



# 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

### WP3.7

D.3.7.2. FINAL SECURITY SERVICES SPECIFICATION DEFINITION  
- Master document -

WORK PACKAGE	<b>3.7</b>
DOCUMENT VERSION	0.4
DATE	<b>16/06/2010</b>

### Document Information

<b>Project name</b>	Smart Open Services – Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription
<b>Author/ person responsible</b>	Eliberto Albertini (LOMBARDY)
<b>Document name</b>	WP3.7_D3.7.2_Security_Services_V04.doc
<b>Status</b>	in process   submitted to QA   accepted by QM   <b>approved</b>
<b>Dissemination level</b>	<b>PUBLIC</b>

### Sub-Project Identification

<b>Work Package</b>	WP3.7
<b>Working Tasks</b>	
<b>Document Owner</b>	Eliberto Albertini (LOMBARDY)

### History of Alteration

Version	Date	Type of editing	Editorial
0.1	11-30-2009	First draft for internal review	LOMBARDY
0.2	12-28-2009	Draft after ASIP / ELGA / NICTIZ / MEDCOM/ NHIC / THESS / CLM Comments	LOMBARDY
0.3	21-01-2010	Final (QR) after ELGA, CLM comments	LOMBARDY
0.4	02-02-2010	Final after QR comments (ANDA,ESNA,NHS,GEMATIK,ELGA)	LOMBARDY

### Referring Documents (input)

#	Date	Type	Description	Ver	Origin
01	2008-06-30	.pdf	Annex I – “Description of Work”		EMP/S.O.S. LSP-eHealth team
02	2009-01-31	.pdf	D2.1 Legal and regulatory constraints on epSOS		WP2.1
03	2009-06-28	.doc	The epSOS trusted domain. Consolidation of concepts		WP2.1
04	2007-02-15		WP 131. Working Document on the processing of personal data relating to health in electronic health records (EHR)		Article 29 Data protection Working Party
05	1995-10-24		95/46/EC EU data protection directive		European Parliament
06	Dec 2003		FIPS 199. Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems		USA Department of Commerce, National Institute of Standards and Technology
07	June 2009		epSOS –Concepts Paper		WP2.1
08	2005		ISO/IEC TR 13335 - Parts 1 to 5 Information technology – Guideline for the management of IT Security		International Organization for Standardization; International Electrotechnical Committee
09	2008		ISO/IEC 27000 – Part 1 to 6 Information Security Management System Standard		As above

### Referred Documents

#	Date	Type	Description	Origin
1	Dec 2009	.doc	D3.7.2 GLOSSARY	WP 3.7
2	Dec 2009	.doc	D3.7.2 – Section I – EpSOS Security Policy	WP 3.7
3	Dec 2009	.doc	D3.7.2 – Section II – EpSOS Security Services	WP 3.7
4	Dec 2009	.doc	D3.7.2 – Section III – EpSOS Suitability Analysis	WP 3.7.



## INDEX

<b>1</b>	<b>D3.7.2 DELIVERABLE. PHYSICAL ORGANIZATION &amp; CONTENTS.....</b>	<b>6</b>
1.1	Contents of “Master document”.....	6
<b>2</b>	<b>INTRODUCTION.....</b>	<b>9</b>
2.1	Goals of the WP3.7 Work Package.....	9
2.2	Glossary & Abbreviations.....	9
<b>3</b>	<b>ASSUMPTIONS &amp; GUIDELINES.....</b>	<b>10</b>
3.1	Security View.....	10
3.1.1	Objectives prioritization.....	10
3.1.2	Indications for choice of security measures.....	11
3.2	Risk Analysis.....	11
3.3	Recommendation to the functional specification team.....	11
<b>4</b>	<b>OVERALL PICTURE &amp; LOGICAL SCHEME.....</b>	<b>12</b>
4.1	Overall picture.....	12
4.2	epSOS LSP Security challenges.....	13
4.2.1	Security challenges.....	13
4.2.2	Security core concepts.....	14
4.3	Logical scheme.....	14
<b>5</b>	<b>DEFINITION OF ELEMENTS AND ACTORS RELEVANT FOR SECURITY ISSUES..</b>	<b>17</b>
5.1	Data classification.....	17
5.2	Actors.....	18
5.3	Actors from a security point of view.....	19
<b>6</b>	<b>SECURITY REQUIREMENTS.....</b>	<b>20</b>
6.1	Security requirements for the epSOS LSP Project level.....	22
6.2	Security requirements for a National Contact Point (NCP) level.....	23
6.2.1	Environmental and operational NCP security requirements.....	25
6.3	Acceptable common security requirements for the different National Information Systems (NIS) level.....	27
<b>7</b>	<b>Reference to SECTION I SECURITY POLICIES.....</b>	<b>29</b>
<b>8</b>	<b>Reference to SECTION II SECURITY SERVICES.....</b>	<b>29</b>
<b>9</b>	<b>Reference to SECTION III SUITABILITY ANALYSIS.....</b>	<b>29</b>
<b>10</b>	<b>QUESTIONNAIRE (Analysis of the Security aspects in MSs).....</b>	<b>29</b>
10.1	Introduction for the use of a questionnaire.....	29
10.2	Questionnaire layout.....	29
10.3	Analysis.....	30
<b>11</b>	<b>ANNEX. WP3.7 ORGANIZATION AND TIMING.....</b>	<b>34</b>
11.1	WP 3.7 Organization.....	34
11.1.1	Authors and reviewers list.....	34
11.1.2	Description of tasks and responsibilities.....	34
11.1.3	EWG Editing process.....	36
11.1.3.1	Project Place (PP).....	37
11.1.3.2	Stepping through the WP3.7 editing process.....	37
11.1.4	EWG Leader task list.....	38
11.2	WP 3.7 Working Methodology.....	38

11.2.1	Selection of the participants in the tasks in WP3.7 .....	39
11.2.2	Tools used for sharing information .....	39
11.2.3	Methodology for generation of consensus report .....	39
11.2.4	Methodology for conflicts resolution .....	40
11.3	WP3.7 Final timing.....	40

### INDEX OF THE FIGURES

Figure 1-1:	Management of IT Security (ISO/IEC TR 13335-3) .....	7
Figure 4-1:	Overall picture of the epSOS LSP Project.....	12
Figure 4-2:	. epSOS LSP Trusted Domain .....	13
Figure 4-3:	Security logical scheme .....	14
Figure 6-1:	Diagram of the security requirements definition process.....	21
Figure 11-1	WP 3.7 Activities Plan .....	42

### INDEX OF THE TABLES

Table 5-1:	Impact dependent on threat and data class.....	18
Table 5-2:	impacts level .....	18
Table 5-3:	Actors Access Rights and Auth. level.....	19
Table 11-1:	WP 3.7 Contributors list.....	34
Table 11-2:	EWGA Contributors list.....	35
Table 11-3:	EWGB contributors list .....	36
Table 11-4:	EWGC contributors list .....	36
Table 11-5:	EWGD contributors list .....	36
Table 11-6:	WP 3.7 PP structure .....	37

## **1 D3.7.2 DELIVERABLE. PHYSICAL ORGANIZATION & CONTENTS**

The process of the management of epSOS Security is based on the principles as defined in ISO/IEC TR 13335 (ISO/IEC 27000). Figure 1-1 shows the major steps of this process and acts as a guide line in describing the contents of this WP deliverable.

As shown in Figure 1-1, WP3.7, involved in the Requirement Specification phase of epSOS project, analyses and describes the process up to the selection of the safeguards that will be necessary for the NCP to NCP data exchange security.

WP3.7 also provides high level security policies and requirements covering the security of the data exchange between the MS pilot sites and the MS NCP. These security policies and requirements shall be further analysed and refined in each MS depending on the MS customization and integration of NCP with pre-existent Health Information Systems.

### **1.1 Contents of “Master document”.**

The D3.7.2 deliverable contains by four separate documents, as follows:

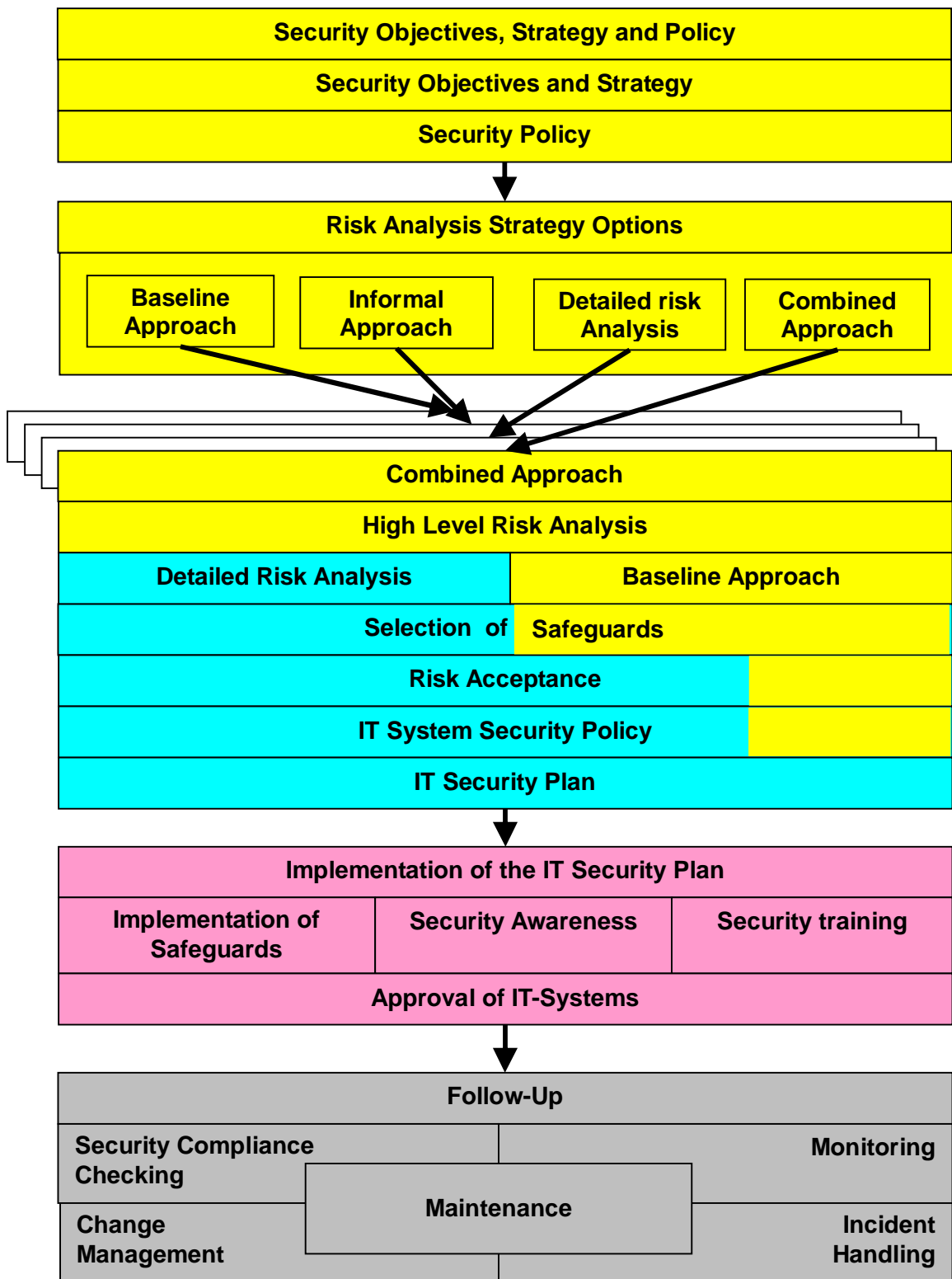
- 1st document (this one): the “Master document”;
- 2nd document: the “epSOS Security Policies”;
- 3rd document: the “Security Services description”;
- 4th document: a “Congruity and Suitability analysis”

The Master document describes the process of the management of epSOS Security; the risk analysis carried out and the safeguards selected; the WP 3.7 Organization and activities.

