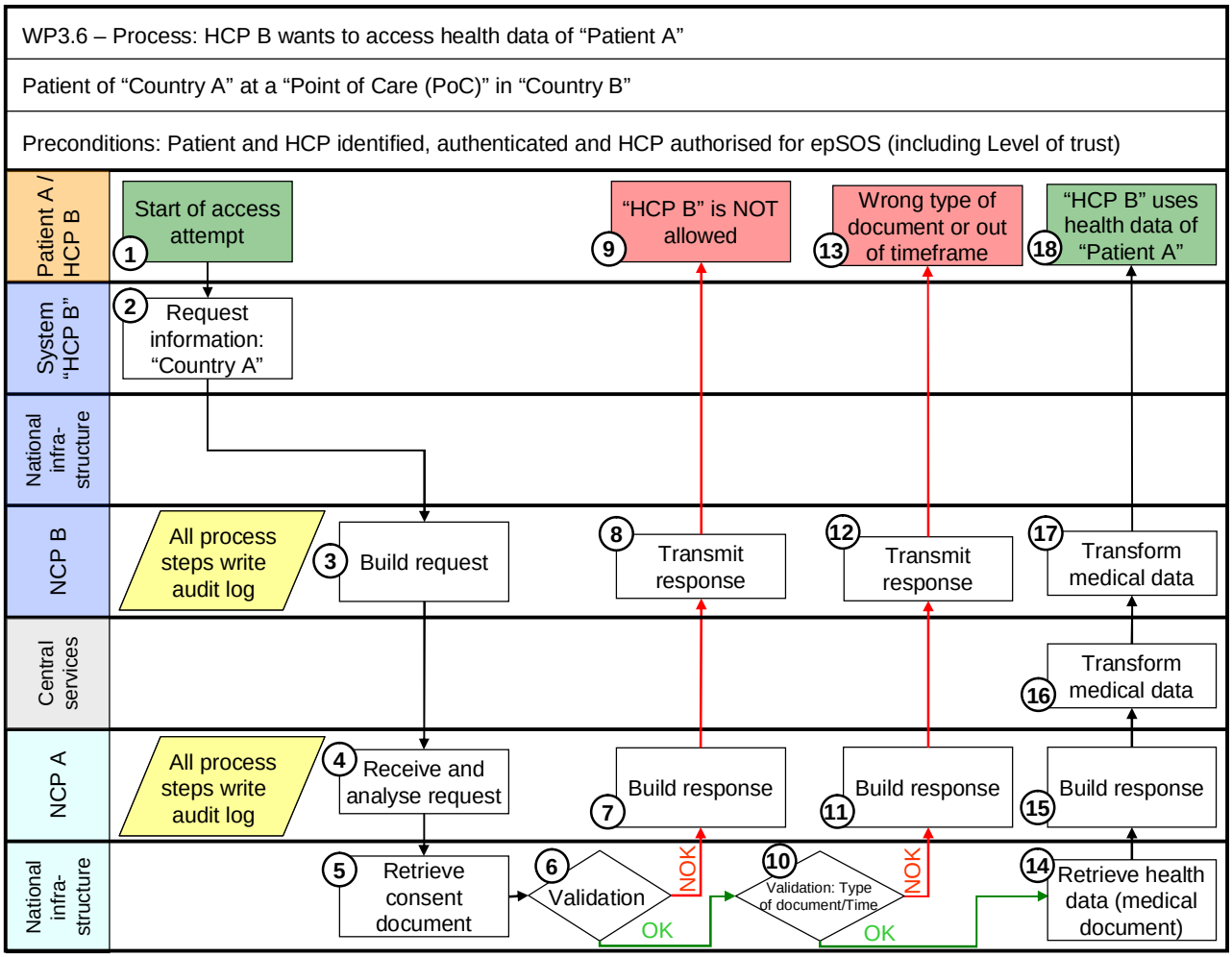

Figure 19 - Process of a HCP access to health data of a patient

The process is depicted in flow diagrams in Figure 19 and consists of the following steps:

1. HCP and patient are situated at the PoC in Country B and HCP wants to access medical information of patient – start of access attempt. The first step in this process includes the revalidation of the authorization of the HCP for epSOS LSP.
2. HCP from his local system requests NCP B for medical information from Country A.
3. NCP B receives the request from HCP system and writes an audit log. Then NCP B builds the request (or maps it to Country A) for NCP A for medical information and writes an audit log.
4. NCP A receives and analyses the request from NCP B and writes an audit log. The analysis includes the completeness, the roles and the level of trust.
5. Then NCP A confirms to NCP B the reception of the request and writes an audit log. NCP B receives the confirmation and writes to audit log. NCP A sends a request for medical information to national infrastructure in Country A and writes an audit log.
6. National Directory in Country A retrieves the consent document of patient.
7. The national infrastructure in Country A checks the status of patient consent for Country B
    a. The national infrastructure in Country A checks the status of patient consent for Country B

i. One of the following results is returned: patient consent for Country B is NO - Country B is not allowed - (continue on step 8) or patient consent for Country B is YES - Country B is allowed - (continue on step 11). If patient restricted some documents or selected only specific HCPs the document will not be sent to country B. This depends on national law of Country A and possible restrictions by a patient.

b. Checking of the role of epSOS LSP actors

i. Not all roles of epSOS LSP actors have access to the health data (depending on national laws of MS)

c. Checking of Level of trust

i. Process will continue depending of trust level.