The second document provides the epSOS high level Security Policy description. This description will form the base of the “epSOS Agreements Annex III Security”.

The third document details the technical aspects of the security services implementing the selected NCP safeguard. These security services, together with the requirements of epSOS Agreement “Annex III Security” must be implemented by each MS in order to establish the “circle of trust” for the interchange of the Citizen health-care data among the MSs, according to the use cases foreseen by Annex I (see doc#1 in the referring document list).

The fourth document analyses the congruity and suitability of the epSOS Security Services and Policies defined by WP3.7.



**Yellow** background = part developed by WP3.7 inside the **Requirements Definition**  
**Cyan** background = part that must be developed by WP3.8 and WP3.9 Integration and customization  
**Pink** background = part that must be developed by WP4.3  
**Grey** background = part that must be developed by WP4.4 and WP4.5

Figure 1-1: Management of IT Security (ISO/IEC TR 13335-3)

Going into details for this “master” document:

- Chapter#2 (Introduction): describes the overall goals of the WP3.7 Work Package.
- Chapter#3 (Assumptions & guidelines): mainly describes the epSOS security objectives; the strategies that WP 3.7 has adopted for the risk analysis of the epSOS project, and the strategy for selection of the security measures. Moreover the chapter highlights the recommendations of this WP that must be kept to improve the security management in the further phases following the conclusion of the Pilot Project.
- Chapter#4 (Overall picture & logical scheme): describes the security environment, the security principles and highlights the boundary of the epSOS Project.
- Chapter#5 (Definition of elements and actors relevant for security issues): describes the classification of the health-data, the Actors who operate on those data, the threats to the data and the related impacts.
- Chapter#6 (Security requirements): lays out the High level risk analysis process adopted (that is the “informal approach”), and describes, as “security requirements” the selected safeguards.
- Chapter#7 (Reference to Section I – Security Policies): contains the explicit reference to the document which describes the epSOS Security Policies.
- Chapter#8 (Reference to Section II – Security Services): contains the explicit reference to the document which details the technical aspect of the Security Services.
- Chapter#9 (Reference to Section III – Suitability Analysis) contains the explicit reference to the document which describes the Suitability Analysis. That document contains, at the beginning, the description of the structure and of the contents of the document itself.
- Chapter#10 (Questionnaire): describes the results of the analysis performed on the questionnaire. This analysis was used as a reference for the risk analysis.
- Chapter#11 (Annex – WP3.7 Organization and Timing): describes the organizational aspects and the timing of the WP3.7 Work Package.

## 2 INTRODUCTION

### 2.1 Goals of the WP3.7 Work Package

As defined in Annex I (see item#01 in the referring documents list), the goal of the WP3.7 Security Services Work Package is the definition of a security system ensuring confidentiality, integrity and availability of data on the basis of the functional service requirements and taking into account the existing level of security implemented in each Member State.

The objective of the Work Package is to select, among different options and on the basis of an *option analysis*, an appropriate, effective and reliable security system to be integrated in the system architecture.

*Special care will be drawn upon the establishment of a security system ensuring confidentiality, integrity, authenticity and non-repudiation of data in the light of the EU legal framework and according to the national legal and regulatory frame. Best practices at MS level will be taken into account as reference for the definition of a security system usable in all EU MS.<sup>1</sup>*

To meet the functional requirements, the epSOS LSP system shall provide necessary security measures and adequate assurance. The required level of security cannot be reached by adding some security functions ex-post; security must instead be considered during the whole life cycle of the system.

This document (that is the “master document “ of D3.7.2 deliverable) , making reference to core concept of ISO/IEC 27000:

- summarizes the architecture of the system;
- identifies the key subjects, the objects, the operations on objects, the main threats to system assets, the security requirements of the system and of its security environments;
- proposes the functional security requirements (security measures) and the security assurances able to meet the stated security goals.

This document (which is the master document of D3.7.2 deliverable) wants to define both the security context/scenario and the security items which must be effective for the whole deliverable. Anyway it is accepted that Section I (security policies), which has to be self-comprehensive, can contain the "repetition" of some terms. This repetition can be done using different words, but the safeguard of the meaning given here must be assured.

### 2.2 Glossary & Abbreviations

The glossary and the abbreviations used in this document are explained in the epSOS LSP common Glossary.

---

<sup>1</sup> Reference to page 126/127 of epSOS annex 1

### 3 ASSUMPTIONS & GUIDELINES

#### 3.1 Security View

##### 3.1.1 Objectives prioritization.

The main objectives of computer security, which follow the ISO/IEC 27002 indications, are:

- **Authenticity:** the identity of an actor has been proven as true;
- **Confidentiality:** information is accessible only to authorized users/[actors];
- **Integrity:** accuracy and completeness of information and processing methods;
- **Availability:** authorized users have access to information and associated assets when required;
- **Accountability/Non Repudiation (Liability):** each communication and each data transaction can be tracked back to a certain originator in a traceable chain of activities.

These objectives can be further divided and applied to Actors which leads to derived security objectives. The most relevant derived security objectives for epSOS LSP are:

- Entity (NCP/HCP) Authenticity: an actor is the one he/she claims to be;
- Originator Authenticity: the source of data is as claimed;
- Access Control: access to information is restricted to authorised actors/entities;
- Non-repudiation of origin: the data Originator cannot deny having the data;
- Non-repudiation of delivery: the data Consumer cannot deny having received the data.

Taking into account the *business-objectives* (namely the transfer of health-care documents between two health-care organizations operating in two different MS in a way that the Consumer is able to grasp the same “clinical meaning” as expected by the Originator) and *IT-objectives* (as they are declared in Annex I –see [1] in the referring document list- and in WP3.1/WP3.2 -Functional Requirements-), the WP3.7 security views are:

- **Integrity** and **Confidentiality** (and the derived objectives of entity authenticity, originator authenticity, and access control) are the most important security objectives as they are closely related to patient safety and to the respect of legal requirements (privacy) and massively influence the acceptance of epSOS LSP by physicians and Patients.
- **Accountability/Non Repudiation (liability)** is important for user acceptance. Due to the trust brokering role of NCPs and the independence of physicians in deciding on their use of provided information, the liability technical aspect, in epSOS LSP, is only an issue in NCP-to-NCP communication.
- **Availability** is important for user acceptance. Availability is a general non-functional requirements of the epSOS LSP Project as a whole.

This leads to the conclusion that integrity of medical data and certain administrative data have a *high* (see ref. in par. 5.1-Data classification) protection demand. The confidentiality of patient data has the same *high* protection demand, such as the liability (non repudiation), and the availability of epSOS LSP managed data have a *moderate* protection demand .

#### **REMARKS:**

a) it must be taken into account that the confidentiality objective is influenced by the requirement that NCP has to carry out a semantic translation so, consequently, it must operate on non-encrypted clinical data and thus be under control of a natural or legal person legally authorised to process medical data. See doc#7 in the referring document list.

b) in order that the Consumer (HCP) is able to use the received clinical data (the data submitted to the semantic translation) for decision-making on the Patient's health, it is necessary that the received document provides the Consumer –from the integrity point of view- with the same or higher integrity assurance as the original sent document. As there is no forecast to submit the epSOS LSP to a formal security evaluation, then the Consumer will use the received document only for decision-support.

### 3.1.2 Indications for choice of security measures.

Given that epSOS LSP deals with sensitive healthcare data, it should evaluate the use of either “detection measures” or “preventive measures”. These measures (control) have different impact on operational abilities and productivity.

In epSOS LSP, to mediate between the needs of HCPs and data Subjects (patients) rights, preventive measures are to be preferred.

## 3.2 Risk Analysis

WP3.7 has recognized the incompatibility of the execution time of a detailed risk analysis (“**detailed** approach”<sup>2</sup>) of the epSOS LSP project with the WP 3.7 time schedule.

Making reference to the ISO/IEC TR 13335-3 (ISO/IEC 27005) guidance, it has therefore been decided to apply a “**combined** approach” to risk analysis.

In particular in this document, at a higher level, it has been decided to apply a Risk Analysis “**informal** approach” -performed by skilled security people - to evaluate the risk of EpSOS LSP project and to define the epSOS LSP security requirements.

It has also been decided to apply a Risk Analysis “**baseline** approach” (ref. to vulnerabilities and threats ISO/IEC 27005 catalogue), to evaluate the risk of each Security Service proposed, in order to select the best solution and also, if applicable, to identify specific security constraints on the selected solution.

## 3.3 Recommendation to the functional specification team.

For a rigorous definition of the epSOS LSP security requirements, it was strongly suggested that in the next epSOS phase, the following activities should be planned:

- Execution of a Detailed Risk Analysis of the epSOS project;
- Preparation of a NCP “Protection Profile”. (*According to the Common Criteria definitions, a Protection Profile states a security problem rigorously for a given collection of systems or products, known as the Target of Evaluation (TOE) and specifies security requirements to address that problem without dictating how these requirements will be implemented.*);
- Evaluation of the NCP Protection Profile.
- Implementation of ISMS (Information Security Management System) according to ISO/IEC 27000 or equivalent standard.

---

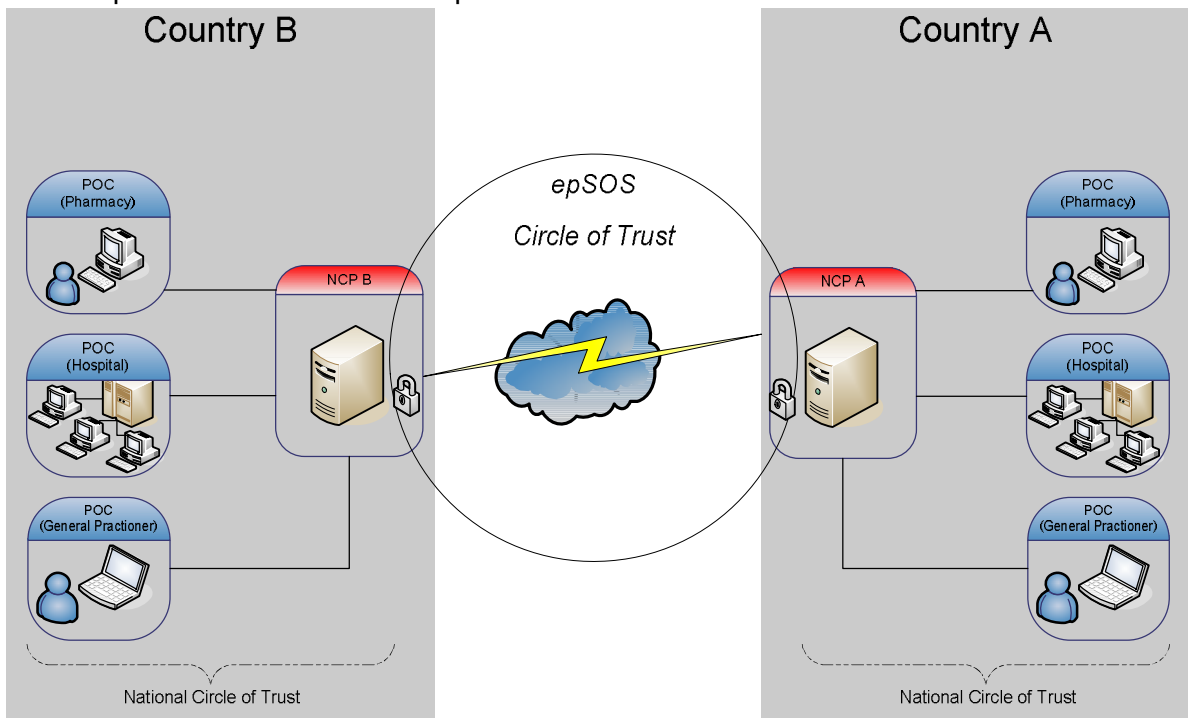
<sup>2</sup> “detailed approach”, “informal approach”, “combined approach” and “baseline approach” are definitions of ISO/IEC TR 13335-3 (see doc#8 in the referring list document).

## 4 OVERALL PICTURE & LOGICAL SCHEME

This chapter is going to give a general view of the security in the epSOS LSP and the introducing concepts will be detailed in the next chapters.

### 4.1 Overall picture.

Figure 4-1 illustrates a conceptual diagram of the epSOS LSP infrastructure for exchanging medical patient data between European countries.



**Figure 4-1: Overall picture of the epSOS LSP Project**

The core paradigm of the epSOS LSP is not to directly connect physicians but to connect the national infrastructures of a patient's home country and the country where a patient currently receives medical services. Within the epSOS LSP the patients' home country is referred to as country 'A', and the country where the patient gets medical treatment is referred to as country 'B':

- Country A is the country of affiliation (CoA), this means that country A is legally the exclusive entity, which is responsible for appropriately storing, archiving and documenting any required health information of a patient within its existing national infrastructure. For the epSOS LSP, it is assumed that all attributes and credentials that could be used to identify and authenticate the patient are issued by country A.
- Country B is the member state (MS) where the point of care (PoC) is located that provides healthcare to a patient from country A. For the epSOS LSP it is assumed that the HCP and HCPO that treat the patient can only be unequivocally authenticated by the competent authorities of country B.

The PoC could be a hospital, an individual practitioner, a pharmacy or any other point of the health care system of any country, participating in the epSOS LSP project. Each communication and each data transaction can be tracked back. Figure 4-1 focuses on a business point of view that relies on the use of health data retrieved from a Country A by a HCP located in Country B. Therefore existing national ePrescription and PS services of country A which persistently maintain the patient's data are not shown.

## The Trust relationships

A legal framework for the epSOS LSP admits the member states' infrastructures. Since all participants must agree to sign a predefined contract, they establish a trust relationship (see doc#7 in the referring list). The signing of the contract and all the related implications, can be assumed as the legal level of the "epSOS LSP Circle of Trust" (CoT). Within this circle of trust each member state is represented by a "National Contact Point (NCP)". The technical level of the epSOS CoT will then be the configuration of NCP endpoints, the NCP access control and digital certificates exchange, that allow inbound and outbound communication for the configured NCPs.

Inside MS, contractual arrangements will be established, aligned as required on the epSOS LSP framework contract. These national Circles of Trust must meet all the local and EU legal requirements on topics e.g. patient consent, data security, patient confidentiality, HCP liability, etc. Routing all epSOS LSP communication through a country's NCP thus ensures that all actions taken within the country are compliant with the epSOS LSP legal framework.

To conclude, the epSOS LSP project leads up to building cascaded circles of trust:

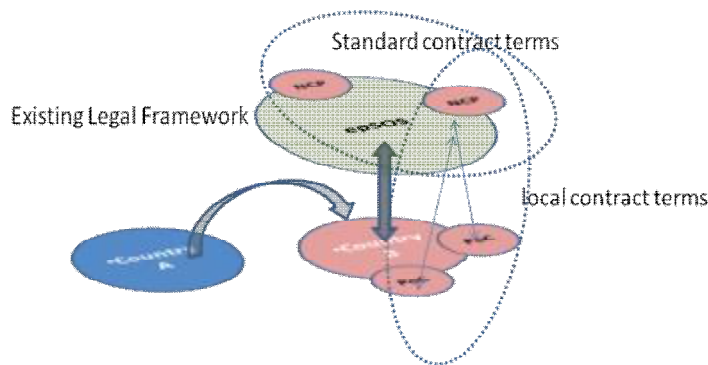


Figure 4-2: . epSOS LSP Trusted Domain

## 4.2 epSOS LSP Security challenges

A security framework needs to consider user authentication and authorization as well as to use encryption to protect communication over non-secure networks. Even more, the integrity of medical data and its assignment to a certain patient have to be protected. [see section 3.1 of this deliverable]

### 4.2.1 Security challenges

While these requirements apply to every eHealth infrastructure, the Circle of Trust topology of the epSOS LSP, its complete decoupling of data users and data providers, and the integration of existing infrastructures lead to some epSOS LSP-specific challenges:

- [a] Security objects are issued and consumed by different countries. The consumer (HCP) has no influence on how a security object is issued. This demands a complete decoupling of the respective services and puts strong emphasis on a secure exchange of authentic, standardized security objects.
- [b] Safeguards are applied by one national infrastructure and must be verified by another infrastructure. As NCPs are the only common known instances they are the only entities that can be used for this. Therefore end-to-end security is only available among NCPs. As a consequence NCPs act as "trust mediators" and require for specific means to broker security down to the "real" ends of secure business end-to-end communication which are the PoC in country B and the data providing systems in country A.

- [c] Access control is distributed among both participating countries. While country B needs access control means to protect its HCPs from accidentally accessing data in an illegal way (e. g. because the data controller in country A allows for an access that is forbidden by the law of country B), country A has to protect the privacy of its citizens and to ensure the required integrity and confidentiality of its internally managed data objects.
- [d] Acting entities are unknown outside their national infrastructure: Country A depends on country B to identify and authenticate the person that requests access to data of country A. Country B depends on country A to provide the means for patient identification/authentication and for identifying/discovering the medical data that will be used by the HCP in country B.

#### 4.2.2 Security core concepts

In order to deal with these challenges, epSOS LSP security builds upon the following core concepts:

- [I] Definition of dedicated security services as business level independent profiles
- [II] Use of security contexts: prior to business transactions, security services set up a secure session context which allows the decoupling of security and business related issues.
- [III] Use of a security token for the transmission of security related information and for holding the secure session context
- [IV] Separation of policy concerns by considering dedicated policies for national legislation, patient consenting, and patient privacy statements.
- [V] NCPs are the only entities that are known within both the epSOS LSP domain and their respective national domains. Trust brokerage among epSOS LSP and national domains is completely encapsulated within NCPs.

#### 4.3 Logical scheme

The figure below provides a logical view of the epSOS LSP project and reflects the solutions proposed to cope with the challenges that were sketched above.

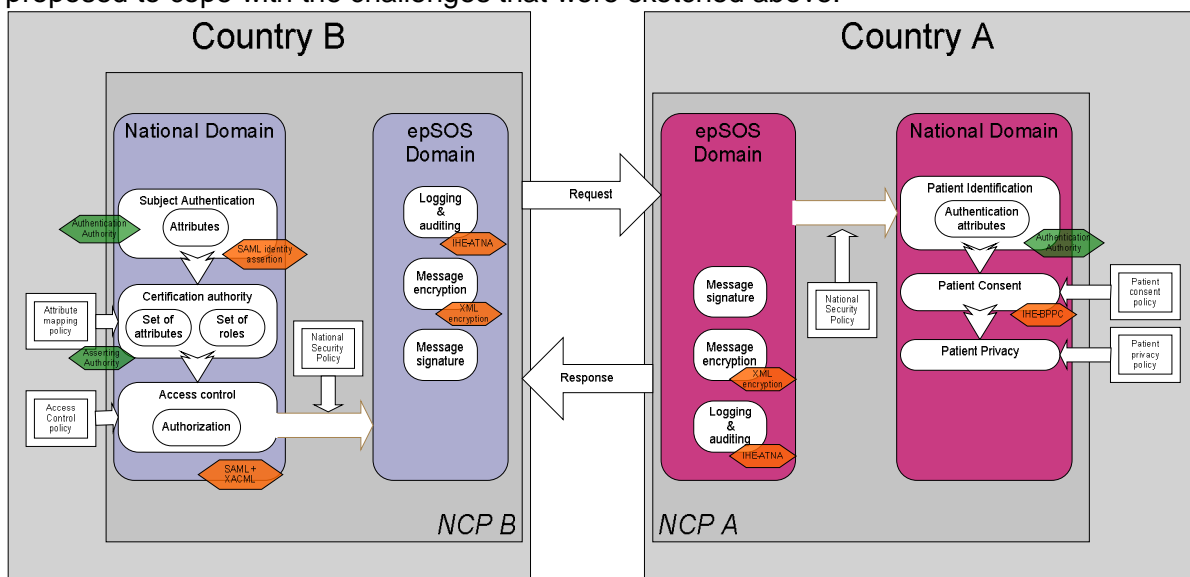


Figure 4-3: Security logical scheme

This logical scheme is based on a generic business process for a HCP to get a medical document.