8. NCP A receives from national infrastructure in Country A the result NO of consent for Country B and writes an audit log. NCP A builds the response (or maps it to Country B) to NCP B on result of consent and writes an audit log.
9. NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HCP and writes an audit log.
10. HCP's access to medical information of patient is refused, because Country B is not allowed to access this information – process is finished.
11. Additional Validation will be done:
    a. The national infrastructure in Country A checks the type of requested document (type of medical information). One of the following results is returned: patient consent for Country B is NO for this type of document (continue on step 12) or patient consent for Country B is YES for this type of document (continue on step 15)
    b. The national infrastructure in Country A checks the timeframe for consent (status YES) of the requested medical information. One of the following results is returned: the request is not within consented timeframe (continue on step 16) or the request is within consented timeframe (continue on step 15).
12. NCP A receives from national infrastructure in Country A the result NO of consent for type of document and writes an audit log. NCP A builds the response (or maps it to Country B) to NCP B on result of consent and writes an audit log.
13. NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HCP and writes an audit log.
14. HCP's access to the requested type of medical information of patient is refused – process is finished.
15. The national infrastructure in Country A retrieves the medical document (medical information) from national repository and sends it to NCP A.
16. NCP A receives from national infrastructure in Country A the medical document of patient and writes an audit log. NCP A builds the response (or maps it to Country B) to NCP B on medical document and writes an audit log.
17. NCP B receives the response from NCP A and writes an audit log. NCP B transmits the response to HCP and writes an audit log.
18. HCP uses the medical document of patient of Country A at PoC in Country B – the process is finished.

REQ 3.6.35 Any participating country must establish organisational procedures and functionalities to support the described process of accessing health data of patients from Country B.

REQ 3.6.36 Based on the analysis of the Member State-specific operation of the National Security Policies, epSOS must be able to communicate not only identity information but additionally a set of assigned attributes. A set of minimal attributes is proposed to be designed as follows:

Attribute	Mandatory	Constraints
ROLE	YES	medical doctors (general medical practitioners, special medical practitioner), nursing professionals, midwifery specialists, pharmacists, medical data administrators
SPECIALTY	NO	GP, urologist, cardiologist, etc.
COUNTRY-OF-CARE	YES	Country where health service is provided
ON-BEHALF-OF	NO	This attribute supports the legitimate delegation of rights to appointed medical assistance personnel. In many Member States, a HCP may delegate certain tasks to assisting personnel acting on his behalf with a subset of his access rights: e. g. nurse acting on behalf of a physician.[14]
TYPE-OF-ORGANISATION	YES	hospital, physicians practice, emergency car, etc.
PURPOSE-OF-USE	YES	standard, emergency, etc.
LEVEL-OF-TRUST	YES	This attribute gives a value for the authentication method and defines the mechanisms by which the subject of the issued assertion authenticates to the authentication authority (e.g. password versus smartcard).

Table 8 – Attributes in HCP access attempts to patient's health data

9.7 Process "HCP accessing health data of patient" (emergency case)

The main differences to the above described process is that the HCP identifies (if patient is responsive and not unconscious) the patient either with an e-ID, other identifiers or with demographic data (whatever is available) and the consent in Country A is NOT checked if the "PURPOSE-OF-USE" attribute is set to "EMERGENCY" in the request of health data.

REQ 3.6.37 For emergency access, special procedures must be designed. The HCP requesting an emergency access must specifically and doubtlessly state his intention and reason for the emergency data access request. This information must be forwarded to Country A as decision support for the access control decision.

REQ 3.6.38 Country A must be the place, where the particular emergency access decision is taken.

REQ 3.6.39 WP 2.1 has to check the different laws in the MS and to define the process for epSOS LSP.

[14] This attributes enables security policies based on functional roles, job titles, and real-world organisation of labour (delegation). Other solutions may be possible and also adequate and should be specifically investigated by WP 3.6.

9.8 Processes for Patient Identification/Authentication/Authorisation and Patient Consent

These processes description is for MS which have EHR implementations and the Patient has the right to access the system.

9.8.1 Identification, authentication and authorisation of a patient via internet portal

This process describes the case in which a patient identifies and authenticates himself for epSOS LSP in his country (Country A) from PoC in Country A and authorises a HCP at PoC for use of his health data. A patient has at his disposal credentials or eID that contains identification, authentication and authorisation data. These data is issued by the national authority (Country A) and stored in national infrastructure (national registry in Country A). The process of patient's identification and authentication for epSOS LSP might be performed twice, either using the national infrastructure (registry) twice or, if the first identification and authentication is not strong enough, the second one (level of trust is not less than x) should take place (for details, see pictures and descriptions below).

This process must not be installed, but in some MS it's installed yet.

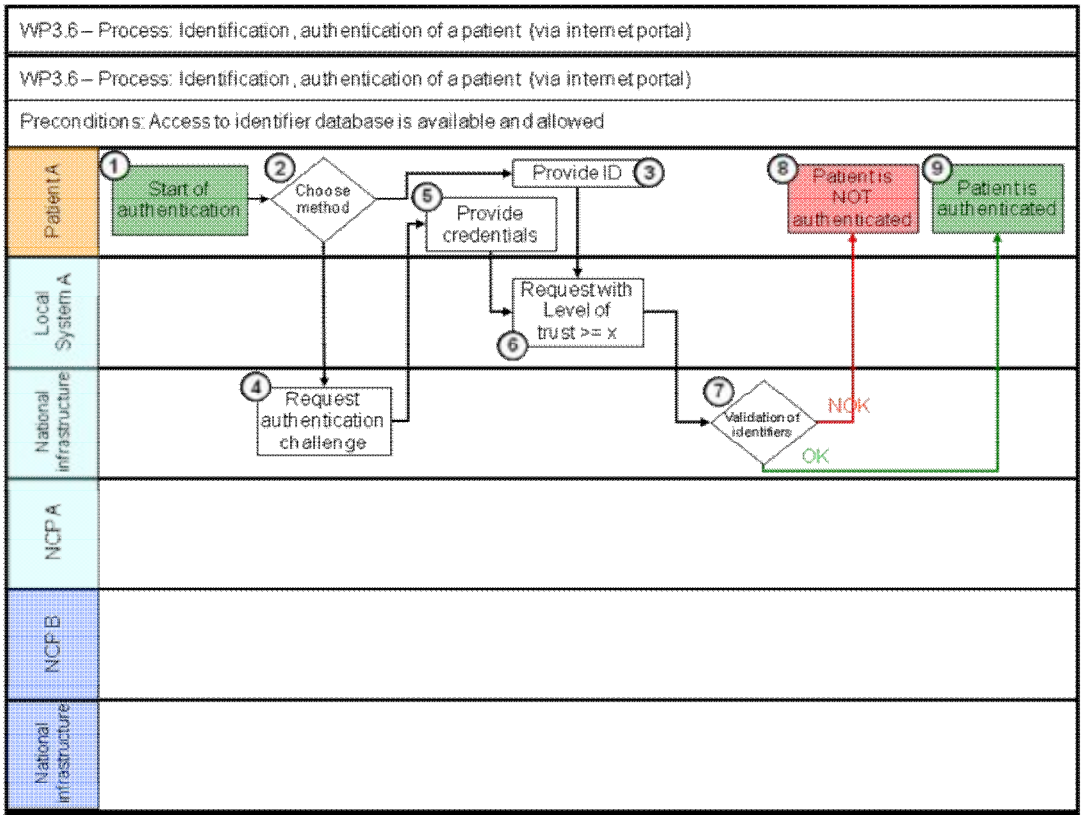

Figure 20 - Process of identification and authentication and authorisation of a patient via internet portal