The patient has to be identified in country B by means of any solutions that country A provides (e. g. by obtaining patient demographics or unique identifiers in an organizational procedure in country B for “epSOS patients”). As the identity of a patient is verified, it means that authentication attributes needed in country B are provided by an authentication authority in country A. For emergency access (“breaking glass scenario”), a special procedure is to be invoked. A HCP requesting an “override” access will specifically and doubtlessly state his intention and reason for the emergency data access request.

This step faces challenges [a] - *Standardize security objects* - and [d] - *Unknown actors* - with respect to the identity/authenticity and consent of the patient. Depending on the required accuracy of patient identification and the kind of identifier used, an exchange of identity related data between country B and A is needed because only country A “knows” the patient. The same applies for the HCP: at a high level, in order to apply the policies (e.g. NCP of country A leads to communicate not only the identity information but also the role of the HCP), there is a need to assess the identity of subjects (HCP or HCPO), i.e. it requires their authentication.

The authentication process provides authentic attributes about the user (e.g. professional identifier, first name, name, qualification, medical specialty, etc.). Given challenges [b] - *National safeguards* - and [d] - *Unknown actors* - a local authentication in B is not enough to authenticate him/her in a way that can be verified by country A.

Therefore a trusted party/entity must be involved in the authentication process: the asserting authority (AA). The AA is the entity that certifies the HCP’s identity attributes, which will be used in order to give the right roles (and consequently permissions) to the HCP.

For the transmission of this information, epSOS will make use of a security token that allows for a decoupling of issuers and consumers of security related data (see challenge [1] - *Standardize security objects* -).

The attribute mapping is performed because the access control policy can be application-dependent and therefore refers to its own roles (which are relevant to that particular application). whereas this meaning may not be the same as the attributes found in the assertions that are provided by the AA (which can be also application-independent).

As mentioned in challenge [c] - *Distributed access control*- , access control is distributed between countries A and B. The access control means used by epSOS LSP security are the enforcement of authorizations and access policies (derived from consents and national legislations) and the auditing of all events:

- The users are not equal, and different users will have different access rights. Security policies must state who can do what and what is allowed to be done and access control mechanisms must enforce these policies. It is necessary that a patient states his consent for the exchange of his medical data, in accordance with the patient consent policy in country A. This supposes that a patient has to give his consent in country A for the data that can be used in the epSOS LSP and in country B (once) for each access of data in country B. (*not indicated in this scheme*).
- National security policies (in country A and in country B) are applied at the output and the input of the NCPs.
- Logging and Auditing are essential features of systems which are *provided by the different services* such as level agreements, contractual obligations or legal requirements. Logging is a general mechanism which is based on specific recordings of configurable aspects regarding the activity of a system in sequential order. Usually a system will offer a large variety of logging mechanisms, like *security logs (records all attempts to access a system; successful as well as failed attempts)*, activity logs, error logs, etc. In case of an emergency, access may be gained even if the patient had not explicitly authorized the doctor to do this. Logging and auditing mechanisms

occur in both NCPs involved in an epSOS LSP UC. Logging and auditing mechanisms must take into account that an activity may require tracing from one NCP to another one (e.g. in case of abuse). They have not been represented on the scheme but audit trails should be also implemented at PoCs.

Request and response messages are based on standard protocols (ref. to “*D3.4.2 Final common components specification*”). Data confidentiality and data integrity between NCPs is provided by cryptographic technologies, processes and operations. In order to solve challenge [b] - *National safeguards* - epSOS LSP security places NCPs in both circles of trust.

This allows them to mediate security services (e.g. confidentiality) between both circles. By doing so the NCP takes the role of a bearer, e.g. by confirming the authenticity of a data originator.

## 5 DEFINITION OF ELEMENTS AND ACTORS RELEVANT FOR SECURITY ISSUES

In this section the elements (data classes) and actors in the epSOS LSP are considered from a security point of view.

### 5.1 Data classification

A generalized data classes are introduced together with their protection requirements. Each element in the epSOS LSP belongs to one of these data classes.

The following data classification is considered in epSOS LSP:

- **Healthcare-related Data:** Healthcare Data of a patient e-prescription or patient summary used for the medical treatment of a patient. According to the Directive 95/46/EC the processing of medical data has to satisfy higher privacy requirements since they belong to the special categories of data (Article 8 Directive 95/46/EC). Healthcare related data contain also:
  - data about the patient's consent;
  - log data which provide information about the access to healthcare related data in epSOS LSP.
- **Critical Meta Data:** Data needed to control the exchange of healthcare related data between NCPs and between NCPs and PoCs, respectively. Critical Meta Data include authentication, identification and administrative data to clearly identify patients, PoCs and HCPs,
- **Non-critical personal data:** Personal data which do not belong to the special categories of data according to Article 8 Directive 95/46/EC and do not belong to the critical meta data.
- **Administrative Data:** They do not contain any personal data. They are used for the administration or configuration of technical components.

The data classes differ in the damage that could occur if the confidentiality, integrity, or availability are lost. The damage is categorised according to the following threats:

Threat	Healthcare-related Data	Critical Meta Data	Non-critical personal data	Administrative Data
Violations of laws, regulations, or contracts	Can have substantial consequences, for example violates national privacy laws or professional secrecy laws	Can have substantial consequences, for example violates national privacy laws or professional secrecy laws	Can have substantial consequences, for example national privacy laws	Have minor consequences
Impairment of privacy	Processing could have a seriously adverse effect on the social standing of the persons.	Processing could have a seriously adverse effect on the social standing of the persons.	Processing could have an adverse effect on the social standing of the persons.	No damage on privacy

Physical injury	Serious injury to an individual is possible. There is a danger to life and limb (e.g. a medical treatment based on modified and false health-care data may have serious consequences on the state of health of a person).	Serious injury to an individual is possible.	Does not appear possible.	Does not appear possible.
Negative internal or external effects	Considerable impairment of the reputation /trustworthiness can be expected.	Considerable impairment of the reputation / trustworthiness can be expected.	Only minimal impairment or only internal impairment of the reputation / trustworthiness is expected.	Only minimal impairment or only internal impairment of the reputation / trustworthiness of the organisation is expected.

**Table 5-1: Impact dependent on threat and data class**

The impacts of the damages on the confidentiality, integrity, availability, authenticity and non-repudiation of the data in data classes are qualified in terms of high, moderate, and low impact according to [FIPS 199] (see [6] in the referring document list). The level for availability is set to low, since there are existing alternative processes (patients are treated already today), so that a medical treatment is also guaranteed without the epSOS LSP data.

<b>Data class</b>	<b>Confidentiality</b>	<b>Integrity</b>	<b>Availability</b>	<b>Authenticity</b>	<b>Non-repudiation</b>
Healthcare-related Data	High	High	Low	High	High
Critical Meta Data	High	High	Low	High	High
Non-critical personal data	Moderate	Moderate	Low	Moderate	Moderate
Administrative Data	Low	Low	Low	Low	Low

**Table 5-2: impacts level**

## 5.2 Actors

The following actors (or entities) are considered in epSOS LSP (see also the epSOS LSP glossary for functional definitions):

- **Patient:** any natural person who receives or wishes to receive health care in a Member State.
- **Health Care Professional (HCP):** see project glossary. Furthermore, a HCP must be under national law or rules established by national competent authorities to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
- **National Contact Point (NCP):** see project glossary (A legal entity representing a country within epSOS LSP, assuming legal duties towards MS partners and its own

network of national gateways: it acts in a bidirectional way transmitting in-outbound messages between national IT infrastructures and NCPs from other MS). A NCP processes medical data in order to achieve interoperability.

- **Technical Staff:** Any person or organization participating in the epSOS LSP processes not involved in the medical treatment of a patient such as
  - System administrator – in charge of the central organisation that maintain the system
  - Local system administrator – in charge of the local, national organisation that maintain the system locally within a member state.
  - System operators.
- **Data Security Officer:** The data security officer of the organization which processes healthcare-related data. For example, he/she can check the log data if there is a reasonable suspicion and the patient agreed.
- **Auditor:** Any person who satisfies the epSOS LSP auditor requirements and who audits epSOS LSP.
- **HCPO:** see project dictionary.

### 5.3 Actors from a security point of view

The actors (active and passive entities) are characterized from a security point of view in the following aspects:

- **Access rights:** describe the data classes an actor is allowed to access
- **Authentication level:** describes the strength of the authentication means an actor must use to access epSOS. The authentication means can be organizational (for example passport, healthcard) or technical (for example password, cryptographic certificate).

Patients (passive entities) have the right to know all about their personal data processed in the epSOS LSP. Access can be carried out either technically by providing patient-centric interfaces or organizationally, e.g. requesting a HCP or a data security officer. Organizational measures (e.g. passport, health card) can be used for the identification and authentication of a patient against a HCP.

Actor (active entity)	Access Rights	Authentication level
Health Care Professional	Healthcare-related data, Critical Meta Data, Non-critical personal data	Organizational against patient (e.g. health professional card), Technical against systems of POC (e.g. password, smartcard)
National Contact Point	Healthcare-related data, Critical Meta Data, Non-critical personal data, Administrative data	Technical against NCP, POC (must use strong authentication mechanism, e.g. cryptographic certificates)
Technical Staff	Administrative data	Technical (e.g. password, smartcard)
Auditor	Non-critical personal data, Administrative data	Technical against systems of POC, NCP (e.g. password, smartcard)
HCPO	Healthcare-related data (only if HCP or NCP, otherwise no access) Critical Meta Data Non-critical personal data Administrative Data	Technical against NCP
Data Security Officer	Healthcare-related data (except of medical information), Non-critical personal data	Technical against systems of POC, NCP (e.g. password, smartcard)

Table 5-3: Actors Access Rights and Auth. level

## 6 SECURITY REQUIREMENTS

Although a detailed risk analysis could not be performed due to time limitations, a detailed study has been made of the epSOS LSP data and processes, and more specifically of the Organizational requirements, the Legal requirements, the Technical requirements, the Security Audit requirements, the user requirements, etc. Based on those security requirements and the security best practices in the field of health, the following epSOS LSP security requirements have been identified.