The process is depicted in flow diagrams in Figure 21 and consists of the following steps:

1. Patient is situated at PoC Country A and wants to identify and authenticate himself for epSOS LSP – start of identification and authentication and authorisation process.
2. Patient can make a choice on identification and authentication method. Internet portal (national infrastructure) is either requesting logon data (continue on step 4) or eID (continue with step 3).

3. Patient owns a unique identifier (e.g. located in smart card) and provides it to a HCP at a PoC for identification and authentication and authorisation process. Continue on step 6.
4. Internet portal is requesting logon data.
5. Patient provides the credentials for identification and authentication and authorisation process.
6. Both identification and authentication and authorisation methods set the request for identification with trust level not less than x.
7. Entered identifier of a patient is validated by the identity verifier service in Country A. One of the following results is returned: patient is authenticated (continue on step 9) or patient is not authenticated (continue on step 8).
8. In case that patient is not authenticated, process is finished.
9. Patient is authenticated.

9.8.2 Patient gives/revokes consent anywhere in Country A

This process describes the case in which a patient is situated at “Any system” in his Country A and gives/revokes patient’s consent by himself. A patient is already identified, authenticated and authorized for epSOS LSP. A patient at “Any system” carries out a modification of the patient’s consent in national infrastructure (national repository in Country A). For information the consent modification document is printed out and patient archives one copy of document (for details, see picture and descriptions below).

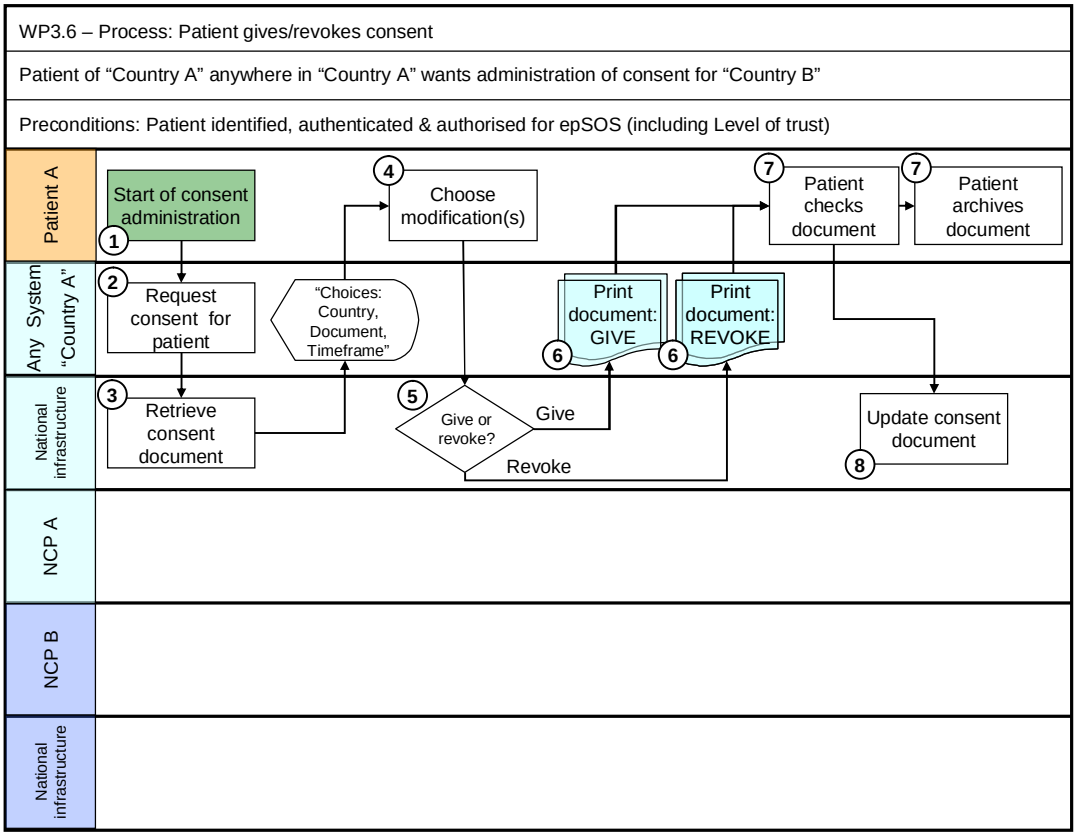

Figure 21 - Process of patient gives/revokes consent anywhere in Country A

The process is depicted in flow diagram in Figure 22 and consists of the **following** steps:

1. Patient is situated at any (local) system in Country A – start of consent management.

2. Patient uses any system and makes a connection to national infrastructure (national repository) and requests consent for patient.
3. On this request the national infrastructure retrieves a consent document (with choices such as country, document, timeframe (start and end date or duration of validity)) from national repository and sends document to „Any system“.
4. Patient chooses the modification(s) of consent document and sends modified consent document to national infrastructure.
5. The national infrastructure checks the validity of either opt-in policy or opt-out policy of modification(s) and sends to “Any system” either document „Patient gives consent” or document „Patient revokes consent“.
6. On “Any system” the document is printed out.
7. The printed document is checked by patient for correctness and patient archives one copy of document as information of consent modification.
8. After checking the document, a patient confirms the modification(s) to national infrastructure and national infrastructure updates the patient’s consent document in national repository. The process is finished.