The aim of this chapter is to describe, at high level, the epSOS LSP security requirements. Following the logical architecture of the project and taking care of the complexity and the number of different approaches of the MSs, it would seem to be useful to divide the security requirements into three levels (see Figure 6-1)

- **1st level** - Security requirements for the epSOS LSP Project as a whole (that is “environmental” requirements).  
These requirements derive mainly from Annex I (see [01] in “Referring Documents” list on the cover) and WP2-deliverables. See the following paragraph for more details.
- **2nd level** - Security requirements for a National Contact Point (NCP), starting from the observation that each NCP must exchange information -in a standard way- with all the others NCPs.  
These requirements derive mainly from the WP3.6/WP3.2/WP3.1 deliverables the “Concept paper final” document and ISO/IEC 27000 baseline safeguards catalogue. See the following paragraph for more details.
- **3rd level** – Minimum acceptable common security requirements for the different National Information Infrastructure, starting from the observation that different levels of security requirements may have been established by the different Health Care National Systems.  
*“Minimum” because they must be the minimum that satisfies the Project;*  
*“acceptable” because they are already implemented or they can be easily implemented by all MSs.*  
These requirements must be derived from the analysis of the answers to security questionnaires (see [02] in “Referred Documents” for the analysis and the following paragraph for more details).

Obviously coherence within the three levels of the security requirements must be assured. This allows an easier definition of the security requirements and the placement of each requirement in the most suitable context within the project.

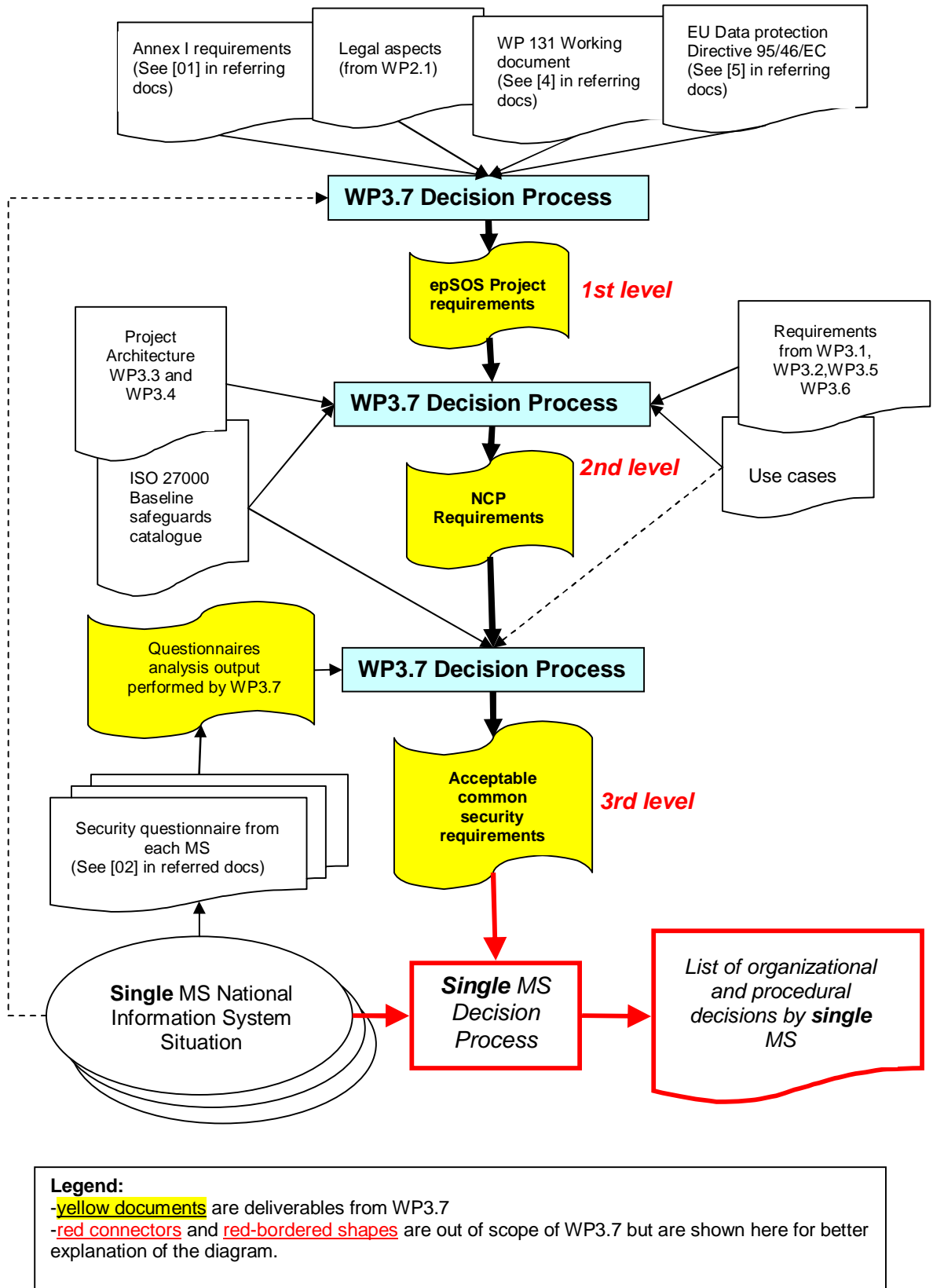


Figure 6-1: Diagram of the security requirements definition process

## 6.1 Security requirements for the epSOS LSP Project level.

The epSOS LSP Project must guarantee the security of health-care data processing. This means that confidentiality, availability and integrity of data must be guaranteed through suitable security requirements.

More precisely, the security requirements for the epSOS LSP Project as a whole must guarantee the following items:

- Identification;
- Authentication;
- Access control;
- Non repudiation;
- Data confidentiality;
- Data availability;
- Logging of any operation, performed by whatever User(Active Actors), which has an impact on security.

Taking into account the indication given in the documents referred as [01], [02], [04] in the referring document list (see cover), enclosed here is a more detailed list of security requirements for epSOS LSP Project.

*Please note that “MUST” is used when the requirement is **mandatory**, while “SHOULD” is used when the requirement is **recommended** but not mandatory.*

*In this document ,following the ITSEC definition, **Accountability** means: “requirements to ensure that relevant information is recorded about actions performed by users or processes acting on their behalf so that the consequences of those actions can later be linked to the user in question, and the user held accountable for his actions”. **Auditing** means: “requirements to ensure that sufficient information is recorded about both routine and exceptional events that later investigations can determine if security violations have actually occurred, and if so what information or other resources were compromised”.*

**EpSOS-Req#3.7.01 (Identification):** For each epSOS LSP Actor a valid and unique electronic identity MUST be established. The standards to which this is unique/valid MUST be established by agreement.

**EpSOS-Req#3.7.02 (Authentication):** The identity of epSOS LSP Users (before each system access, transaction or message) MUST be validated.

**EpSOS-Req#3.7.03 (Robustly Authenticating Users):** Each MS MUST robustly grant the authentication of his own **Users**. The conditions on which a single MS may guarantee the User authentication, may be based on technical and/or organizational measures, These measures, in any case, SHOULD provide that the authenticated entity MUST not be repudiated.

**EpSOS-Req#3.7.04 (Access control):** The confidentiality and integrity of epSOS LSP information assets MUST be protected by preventing unauthorised access and use. (protection from both the technical and organizational point of view).

**EpSOS-Req#3.7.05 (Access control, privilege management and HCP authorization):** the authorization with which an identified and authenticated Health Care Professional can get access to epSOS medical information (Patient Summary & ePrescription) of a Patient MUST be based on the role assigned to the HCP (as defined by the Health-care MS organization or

authority), on the verification of the parent health-care Organization, on the fact that “that” HCP is treating “that” Patient.

**EpSOS-Req#3.7.06 (Confidentiality):** The unauthorized disclosure of personal medical information during the transfer, processing and storage within epSOS LSP MUST be strongly prevented. The use of cryptographic mechanisms SHOULD be adopted.

**EpSOS-Req#3.7.07 (System and data integrity):** the integrity of data within epSOS LSP documents, transactions or messages MUST be assured for both data rest and transit.

**EpSOS-Req#3.7.08 (Availability):** It MUST be ensured that information assets are, according to the service level agreements agreed, available in a timely and reliable manner when needed in the scope of their professional activity by authorised epSOS Users and systems.

**EpSOS-Req#3.7.09 (Non Repudiation):** it MUST be ensured that both the User-Originator and the User-Receiver of documents and messages cannot deny their actions (documents production, message sending, message receiving).

**EpSOS-Req#3.7.10 (Accounting):** it MUST be ensured that each activity of a User is accounted for. In any case accounting information MUST not include personal health care data.

**EpSOS-Req#3.7.11 (Auditing):** it MUST be ensured that each action which has an impact on security or privacy must be audited. In any case auditing information must not include epSOS personal health care data.

**EpSOS-Req#3.7.12 (Fraud detection):** epSOS LSP SHOULD provide tools able to discover possible frauds in the use of medical data.

**EpSOS-Req#3.7.13 (Traceability):** It MUST be ensured that log data can be connected from different sources in a privacy-compliant way.

**EpSOS-Req#3.7.14 (End-of-Life process):** A process MUST be developed by each MS on when and how to destroy all data objects created for the epSOS LSP after its conclusion

**EpSOS\_Req#3.7.15 (Privacy):** each epSOS LSP Data Controller MUST guarantee the respect of the privacy obligations foreseen by its National Law and the European Directive 95/46/EC (see [5] in referring doc. List).

**EpSOS-Req#3.7.16 (Trust):** each MS SHOULD show evidences of the respect, by its own health-care information system, of the security requirements established by the pilot sites agreement

## **6.2 Security requirements for a National Contact Point (NCP) level.**

Taking into account the indications given in doc#3 in the referring document list, the list of the security requirements at epSOS LSP Project level (see previous paragraph), and the ISO/IEC 27005 baseline safeguard catalogue, enclosed here is a more detailed list of security requirements for a National Contact Point.

*Please notice that “MUST” is used when the requirement is **mandatory**, while “SHOULD” is used when the requirement is **recommended** but not mandatory.*

**NCP-Req#3.7.01a (NCP identification):** a NCP MUST have a unique electronic identity in a common cryptographic domain (such as, for example, digital certificates following x509 Standard).

**NCP-Req#3.7.01b (NCP local User I&A):**

I&A of each local User (NCP technical staff) MUST be performed before he/she starts processing. The tool/mechanism used (individually or with other security tools/mechanisms/procedures) for I&A MUST prevent the User's identity (previously submitted to I&A) from being repudiated.

**NCP-Req#3.7.02 (Authenticating Network Access):** each NCP MUST ensure that all connections to remote servers (both other NCPs and local systems) and applications are authenticated.

**NCP-Req#3.7.03a (Digital Signatures):** if in a MS the epSOS LSP Users apply a digital signature, then the MS-related NCP MUST be able to:

- verify that the digital signature is valid (this implies that the user certificate is also valid)
- confirm that validity to any other MS-NCP, through a digital signature.

**NCP-Req#3.7.03b (Digital Signatures):** if a MS does not adopt a digital signature, then the MS-related NCP MUST be able in any case to:

- confirm to any other MS-NCPs connecting, the data integrity of the exchanged data through a digital signature.

**NCP-Req#3.7.04 (Access Control):** a NCP MUST provide Access Control mechanisms which provide functionalities that allow, for a given User, the specification of which data and services the User can get access to, and which privileges the User has with regard to the data and services.

**NCP-Req#3.7.05 (Confidentiality):** a NCP MUST use strong cryptographic mechanisms to prevent the unauthorized disclosure of personal medical information or security critical system data during the transfer and processing within the NCP itself if this processing has confidentiality vulnerabilities.

**NCP-Req#3.7.06 (Protecting Source and Destination Integrity during data transmission):** the source and destination of the message during data transmission between NCPs MUST be protected to maintain its integrity.

**NCP-Req#3.7.07 (Protecting Data Storage):** if storage is performed, a NCP MUST protect medical information or security critical system data it contains. The use of pseudo-anonymization mechanisms SHOULD be used if possible or reasonable.

**NCP-Req#3.7.08 (System and data integrity):** a NCP MUST ensure, by strong cryptographic mechanisms, the ability to discover if the medical information has been altered or destroyed in a unauthorized manner, so that that medical information may not be further processed.

**NCP-Req#3.7.09 (Availability):** NCP best effort MUST ensure the respect of the agreed Service Level Agreements.

**NCP-Req#3.7.10(Non Repudiation):** a NCP MUST have a strong cryptographic mechanism (i.e. RSA) to ensure the non repudiation of each document produced by itself or messages exchanged with other NCPs.

**NCP-Req#3.7.11 (Accounting and Control):** a NCP MUST have a mechanism to record every access request and disclosure of medical information and clinical data, together with the time and identity of the accessing User.

Clinical data MUST NOT be included in accounted data. Accounting records MUST be maintained as long as the pilot project lasts, unless otherwise legally required.

**NCP-Req#3.7.12 (Auditing):** it MUST be ensured that each action which has an impact on security is recorded. If data to be recorded contain both medical and personal data, an anonymization or pseudo-anonymization process SHOULD be used if possible or reasonable. In any case the recorded data MUST not contain personal health care data, but can contain a unique identifier to a data object. Audit records MUST be maintained as long as the pilot project lasts, unless otherwise legally required.

**NCP-Req#3.7.13 (fraud detection):** NCP MUST provide tools to discover possible frauds in the use of medical data

**NCP-Req#3.7.14 (Continuously Logging):** logging on the NCP SHOULD be operational at all times. In case of failure, the NCP involved MUST inform all the other NCPs.

**NCP-Req#3.7.15 (Securing Access to Audit/Account Logs):** a NCP MUST secure the access to audit records to prevent misuse or compromise.

**NCP-Req#3.7.16 (Logging Transactions):** a secure audit record MUST be created each time a User asks to access medical information of a Patient or to send an e-prescription dispensation's notification.

**NCP-Req#3.7.17 (Trust):** it SHOULD be allowed to submit each NCP to a "second part" (see ISO 9000) security audit procedure performed by the other MS, so that it will be possible to verify the compliance with the security requirements established by the pilot sites agreement.

**NCP-Req#3.7.18 (Minimum Content of Accounting Logs):** the logs SHOULD contain:

- the user ID of the accessing User;
- the role the User is exercising;
- the organisation of the accessing User (at least in those cases where an individual accesses information on behalf of more than one organisation);
- the unique Patient ID;
- the function performed by the accessing User;
- the NCP-id of the Originator/Target;
- a time stamp including time zone used.

**NCP-Req#3.7.19 (Reporting Every Access medical information, notifications included):** it SHOULD be possible to identify all requests to access to any Patient's record(s) (dispensations and modifications included) over a given period of time according to different parameters (Users, Patients' records,...)

### **6.2.1 Environmental and operational NCP security requirements.**

It is strongly recommended that the following security requirements SHOULD be met by all NCPs engaged in the epSOS pilot phase.

**NCP-Req#3.7.20 (Personnel security – security in job definition and resourcing)** Security responsibilities for technical staff, data security officer and auditor SHOULD be

addressed at the recruitment stage, included in contracts, and monitored during an individual's employment. All employees and third party users of information processing facilities SHOULD sign a confidentiality (non-disclosure) agreement.

**NCP-Req#3.7.21 (Personnel security – user training)** Technical staff SHOULD be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.

**NCP-Req#3.7.22 (Personnel security – Responding to security incidents and malfunctions)** Incidents affecting security MUST be reported to the designated (by each MS) point of contact through appropriate management channels as quickly as possible.

**NCP-Req#3.7.23 (Personnel security – Responding to security incidents and malfunctions)** All employees and contractors MUST be made aware of the procedures for reporting the different types of incident (security breach, threat, weakness or malfunction) that might have an impact on the security of NCP assets. They MUST be required to report any observed or suspected incidents as quickly as possible to the designated (by each MS) point of contact.

**NCP-Req#3.7.23 (Physical and Environmental security – secure areas):** Critical or sensitive information processing facilities SHOULD be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They MUST be physically protected from unauthorized access, damage and interference.

**NCP-Req#3.7.24 (Physical and Environmental security – secure areas):** The protection provided SHOULD be commensurate with the identified risks.

**NCP-Req#3.7.25 (Physical and Environmental security – equipment security):** Equipment SHOULD be physically protected from security threats and environmental hazards. Protection of equipment is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. This should also take into consideration equipment location and disposal. Special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

**NCP-Req#3.7.26 (Physical and Environmental security – general controls):** Information and information processing facilities SHOULD be protected from disclosure, modification or theft by unauthorized persons, and controls SHOULD be in place to minimize loss or damage.

**NCP-Req#3.7.27 (Communications and operations management - Operational procedures and responsibilities):** Responsibilities and procedures for the management and operation of information processing facilities MUST be established. This includes the development of appropriate operating instructions and incident response procedures.

**NCP-Req#3.7.28 (Communications and operations management - System planning and acceptance):** The operational requirements of new systems SHOULD be established, documented and tested prior to their acceptance and use.

**NCP-Req#3.7.29 (Communications and operations management - Protection against malicious software):** Precautions SHOULD be required to prevent and detect the introduction of malicious software. Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses and logic bombs.

**NCP-Req#3.7.30 (Communications and operations management - Housekeeping):** Routine procedures SHOULD be established for carrying out the agreed back-up strategy taking back-up copies of data and rehearsing their timely restoration, logging events and faults and, where appropriate, monitoring the equipment environment.

**NCP-Req#3.7.31 (Communications and operations management – Network management):** The security management of networks which span organizational boundaries requires attention. Additional controls may also be required to protect critical data passing over public networks.

**NCP-Req#3.7.32 (Communications and operations management – Media handling and security):** Media SHOULD be controlled and physically protected. Appropriate operating procedures SHOULD be established to protect documents, computer media (tapes, disks, and cassettes), input/output data and system documentation from damage, theft and unauthorized access.

### **6.3 Acceptable common security requirements for the different National Information Systems (NIS) level**

The acceptable security requirements for the different National Information Infrastructure derive (see Fig.1) from the requirements listed in the previous paragraphs, the analysis of the answers to the questionnaire (see following chapter) and –in any case- must be compliant with the EU directive for data protection (see [5] in the referring list).

*Please notice that “MUST” is used when the requirement is **mandatory**, while “SHOULD” is used when the requirement is **recommended** but not mandatory.*

**NIS-Req#3.7.01 (Identity and Authorization of a User):** I&A of a User MUST be performed before he/she starts processing. The tool/mechanism used (individually or with other security tools/mechanisms/procedures) for I&A MUST prevent the User’s identity (previously submitted to I&A) from being repudiated.

**NIS-Req#3.7.02 (Access Control):** an Access Control tool/mechanism which enables access to medical information on the basis of the User Identity and the role (and related authorizations) he/she plays, MUST exist.

**NIS-Req#3.7.03 (Confidentiality and Integrity):** confidentiality and integrity of the medical informations produced, sent or stored, MUST be guaranteed. Data SHOULD be protected by the use of acknowledged (by the single MS) cryptographic algorithms.

**NIS-Req#3.7.04 (Audit & Accounting):** a process which allows the collection and the consultation of the information of both the actions performed by the Users and the events which impact on security, MUST exist. All the data collected MUST be protected from unauthorized access.

**NIS-Req#3.7.05 (Limiting Use and Disclosure of Personal Health Information to Identified Purposes):** Organisations connecting to the epSOS LSP and organisations hosting components of the epSOS LSP MUST only use or disclose medical information for purposes consistent with those for which it was collected, except in the case of Patient consent or if permitted (or required) by law.

**NIS-Req#3.7.06 (Segregating Network Users, Services and Systems):** Organisations hosting epSOS LSP components MUST introduce network controls to segregate information services, Users and information systems that are not involved in access to or hosting of the epSOS LSP systems. Separated management networks are recommended.

**NIS-Req#3.7.07 (Privacy):** each epSOS LSP Data Controller MUST guarantee the respect of the privacy obligations foreseen by its National Law.

**NIS-Req#3.7.08 (Trust):** each MS SHOULD show evidence of the respect, by its own health-care information system, of the security requirements established by the pilot sites agreement

**NIS-Req#3.7.09 (Protecting Against Malware):** each MS IT-system involved in the epSOS LSP Project MUST implement, according to ISO/IEC 27000, appropriate detection and prevention controls to protect against malicious software (viruses, worms, etc).

## **7 Reference to SECTION I SECURITY POLICIES**

For this matter please refer to document #2 in the Referred Documents list placed on the cover of this document. The structure of that referred document is shown at the beginning of the document itself.

## **8 Reference to SECTION II SECURITY SERVICES**

For this matter please refer to document #3 in the Referred Documents list placed on the cover of this document. The structure of that referred document is shown at the beginning of the document itself.

## **9 Reference to SECTION III SUITABILITY ANALYSIS**

For this matter please refer to document #4 in the Referred Documents list placed on the cover of this document. The structure of that referred document is shown at the beginning of the document itself.

## **10 QUESTIONNAIRE (Analysis of the Security aspects in MSs)**

### **10.1 Introduction for the use of a questionnaire**

In order to provide an optimum analysis of security services, a questionnaire was sent to the Member States.