REQ 3.6.40 Any participating country must establish organisational and technical procedures to support the management of patient’s consent by an authorised patient himself regardless of which of the above described processes for authorisation is used.

9.8.3 Additional future use of patient consent

The countries participating in epSOS LSP project or countries which will participate in epSOS LSP environment in the future may have jurisdictional or organizational policies required to support more complex patient consent policies. These policies may require that a patient explicitly consents to disclosure of protected or sensitive health information to specific entities. epSOS LSP provides a starting point for implementing these types of privacy consent policies, but does not explicitly specify what additional information will be needed to enforce these policies. An example of an Advanced Patient Consent would be when a patient wants to name individuals that can access her/his documents.

9.9 Additional Recommendations

If data hiding[15] is to be implemented and operated during the epSOS LSP-pilots, data hiding should be exclusively a national concern of the data controlling country.

REC 3.6.7 Future designs of the epSOS LSP services should enable the exchange of consent specific information, such as the way a patient consent was stated: orally, implicitly, explicitly (with signature).

REC 3.6.8 Future designs of the epSOS LSP services should provide patients the means to withdraw their consent by any Internet-enabled system.

REC 3.6.9 Future designs of epSOS LSP should provide patients with a procedure to view currently authorised actors (HCP, countries), as well as a list of who has actually accessed the patient’s health data (right of self-disclosure).

[15] “Data hiding” allows the patient to mark chapters of medical documents or even the whole document as invisible for HCPs.

10 Working methodology

The goal of WP 3.6 was defined in Annex I and the used Methodology is based on the guidelines of Project Management (PMI – Project Management Institute International – US). .

10.1 Approach of WP 3.6

WP 3.6 decided to proceed in following steps:

- Set up of 3 different Working Groups
  - WG (Work Group) A: Managing Time Frame and Scope of the other WGs
  - WG B: Define, Send Out and Analyze the Questionnaire to all MS
    - Questionnaire is a basic source of this document
  - WG C: Editors of Draft and Final Document
- Meetings/Tcons with different running EU Projects
  - HPRO
  - Stork
  - NETC@RDS
  - STepS
- Questionnaire with specific questions on Identification/Authentication
  - Questionnaire with questions depending of WP 3.6 were sent out to all MS
  - All MS, except Greece, answered the Questionnaire and sent it back
- Multiple Face-to-Face Meetings (see Chapter 10.4.1 Face-to-Face (F2F) Meetings)
  - Goals:
    - Harmonized opinion
    - To proceed the process
- Multiple TCons were set up (see Chapter 10.4.2 Telephone conferences (TCons))
  - Goals:
    - Harmonized opinion
    - To proceed the process
- Draft Document (D 3.6.1)
  - Developing Draft Document based on TCons and F2F meetings
  - 3 Reviews
    - 1 Internal Review (within WP Participants)
    - 2 External Reviews (members of epSOS LSP which were not beneficiaries of WP 3.6)
- Developing Final Document (D 3.6.2)
  - Developing Final Document based on Draft Document and Reviews
  - 2 Reviews
    - 1 Internal Review (within WP Participants)

§ 1 External Reviews

- members of WP 3.6
- all WPL of WP 3.x (WP 3.1 till WP 3.10)
- Additional: ANDA, ESNA, THESS

10.2 Timeline of WP3.6

WP 3.6 started official on April, 16th with the Kick Off in Milano and ended on Dec., 22nd 2009.

7 different Project Plans were developed and all of them are stored in Project Place (see TCon's)

10.3 Interdependencies to other EU Projects

The interdependencies to other EU Projects are described in Chapter 5 Interdependencies to other EU-Projects.

To get an overview about running different EU projects, WP 3.6 decided to set up different meetings (F2F, TCons). Target was to get an impression what can be taken over to WP 3.6.

Outcome of the meetings:
The other EU Projects are in Definition/Analyzing Phase and at the moment nothing can be taken over except process definitions for Identification with eID from Stork.

10.3.1 Meetings with HPRO

- Apr., 1st 2009
- Apr., 8th 2009 - TCon
- Apr., 15th 2009
- May, 6th 2009 – Workshop
- June, 29th 2009
- Sept., 28th 2009

10.3.2 Meetings with Stork

- Jan., 22nd 2009
- Feb., 17th 2009
- Mar., 23rd 2009
- Apr., 24th 2009
- Apr., 15th 2009
- May, 7th 2009 – Workshop

10.3.3 Meetings with STepS

- Feb., 17th 2009
- Mar., 26th 2009
- Apr., 23rd 2009
- Apr., 24th 2009
- June, 17th 2009
- July, 3rd 2009

- July, 30th 2009
- Aug., 17th 2009

10.3.4 Meetings with NETC@ARDS

- May., 15th 2009 – Workshop
-

10.4 Steps within WP 3.6

For a harmonized opinion within WP 3.6 and for faster progress, WP 3.6 decided to have different Face-to-Face Meetings (F2F), TCons (Telephone Conferences) and Workshops.

10.4.1 Face-to-Face (F2F) Meetings

All Minutes of F2F Meetings are stored in Project Place

- Apr., 16th 2009 : Kick Off in Milano
- Apr., 20th 2009 : Vienna
- Apr., 23rd 2009 : Vienna
- May, 18th 2009 : Vienna
- July, 28th 2009 : Vienna
- Sept., 3rd 2009 : Bratislava
- Oct., 5th 2009 : Vienna
- Nov., 25th 2009 : Vienna

10.4.2 Telephone conferences (TCons)

All Minutes of TCons are stored in Project Place

- Mar., 30th 2009
- April, 30th 2009
- May, 11th 2009
- May.,22nd 2009
- June, 3rd 2009
- June, 18th 2009
- June, 26th 2009
- July, 3rd 2009
- July, 10th 2009
- July, 17th 2009
- Sept., 4th 2009
- Sept., 11th 2009
- Sept.,22nd 2009
- Oct., 2nd 2009
- Oct., 16th 2009
- Nov., 13th, 2009

- Dec., 2nd 2009
- Dec., 14th 2009
- Dec., 17th 2009

10.4.3 Workshops

- Feb, 29th 2009 : SVC
- May, 6th 2009 – HPRO
- May, 7th 2009 – Stork
- May, 15th 2009 – NETC@RDS
- Dec., 14th 2009 : F2F Meeting in Vienna with WP 3.6 participants
- Dec., 21st 2009 : F2F Meeting in Vienna with WP 3.6 participants

10.4.1 Questionnaire

Questionnaire about Identification and Authentication of HCP's and Patients was sent out at the end of April 2009. All Countries, except Greece, answered the questionnaire.