The use of a tool like a questionnaire is motivated by the objective of knowing, through a structured system of proper questions, the overall status of security policies, services and protocols for handling Protected Healthcare Information (PHI) System in each MS, so that it is possible to define –if and when applicable- the best practices to be adopted in the epSOS LSP Project.

The collected information support the definition of a high level epSOS LSP security policy, coherent with the solutions already in place and supporting the design of the epSOS LSP security services, compliant with the constraints of not-obliging any change in the MSs systems.

In this connection, the questions of the questionnaire are constructed so that it is possible to help the Working Group in defining the security measures that are “useful-applicable-economically viable” by all MSs within the epSOS LSP Project.

The questionnaire was sent to 12 MSs.

### **10.2 Questionnaire layout**

The questionnaire is divided in five main sections:

1. Security Policies
2. Security Services
3. Backup
4. Auditing and Logging
5. Network Security Protocols

Each section contains a *list of questions* with a list of *answer options*.

In order to make data collection and analysis easier, as many as possible questions were drawn with “closed” answers.

Two Member States filled in an old version of the questionnaire without the Backup section and with fewer questions about Security Policies and Services sections.

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

### **10.3 Analysis**

This paragraph provides the analysis performed on the answers given by the MSs. The analysis is made as follows: each question is presented, all the answers are collected and a factorization is made.

#### **Section 1 – Security Policies**

##### **1. Level of definition of security policies (national, regional or HCPO).**

There is no homogenous approach. The definition is mainly at national level, or at least based on rules defined at national level. Answers highlight, anyway, the presence of policy definition in all MSs.

##### **2. Level of implementation of security policies (national, regional or HCPO).**

For the implementation of security policies the approach of MS varies from national to local, therefore not allowing the definition of a common trend.

##### **3. Security policies mandatory or not.**

In all MS the adoption of security policies is mandatory. Therefore it is reasonable to assume that the EPSOS LSP security policies, once defined, will be made mandatory for all participants.

##### **4. Normative body responsible for setting/checking security policies.**

For most MS the agency in charge is the Ministry of Health or a specific Agency devoted to personal data protection, or a combination of both. The epSOS LSP security policies should be, therefore, compliant with prescriptions given by those entities.

##### **5. Certification process for security.**

Where a certification process exists it is usually based on the ISO/IEC 27002 standard. Some exceptions exist, but the adoption of ISO/IEC 27002 should be selected as the best choice for optimal security certification in the epSOS LSP.

##### **6. Certification process mandatory.**

A certification process is not mandatory in any MS. Therefore the certification process cannot be reasonably made mandatory in epSOS LSP, but nevertheless it should be proposed to all participants.

#### **Section 2 – Security Services**

##### **1. Data protection within healthcare organizations.**

All different means proposed (cipher, point-to-point, VPN) are used without a clear prevalence; moreover it is clear that authorities in the majority of cases, do not regulate such a transmission in a homogenous or mandatory way. It is clear that, in the majority of cases, one of the solutions is adopted.

##### **2. Data protection among healthcare organizations.**

Cryptography is the most commonly adopted solution. It is therefore reasonable to assume that data encryption will be the solution adopted for data communication among epSOS LSP NCPs.

##### **3. OSI-layer mechanism to ensure data confidentiality.**

There is a prevalence of transport-based solutions, but with mixed- and application-based solutions as well.

- 4. OSI-layer mechanism to ensure authentication.**  
At this level a prevalence of application-based solution is evident.
- 5. OSI-layer mechanism to non-repudiation.**  
At this level a prevalence of application-based solution is evident.
- 6. Authentication of end-points required.**  
It is required in the majority of MS. This will help the definition of a common standard for a common security approach definition for end-points.
- 7. Access control for PS (Patient Summary).**  
In most MS a mixed approach based on identity and role is adopted.
- 8. Access control for EP (e-Prescription).**  
In most MS a mixed approach based on identity and role is adopted.
- 9. Solution to ensure data integrity.**  
In all MSs digital signature is the solution adopted. This allows the adoption of digital signature as an epSOS LSP security service to ensure data integrity with an almost universal coverage by MSs.
- 10. Mechanisms to guarantee data confidentiality of stored data.**  
Access control is the more commonly adopted solution, with some adoption of data encryption.
- 11. In case of data anonymization, complete or pseudo-anonymization adopted.**  
The mechanism of data anonymization is not widely adopted; where it is adopted both complete anonymization and pseudo-anonymization are used.
- 12. Mechanisms to ensure non repudiation.**  
Both digital signature and secure log are adopted.
- 13. National (and mandatory) standard time at national level.**  
A standard time is available for almost all MS, but adoption is not mandatory for everybody. In the epSOS LSP it should be adopted and made mandatory, to be defined by the time server to be used.
- 14. Definition of service levels (SLA) for data and service availability.**  
There is mandatory definition of SLA in most of the MS. At the epSOS LSP level SLA should be defined at least for NCP.
- 15. Authentication mechanism to grant access to medical data.**  
Smartcards is the most commonly adopted mechanism, while software certificates are widely adopted. Passwords are also accepted.
- 16. Encryption mechanism for medical data.**  
The encryption of medical data is not universally adopted. Where it is present, technical mechanisms vary. At the epSOS LSP level it should be clarified which mechanism (if any) should be adopted.
- 17. Quantity of data encrypted by a single key.**  
No analysis due to different understanding of the question.
- 18. Network security concept granting access only to medical professionals.**

In most MS security mechanisms are in place to grant access to medical organizations only. This is a critical element to be clarified (within the I&A services) at epSOS LSP level.

### **Section 3 – Auditing & logging**

#### **1. Auditing and logging mandatory.**

It is mandatory in the large majority of MS with some exceptions. Despite the principle of non modification of existing national systems which has to be guaranteed, the epSOS LSP should act as a promoter for the universal adoption of Auditing and logging solutions that will facilitate the creation of a “circle of trust” among participants.

#### **2. Access control for audit and logs.**

Where the function exists, a control access exists as well.

#### **3. Accounting capability for the function.**

Where the function exists, a control access exists as well.

#### **4. Minimum and maximum required time for logs conservation.**

Where the service exists there is a common minimum level of six months that seems to be widely accepted. Maximum time for storage varies widely from 1 to several years.

#### **5. Who is allowed to access log.**

In this point the answers are very different. A relevant difference is where the patient is entitled to access his/her own logs and where this is not envisaged. Most MS grant access to specific institutional operators (security officers).

#### **6. Tools for automated log analysis.**

There are tools under test in some MSs, but tools are not present at all in the majority.

#### **7. Logs contain health-related patients data.**

In only one case the answer is “yes” (in part). It should be “no” for everybody.

### **Section 4 – Backup**

#### **1. Availability of back-up and system recovery process (national level, regional level, POC).**

All Member States support backup and system recovery at organization/POC level. epSOS LSP should define backup (if any) at this level

#### **2. Permission of use of any degraded/reduced mode.**

Many member states do not have any degraded or reduced mode, even at POC level.

#### **3. Specification of related impacts for degraded mode (availability delay, no logs, minimal logs).**

See above.

#### **4. Availability of any application’s agent to perform management and/or monitoring activities (yes/no with possible specifications).**

The monitoring system is not defined by almost any Member State

### **Section 5 – Network Security Protocols**

#### **1. Type of protocol adopted for data protection & authentication (IPSEC, TLS).**

TLS is widely adopted.

- 2. Type of public-key cryptographic protocol adopted to create a shared secret key (Diffie-Hellman group 1,2,5 for IPSec, RSA, Diffie-Hellman for TLS).**  
Standard cipher-suites are in place. DH seems to be preferred.
- 3. Name of the encryption algorithm adopted**  
Security standard cipher-suites are in place for encryption. It should not be a problem for the epSOS LSP to define one.
- 4. Name of the public-key cryptographic protocol adopted for user authentication (RSA, pre-shared keys, certificates, DSA, ECDSA)**  
User authentication can be factorized on the use of certificates.
- 5. Name of the algorithm adopted for data authentication (US Secure Hash SHA1, IP auth using Keyed SHA1 (IP-MAC), HMAC-SHA-256/384/512 with IPSec (SHA2)).**  
Both HMAC-MD5 and HMAC-SHA1 are widely used.
- 6. Name of the security protocol adopted to ensure data confidentiality & origin authentication (RFC4302, RFC4835, RFC 4303).**  
There is no common trend on the security protocol adopted to ensure data confidentiality and origin authentication.

## 11 ANNEX. WP3.7 ORGANIZATION AND TIMING

This chapter describes how was:

- the responsible Organisation, the Document organization and the Working Methodology used in WP3.7;
- the activity plan set for the WP.

### 11.1 WP 3.7 Organization

This paragraph provides information about the organization of Project WP 3.7 and the working methodology established.

#### 11.1.1 Authors and reviewers list

Contributor/reviewer		
Name/Names	Organization	(*) Which document
Eliberto Albertini, Giorgio Orsi;	LOMBARDY	(a),(b),(c),(d)
Soren Bittins, Raik Kuhlisch, Jorg Caumans;	FHGISST	(a),(c)
Henrik Lune Nielsen	MEDCOM	(a),(c)
Didier Ambroise, Manuel Metz;	ASIP	(a),(b),(c),(d)
Anders Egnell;	SALAR	(a),(b)
Manuel Koch	GEMATIK	(a),(c)
Massimiliano Masi, Rainer Horbe;	ELGA	(a),(c)
George Pangalos;	THESS	(a),(b)
Celia Varela,Gustavo Rojo	CLM	(a),(b),(c),(d)
Alexander Van Dujin	NICTIZ	(a),(c)
Milan Ruzika	IZIP	(c)
FRANTISEK Sovis, Daniel Olejar	NHIC	(a)

Table 11-1: WP 3.7 Contributors list

- (\*) Legend:
- (a): this document
  - (b). D3.7.2 – Section I – epSOS LSP Security Policy
  - (c): D3.7.2 – Section II – epSOS LSP Security Services
  - (d): D3.7.2 – Section III – epSOS LSP Suitability Analysis

#### 11.1.2 Description of tasks and responsibilities

In order to reach the goal of WP3.7 four editorial working groups (EWG) were defined:

- EWG A, in charge of overall objectives and contest definition;
- EWG B, in charge of security policy definition;
- EWG C, in charge of security services definition;
- EWG D, in charge of congruity and suitability analysis.

Each EWG was managed by a EWG Leader.

The following tables (one for each workgroup) provide more details on the contents of EWGs jobs themselves and identification of leaders and members.

The column named “chapter” summarizes the tasks developed.