10.5 Participants of WP 3.6

Beneficiary	Committed Person/Month
ELGA (WPL)	9,0
SALAR	3,0
IZIP	3,0
Gematik	2,0
Medcom (Digital Health)	2,0
CLM	6,0
GIPDMP (AZIP)	3,0
FRNA	1,0
Lombardy	3,0
NICTIZ	3,0
NHIC	1,0 (extended to 6,0)
NHS	6,0
FHGISST	2,0
Industry Team	2,3 (extended to 3,3 after Kick-Off)

Table 9 – Beneficiaries of WP 3.6

11 Abbreviations

CA - Certification Authority

CIS – Clinical Information System

CoT – Circle of trust

EC – European Communities

EHIC - European Health Insurance Card

EHR – Electronic Health Record

eID – electronic IDentity

epSOS LSP – european patient Smart Open Services

EU – European Union

GP – General Practitioner

HCP – Health Care Professional

HCPO – Health Care Provider Organization

HIS - Hospital Information System

HPRO Card – Health PROfessional Card

ID – Identification

ISIC – International Student Identification Card

ISO/IEC – International Organization for Standardization / International Electrotechnical Commission

IT – Information Technology

ITIC - International Teacher Identification Card

LET – Legal Experts Team

MS – Member State

NCP – National Contact Point

NSP – National Security Policy

OID – Object Identifier

PEB - (epSOS LSP) Project Executive Board

PEPPOL - Pan European Public Procurement on-line

PIN – Personal Identification Number

PoC – Point of Care

PPP – Patient Privacy Policy

PS – Patient's Summary

SPOCS - Simple Procedures Online for Cross-border Services

SSL – Secure Sockets Layer

STORK - Secure Identity Across Borders Linked

TLS – Transport Layer Security

WP – Work Package of epSOS LSP

12 Glossary

This glossary contains the most important terms (medical and technical) used in the present document. Some basic definitions are adopted from WP5.2.1. Project glossary and other necessary terms defined in various epSOS LSP documents or international standards are added.

Access – (1) Capability and opportunity to gain knowledge of or to alter information or material. (2) Ability and means to communicate with (i.e. input to or receive output from), or otherwise make use of any information, resource, or component in a system**.**

Access control - The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical **facilities.**

Assertion - A set of statements that can be evaluated by an authority (usually an Identity Provider) concerning an entity. The statements can be concerning identifying information (e.g. name) as well as attributes (e.g. role).

Attribute - **Property or a characteristic of an** entity.

Audit - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Authentication - Formalized process to create a validated identity for a claimant, based on the value of one or more attributes of its identity.
Note: Authentication typically involves the use of a policy to specify a required level of assurance in the result after a successful completion of the process.

Authenticity - **The** property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.

Authorisation - **Process** to approve a temporary granting of a set of privileges to an entity. The privileges enable the entity to access to some sources or to use some services of a system. Authorisation is based on policy rules for permitting an activity in a particular system.

Availability - The property of a system or a system resource being accessible, or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.

Claimant - **Entity** that initiates an authentication of its identity.

Clinical Information System – Solutions of Primary Care Centers, GP's for documentation and **Prescription.**

Confidentiality - The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

Context - **Property** of an attribute that specifies the meaning and possible values of the attribute (the same attribute, e.g. a number can have different meaning in various contexts.)

Country A - **This** is the home country of the patient which holds information about the patient, where the patient can be univocally identified and his data may be accessed.

Country B - **This** is the country (different from Country A) in which information about a patient is needed in **case the** patient needs healthcare.

Cross-border interoperability - Interoperability between neighbouring and non-neighbouring Member States and their entire territories

Data Controller - The natural or legal person, public authority, agency or any other entity which alone or together with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law [Dir 95/46/EC].

Data Processor - **Natural** or legal person, public authority, agency or any other body which processes personal data on behalf of the controller [Dir 95/46/EC].

Dispenser - **Health** care professional who provides the order of a prescription. The professional person must be authorised to do so.

Domain of applicability - **Domain** (area, space) where an entity can use a set of attributes for identification and other purposes (e.g. epSOS LSP environment, eHealth systems of a MS).

Electronic Health Record - Comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related **purposes.**

Electronic Health Record System - **System** for recording, retrieving and manipulating information in electronic health records**.**

Electronic Prescription ("ePrescription") - Medical prescription, provided in electronic format: "A prescription is understood as a set of data like drug ID, drug name, strength, form, dosage, indication or as a list of drugs together covering the patients current medication. The dataset might differ slightly between the countries." In the context of epSOS LSP, this definition of ePrescription data will apply. However, it is not excluded that the use of the infrastructure and the service developed in epSOS LSP might be afterwards extended to handle ePrescription data different from medicinal prescriptions.

Enrolment - Process consisting of identity proofing and identity registration to allow an entity to be known within a particular domain of applicability.
Note: In general enrolment collates and creates identity information for storage in an identity register to be used in subsequent authentication of the entity in the domain of applicability. It is the start of the lifecycle of an identity in the domain of applicability for an entity.

Entity - **Natural** person, organisation, active or passive object, device or group of such items that has an identity. (Patient, HCP, HPCO, patient summary, patient consent documents are entities of the epSOS LSP environment).

epSOS LSP environment - **Synonym** for all systems and other entities which are needed to perform the described processes of health data exchange abroad with respect to the requirements stated by all work packages of epSOS LSP.

Health Care Professional - **Doctor** of medicine or a nurse responsible for general care or a dental practitioner or a midwife or a pharmacist within the meaning of Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC . This means that a Health Care Professional is a person who delivers health care or care products professionally to any individual in need of health care services, in order to prevent, relieve or treat a medical problem. A Health Care Professional must be related to at least one HCPO (see below).

Health Care Professional Organization or **Health Care Provider Organization** - **An** institution, authorised to provide health care services, univocally identified in the set of the Health Care Institutions. Examples: Health Center / Hospital / Medical Emergency Vehicle / Medical Practice / Pharmacy.

Health Care Provider Organisations - **Associations** or federations of health care providers, **who** search a benefit from coordinating or associating among them. Health services provider

organisations can include GP practices, general hospitals, specialised hospitals, teaching and university hospitals, social care organisations, and so on.

Health Care Service Provider - **Organisation** that delivers proper health care in a systematic way professionally to any individual in need of health care services. It is an entity that provides, coordinates, and/or insures health and medical services for people (International Classification for Patient Safety, World Health Organization). They can vary considerably in size (they range from small organisations run by a single person, through medium sized commercial enterprises, to large Trusts). They can be commercial, public or non-profit (Picker Institute). Examples: hospitals, home health agencies, clinics, nursing homes, ambulance companies, and the health care provider corporations formed by individuals.

Hospital Information System – Implemented Solutions in Hospitals for documentation, accounting, etc. HIS delivers PS, eP for epSOS LSP.

Identification - **Process** to determine that presented identity information associated with a particular entity is sufficient for the entity to be recognized in a particular domain of **applicability.**

Identifier - **Non**-empty set of attribute values that uniquely characterize an entity in a specific domain of **applicability.**

Identity - Set of attributes related to an entity.
Note: Each entity is represented by one holistic identity, which comprises all possible information elements characterizing such entity (the attribute). Since such identity can be very large, even infinite for practical purposes only a subset of relevant attributes represents the entity. (e.g. name, address, date of birth, passport number, etc.).

Identity authority - **Entity** related to a particular domain of applicability that can make authoritative assertions on the validity of one or more attribute values in an identity.

Identity evidence - **Identity** information pertaining to an entity required for successful enrolment of the entity.

Identity federation - **Agreement** between two or more identity authorities to mutually recognize credentials for authorisation
Note: Establishing an identity federation typically includes an agreement on the use of common protocols and procedures for privacy control, data protection and auditing and the use of standardized data formats and cryptographic techniques.

Identity information - Set of values of attributes in an identity.

Identity provider (IdP) - Entity that makes available identity information and entity that operates the functions necessary to complete authentication.
Note: A verifier may be the same as or act on behalf of the entity that controls identification of entities for a particular domain of applicability.

Identity reference - **Attribute** that is an identifier and that persists in a domain of applicability for the existence of the entity.

Identity register (IDMS register) - **Repository** of identities for different entities indexed by their identity reference during enrolment.

Note: the identity reference may exist longer than the entity.
Examples: driver license' number, the number printed on a membership card, a phone number

Integrity - The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Level of Assurance (Level of Trust) - A risk category for objects to be protected. It defines the set of required security controls to reduce the risk to an acceptable level. The purpose is to hide the particular implementation details of a security policy on the level of a single electronic transaction.

Medical Record or Health Record – **A Systematic** documentation of a patient's medical history and care. The term 'Medical record' is used both for the physical folder for each individual patient and for the body of information which comprises the total of each patient's health history. Medical records are highly personal documents and there are many ethical and legal issues surrounding them such as the degree of third-party access and appropriate storage and disposal. Although medical records are traditionally compiled and stored by health care providers (HCP) personal health records maintained by individual patients have become more popular in recent years.

Medicinal Prescription - Any medicinal dispensation issued by a professional person qualified to do so.

National Contact Point (NCP) - **Organisations** delegated by each participating Country, acting as a bidirectional way of interfacing between the existing different national functions provided by the national IT infrastructures and those provided by the common European infrastructure, created in epSOS LSP. The NCP takes care of external and internal national communication and functions in epSOS LSP and the semantic mapping (if necessary) between information on either side. The NCP also acts as a kind of mediator as far as the legal and regulatory aspects are concerned. The NCP creates the conditions (by supporting trust, data protection and privacy) for a trusted relationship with other countries' NCPs.

Need-to-know - The term "need to know", when used by government and other organizations, describes the restriction of data which is considered very sensitive. Under need-to-know restrictions, even if one has all the necessary official approvals (such as a security clearance) to access certain information, one would not be given access to such information, or read into a clandestine operation, unless one has a specific need to know; that is, access to the information must be necessary for the conduct of one's official duties.
As with most security mechanisms, the aim is to make it difficult for unauthorized access to occur, without inconveniencing legitimate access. Need-to-know also aims to discourage "browsing" of sensitive material by limiting access to the smallest possible number of people.

Need-to-know principle - **A** basic requirement of data protection and therefore found in data protection legislation. Data protection guideline 95/46/EG states this in item (28): "the data must be adequate, relevant and not excessive in relation to the purposes for which they are **processed**". Necessity is also stated in article 7.

Non repudiation - **The** security service by which the entities involved in a communication cannot deny having participated. Specifically the sending entity cannot deny having sent a message (non-repudiation with proof of origin) and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery).

Patient - **Any** natural person who receives or wishes to receive health care in a Member **State.**

Patient consent provided to the data controller - **Any** freely given specific and informed indication of his/her wishes by which the data subject signifies his agreement to personal data relating to him/her being processed.

Patient Summary - **Minimum** set of patient's data which would provide a health professional with essential information needed in case of unexpected or unscheduled care (emergency, accident...) and in case of planned care (citizen movement, cross-organisational care path...).

Personal data - Set of data directly linked to a physical person and used to identify and authenticate this person.

Point of Care – Any location where health care is provided.

Privacy - **The** right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Profile - **Identity** that contains attributes that are relevant in the interactions with one or more distinct domains of applicability by the entity associated with the identity

Relying Party - An individual or organization providing a service that depends on identity provider about a subject to control access to the service.

Role - A role typically implies a collection of privileges to access or use resources available in a domain of applicability (the most important roles in epSOS LSP are patient and various kinds of **HCP).**

Validation - **P**rocess to determine that presented identity information associated with a particular entity is applicable for the entity to be recognized in a particular domain of applicability at a point in time.
Note: validation usually involves verifying the syntax, and correctness of attribute values, controlling their validity status and matching them with the requirements to recognize an entity.

13 References

[1] Smart Open Services - Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription, Annex I – "Description of Work", 2008

[2] The epSOS LSP Security Policy, WP 3.7 Version 0.1

[3] epSOS LSP Architecture – Consolidated Works, WP 3.3., Version 0.4, 20/08/09

[4] ISO/IEC 27002, Information technology -- Security techniques – Code of practice for Information security management

[5] ISO/IEC 9798 (all parts), Information technology -- Security techniques – Entity Authentication

[6] ISO/IEC 29146, Information technology -- Security techniques – A framework for access management

[7] ISO/IEC 1st CD 24760 Information technology -- Security techniques – A framework for identity management

[8] Directive 95/46/EC of the European Parliament and of the Council of 14 October 1995 on the protection of individuals with regard to the processing personal data and on the free movement of such data

[9] Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications

[10] Marshall G.: Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications, RFC 3881, The Internet Society (2004)

[11] Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

14 List of Figures

15 List of Tables

16 Annex I Overview about requirements/recommendations and responsibilities

The following table summarizes the analysed requirements/recommendations and specifies who must handle them.

Requirement/ Recommendation	Chapter	Handled by			Remark
		WP 3.6	Other WP	National domain	
REQ 3.6.1	3.4		3.7	**P**	Appropriate values for level of trust
REQ 3.6.2	7.2		3.8 3.9	**P**	National identity registers
REQ 3.6.3	7.3.2		3.8 3.9	**P**	One (out of three) identification and authentication processes for patients
REQ 3.6.4	7.3.2.3		3.8 3.9	**P**	Wildcards in demographic queries
REQ 3.6.5	7.3.2.3		3.8 3.9	**P**	Handle “more than one” demographic matches
REQ 3.6.6	7.4.2.5		3.3 3.7 3.8 3.9	**P**	Health data administrator
REQ 3.6.7	7.5		3.3 3.8 3.9		Consent in Country B for Country B
REQ 3.6.8	7.5		3.3 3.8 3.9		Confirm consent in Country B
REQ 3.6.9	7.5		3.3 3.7 3.8 3.9		Entries in audit log Country A
REQ 3.6.10	7.5		3.7 3.8 3.9		Entries in audit log Country B
REQ 3.6.11	7.6		3.8	**P**	Audit log extraction on patient’s request (Country A)
REQ 3.6.12	7.6.1		3.3 3.7	**P**	Audit trail definitions
REQ 3.6.13	7.6.2		3.7		Audit process description
REQ 3.6.14	7.6.2		3.7		Audit log encryption
REQ 3.6.15	8.1.5		2.1	**P**	Patient consent templates
REQ 3.6.16	8.1.5		2.1 3.3	**P**	Language of patient consent
REQ 3.6.17	8.2		3.5	**P**	epSOS LSP HCP Roles
REQ 3.6.18	8.3		3.7	**P**	Expected accuracy of identifiers must be

					predefined
REQ 3.6.19	8.5		3.9	**P**	Test cases and test plans
REQ 3.6.20	8.6		3.9 ff	**P**	Interfaces NCP – national infrastructure
REQ 3.6.21	8.8		3.9	**P**	Using ASCII characters (ISO 646)
REQ 3.6.22	8.9		3.4	**P**	Confirmation Check
REQ 3.6.23	9.2.1	**P**	3.8	**P**	Patient's authentication with demographic data
REQ 3.6.24	9.2.1	**P**	3.8	**P**	Patient's authentication with extended demographic data
REQ 3.6.25	9.3	**P**	3.4 3.7	**P**	Existence and location of patient consent
REQ 3.6.26	9.3		3.8 2.1	**P**	Withdrawing patient consent
REQ 3.6.27	9.3		3.3 3.8	**P**	Self-disclosure
REQ 3.6.28	9.3		2.1 3.8	**P**	Consent for Country B may be different from consent for Country A
REQ 3.6.29	9.3		2.1 3.8	**P**	Patient consent regards to countries not to organisations
REQ 3.6.30	9.3.2	**P**	2.1	**P**	Consent for Country B modified in Country B
REQ 3.6.31	9.3.3		2.1	**P**	Consent confirmation
REQ 3.6.32	9.4.1		3.8 3.9	**P**	HCP directory
REQ 3.6.33	9.5		3.8 3.9	**P**	Processes for audit log extraction
REQ 3.6.34	9.6		3.5	**P**	Mapping of transactions
REQ 3.6.35	9.6		3.9	**P**	Access to patient's health data
REQ 3.6.36	9.6		3.3 3.4 3.9	**P**	Transmitted attributes in health data access attempts
REQ 3.6.37	9.7		3.8 3.9	**P**	Processes for emergency cases
REQ 3.6.38	9.7			**P**	County A decides in emergency cases
REQ 3.6.39	9.7		2.1		Laws regulating emergency cases
REQ 3.6.40	9.8.2		2.1 3.9	**P**	Process for consent administration by patient
REC 3.6.1	9.1.1			**P**	HCP with eID
REC 3.6.2	9.1.2			**P**	HCP via internet portal
REC 3.6.3	9.1.3			**P**	HCP processes within existing local systems
REC 3.6.4	9.2.2			**P**	Patient with eID
REC 3.6.5	9.3.1			**P**	Consent management via internet

REC 3.6.6	9.3.4			**P**	Combined process for give/revoke consent and confirmation
REC 3.6.7	9.9				How consent was stated
REC 3.6.8	9.9				Withdrawing consent via internet
REC 3.6.9	9.9				Check consent and accesses via internet

Table 10 - epSOS LSP identity management requirements and recommendations

17 Annex II Additional EU Projects

For Identification of citizens EU set up different additional projects which were not checked by the members of WP 3.6.

17.1 FIDIS (Future of Identity in the Information Society)

Link: http://www.fidis.net/home/

The Future of Identity in the Information Society (FIDIS) is a large EU-sponsored NoE (Network of Excellence) targeting various aspects of digital identity and privacy. The partners of the project are universities and companies working in areas related to digital identity. FIDIS areas of interest include new forms of ID cards, usage of identifiers in information systems, technologies used for citizen's identification and profiling. The activities of FIDIS officially ended with the closing event in May 2009

FIDIS objectives are (1) to analyse various concepts of identity, (2) to analyse current and future instruments for Identity management (IdM) from an interdisciplinary perspective, (3) to build up definitions, taxonomies and classification systems, and (4) to give advice to stakeholders in European governments, the economic sector and citizens:

- "Identity of Identity"
- Profiling
- Interoperability of IDs and ID management systems
- Forensic Implications
- Privacy and the legal-social content of identity
- HighTech ID
- Mobility and Identity

As a multidisciplinary and multinational NoE FIDIS, appropriately, comprises different Country research experiences with heterogeneous focuses, and integrates European expertise around a common set of activities. Additionally, all relevant stakeholders are addressed to ensure that the requirements are considered from different levels. FIDIS overcomes the extreme fragmentation of research into the future of identity by consolidating and fostering joint research in this area. Research results will be made accessible to European citizens, researchers and in particular to SMEs. FIDIS will accomplish ERA objectives by durably integrating the research implementation efforts, as well as the medium term target setting, and in the long run the strategic objective planning.

17.2 PRIME (Privacy and Identity Management for Europe)

Link: https://www.prime-project.eu/

- Timeframe: 2004/03 – 2008/06

17.3 PICOS (Privacy and identity management for community services)

Link: http://cordis.europa.eu/search/index.cfm?fuseaction=prog.document&PG_RCN=8737572

- Timeframe: 2007/01 – 2013/12

17.4 PRIMELIFE (Privacy and identity management in Europe for life)

Link: http://cordis.europa.eu/search/index.cfm?fuseaction=prog.document&PG_RCN=8737572

- Timeframe:2008/03 – 2011/02

18 Annex III Personal identifiers used in European States

Country	Health Identifier / token	Type	Comments
Austria	social security number / health insurance card or citizen card		10-digit number nnnc-ddmmyy (nnn .. serial, c .. check-digit, date of birth
Belgium	Identification Number Social Security (INSS) / Social Information System card (SIS card)		the INSS number is usually the RRN number (national register number)
Croatia	Health Insurance Number / CIHI card (Croatian Institute for Health Insurance)		
Cyprus	social insurance number		derived from unique national identifier
Czechia	Personal Identity Number		
Denmark	Danish Central Personal identification number / social security card		
Estonia	PIC Number / ID card		
Finland	FINUID Number / healthcare card, FINEID card		SSIN number for health care providers
France	NIR - numéro national d'inscription au répertoire des personnes physiques / VITALE card		NIR: 13 digit coding the gender, date, province and city of birth
Germany	Health Insurance Number / electronic health card eGK being introduced		
Greece	Health Identifier/token --> Social Security Number (AMKA). Comments--> AMKA number is stated on a simple card (not a smart card). As of 1/10/2009 AMKA has been attributed to all insured individuals (working or not).		
Hungary	Social Security Number		
Iceland	Social Security Number (SSN#) / ID card		
Ireland	Personal Public Service (PPS) Number		7 digits + 1 letter
Italy	Tax Number (Fiscal Code) / health card; CNS card		
Latvia	?? / health insurance card		
Lithuania	?? Peronsal ID Code ??		
Luxembourg	identity number		sequence number + date of birth + gender + check digit
Malta	national identity number or social security number		
Netherlands	Citizen Service Number		
Norway	?? Personal Identity Number ?? / health insurance card		
Poland	PESEL number		
Portugal	health user number / citizen card (replacing Social Security card and National Health Service card)		
Romania	?? (national health insurance card postponed)		

Spain	National register number / eHealth Card, DNI card		If it is of ant use: the type will be unique through the health card number (different from the insurance number). There are regional databases connected with the national database so everyone has a unique national number and can have different regional ones linked to the national.
Slovakia	?? birth number ??		
Slovenia	unique identification insurance number (HIIS) / health insurance card		
Sweden	Personal Identity Number		date of birth + serial number + check digit
Turkey	?? / Health card project launched		
United Kingdom	NHS number (national health service number)		

Table 11 - Person Health Identifiers

Country	eGovernment Identifier	Type	Comments
Austria	Source PIN	unique	sector-specific identifiers are derived from source-PIN
Belgium	RRN Number	unique	national register number
Bulgaria	Unified Citizen Number - UCN	unique	
Croatia	Personal Identification Number	unique	
Cyprus	Single Identification Number	unique	assigned at birth
Czechia	Personal Identity Number	unique	
Denmark	Central Personal Identification Number	unique	
Estonia	PIC Number	unique	
Finland	FINUID Number	unique	
France	National Registration Number - NIR (numéro d'inscription au repertoire)	unique	
Germany			
Greece	eGoverment Identifier --> Identity Number. Type --> Unique. Comments--> 1letter + 6 digits		
Hungary	Personal Identification Number		11 digit, including gender and date of birth
Iceland	ID-Number (SSN#)	unique	
Ireland	Personal Public Service (PPS) Number	unique	7 digits + 1 letter
Italy	Tax Number (Fiscal Code)	unique	LLL LLL DDLDD LDDD L Surname + Name + Year of birth + Month of Birth + Day of birth + 0 = Male or + 40 = Female + Catastal code for city of birth + Check-Sum
Latvia	Personal Identity Number	unique	

Liechtenstein			
Lithuania	Peronsal ID Code	unique	
Luxembourg	Identity Number	unique	sequence number + date of birth + gender + check digit
Malta	Identity Number	unique	
Netherlands	Citizen Service Number - BSN (BurgerServicenummer)	unique	
Norway	Personal Identity Number	unique	
Poland	PESEL Number	not unique	
Portugal	* Personal Identification Number * Social Security Number * Tax Number * Health User Number	-	Depending on the sector, the suitable number is chosen
Romania	Personal Numeric Code - PNC (Cod numeric personal)	unique	
Spain	Personal ID Number	unique	
Slovakia	Personal Identifier (birth number – rodné číslo)	unique	
Slovenia	Personal Registration Number	unique	
Sweden	Personal Identity Number	unique	
Turkey	Turkish Republic Identification Number	unique	
United Kingdom			

Table 12 - eGovernment Identifiers