<b>EWG A</b>			
<b>Overall objectives and contest definition</b>			
#	<b>EWG Leader: REGLOM</b>		
#	<b>Chapter</b>	<b>Editor Leader</b>	<b>Role played: Contributor (k) Reviewer (r)</b>
01	D3.7.2 Deliverable Physical Organization & Contents	REGLOM	THESS(r), ASIP(r), GEMATIK(r), MEDCOM(r), CLM(r), NICTIZ(r);
02	Introduction ...	REGLOM	THESS(r), ASIP(r), GEMATIK(r), MEDCOM(r), CLM(r), NICTIZ(r);
03	Assumptions & Guidelines	REGLOM	MEDCOM(k), THESS(r), ASIP(r), GEMATIK(r), CLM(r), NICTIZ(r);
04	Overall picture & logical scheme	ASIP	GEMATIK(k), FHGISST(r); THESS(r), MEDCOM(r), CLM(r), NICTIZ(r);
05	Definition of Elements and Actors ...	ASIP	GEMATIK(k), THESS(r), MEDCOM(r), CLM(r), NICTIZ(r), SALAR(r);
06	Security Requirements	REGLOM	GEMATIK(k), NHIC(k), THESS(r), ASIP(r), MEDCOM(r), CLM(r), NICTIZ(r);
07	Reference to section I (Security Policy)	REGLOM	ASIP(r), GEMATIK(r), MEDCOM(r), CLM(r), NICTIZ(r);
08	Reference to section II (Security Services)	REGLOM	ASIP(r), GEMATIK(r), MEDCOM(r), CLM(r), NICTIZ(r);
09	Reference to section III (Suitability Analysis)	REGLOM	ASIP(r), GEMATIK(r), MEDCOM(r), CLM(r), NICTIZ(r);
10	Questionnaire	ELGA	REGLOM (k) THESS(r), ASIP(r), GEMATIK(r), MEDCOM(r), CLM(r), NICTIZ(r);
11	Annex WP3.7 Organization & Timing	REGLOM	ASIP(r), GEMATIK(r), MEDCOM(r), CLM(r), NICTIZ(r);

Table 11-2: EWGA Contributors list

<b>EWG B</b>			
<b>Security policy definition for POC, NCP and global services</b>			
#	<b>EWG Leader: THESS</b>		
#	<b>Chapter</b>	<b>Editor Leader</b>	<b>Role played: Contributor (k) Reviewer (r)</b>
all	Objectives and principles. Security infrastructure (organization and responsibilities). Risk management strategy. Hw/Sw/Communication security services and measures. Physical security. Personal security (training and	THESS	MEDCOM(r), CLM(r), REGLOM(r), SALAR(r), ASIP(r);

	procedures). Security compliance checking.		
--	---	--	--

Table 11-3: EWGB contributors list

<b>EWG C</b>			
<b>Security services definition</b>			
	<b>EWG Leader:</b>		
<b>#</b>	<b>Chapter</b>	<b>Editor Leader</b>	<b>Role played: Contributor (k) Reviewer (r)</b>
01	Introduction...	REGLOM	GEMATIK(r), ELGA(r), IZIP(r), ASIP(r), MEDCOM(r), CLM(r);
02	Access control security services	ELGA	FHGISST(r), GEMATIK(r), REGLOM(r), IZIP(r), ASIP(r), MEDCOM(r), CLM(r);
03	Data integrity security services	NICTIZ	GEMATIK(r), REGLOM(r), MEDCOM(r), ELGA(r), IZIP(r), ASIP(r), CLM(r);
04	Data confidentiality security services	IZIP	ELGA (k); FHGISST(r), GEMATIK(r), REGLOM(r), ASIP(r), MEDCOM(r), CLM(r);
05	Data exchange security services	FHGISST	GEMATIK(r), REGLOM(r), MEDCOM(r), ELGA(r), IZIP(r), ASIP(r), CLM(r);
06	Auditing & accounting security services	REGLOM	GEMATIK(r), ELGA(r), IZIP(r), ASIP(r), MEDCOM(r), CLM(r);
07	Non-repudiation security services	NICTIZ	FHGISST(r), GEMATIK(r), REGLOM(r), ELGA(r), IZIP(r), ASIP(r), MEDCOM(r), CLM(r);
08	PKI concept and operational requirements	CLM	GEMATIK(r), REGLOM(r), MEDCOM(r), IZIP(r), ASIP(r);

Table 11-4: EWGC contributors list

<b>EWG D</b>			
<b>Congruity and suitability analysis</b>			
	<b>EWG Leader: CLM</b>		
<b>#</b>	<b>Chapter</b>	<b>Editor Leader</b>	<b>Role played: Contributor (k) Reviewer (r)</b>
all	Introduction Scope Methodology Analysis details Conclusion	CLM	REGLOM(r), ASIP(r),

Table 11-5: EWGD contributors list

### 11.1.3 EWG Editing process

This chapter gives the instructions used for structuring and deploying the editing process.

### 11.1.3.1 Project Place (PP)

ProjectPlace was the main cooperation means among the workgroup members. E-mail was only used in addition to ProjectPlace. E-mail messages were used to notify the creation and publication of specific documents, without sending such a document as an attachment.

Under the root of WP3.7 in ProjectPlace a folder named <11\_EWG> was set.

Each EWG had a folder assigned under such a EWG folder.

This folder was named “EWGx” where x is the letter of that specific working group, in the range A-D.

All EWG folders were equally structured and contained the same minimum set of documents and folders (see following table).

EWGx			
	Contacts_EWGx	Excel file	contains contact information about the EWG participants
	Timeplan_EWGx	MS Project file	define the timeplan for EWG activities
	Initiation_EWGx	Word file	
	Templates	Folder	contains the template(s) for the editing of each section of the chapter of deliverable in charge for that EWG
	Draft	Folder	contains the versioned draft documents as a result of the EWG members' activities. Drafts can include any type of documents (text, mails, pictures, etc.)
	Comments	Folder	contains comments and suggestions from the EWG members to the previously published drafts
	Released	Folder	Contains documents that the EWG considers in a final version
	References	folder	Contains documents useful for the EWG activities

Table 11-6: WP 3.7 PP structure

This structure was set up in advance by the WPL for all EWGs, while it was the responsibility of the EWG leader to fill such a structure with the needed files.

### 11.1.3.2 Stepping through the WP3.7 editing process

The following sections were a guideline for the EWG Leader through the steps of the editing process.

#### a-Step 1: Initialisation

##### Step 1.1: Set up own editing team

Each EWG Leader was in charge of setting up his/her own EWG structure.

The first step as EWG leader was to get in touch with all the participating organizations, to get confirmation about the contact information and build the file <contacts\_EWGx.xls> and publish it in the appropriate folder. It was the EWG Leader's responsibility to keep such a file updated with all the contact information.

If the EWG Leader didn't get response from a committed beneficiary within 3 working days, he had to inform the WPL immediately.

##### Step 1.2: EWG initiation document and templates

Each EWG had an initiation document describing in brief the:

- objectives to be reached
- content of the documents to be produced by the EWG
- assignment of responsibilities for each sub-task.

It was recommended that the EWG leader wrote the first draft of the initiation document and sent it to the rest of the group for commenting.

A reasonable/short time to share and approve the initiation document had to be allowed. Once the document was approved by both the EWG Leader and the WP leader it was closed. If, in the approval process of the document, open issues were raised without a common agreement, they were assigned to a specific EWG participant who was in charge of making an in-depth analysis with all the EWG members.

The main purpose of the document was that all members of the group had the same perception of what the EWG was in charge of, and each member had a clear understanding of the workload assigned to his/her institution.

For the deployment of the EWG activities, and the drafting of the deliverable sections, the adoption of templates was highly recommended. This was particularly valid for EWGB (policies) and EWGC (security services).

### Step 1.3: Adapting the Schedule

Each EWG leader had to define a time-plan for the activity, including Tconf if needed. The EWG time-plan was derived from the WP overall plan in order to ensure coherence of deadlines.

It was recommended that the EWG leader wrote the first draft of the schedule and sent it to the rest of the group for commenting. Take holiday time into consideration but try to find a resource allocation that allows for stepping forward with reduced speed even during that time.

### **b-Step 2: Collection and review of contributions**

After the end of the initialization phase each EWG leader was in charge of:

- organizing Tconf if/when needed among EWG participant or WP participants who should notify any relevant issue to be raised
- soliciting contributions from participants in due time
- sharing relevant contributions with other WP members when this was considered fruitful
- notifying WP leader (and other WPs) in case relevant issues were raised
- managing assignment of in-depth analysis in case of need
- editing contributions received towards a final version

### **11.1.4 EWG Leader task list**

Each EWG Leader had the following responsibilities:

1. setup his/her own EWG
2. define the contact list of the EWG (contacts\_EWGx.xls)
3. define a work-plan with deadlines (Timeplan\_EWG.mpp)
4. define a template for subtasks contributions
5. assign subtask responsibilities among EWG participants
6. ask/urge for contributions from EWG members
7. define Tconf if/when needed
8. notify WP leader of unsolved issues
9. circulate comments
10. assign in-depth analysis where necessary.

### **11.2 WP 3.7 Working Methodology**

This chapter describes some relevant topics of the working methodologies.

### 11.2.1 Selection of the participants in the tasks in WP3.7

- Each user beneficiary identified one person as a representative in WP3.7. More participants per partner could contribute but one acted as the main contact point (responsible partner);
- Identification of all participants and contact information was placed in the ProjectPlace (PP) (WP 3.7 contact list);
- It was strongly encouraged that the representative of each user beneficiary had security systems experience, better if in Health Information Systems.

### 11.2.2 Tools used for sharing information

They were:

- **epSOS LSP electronic workspace: ProjectPlace** (PP) was used to keep up to date on the progress of the WP (see also paragraph 2.2.1);
- **e-mailing**: through the mailing list for communication of issues regarding 3.7 progress work:
- **conference calls** (referred as *Telco* or *Tcon*):
  - with a specific objective and a previously delivered agenda of the topics to be discussed;
  - agenda delivered with two (roughly) calendar days prior notice;
  - proposed uses:
    - § approval of final TOC of deliverable;
    - § for agreeing on the required changes of contents in each topic of TOC;
    - § opinion pool for discussion of controversial issues.
- **face to face (F2F) meetings**:
  - with a specific objective and a previously delivered agenda of the topics to be discussed;
  - agenda delivered with two (roughly) calendar days prior notice;
  - If possible, to be aligned with PEB meetings;
  - proposed uses:
    - § presentation of 3.7 workplan description and revisions;
    - § for discussion and approval of work-in-progress documents and final reports.
- **specific workshops**:
  - attended only by specific people with recognised experience in the field of security systems;
  - 1-3 days duration;
  - To be held in a country according to the indications of PEB at the proposed dates (these dates were established based on the dependency between the different contents of discussion of the workgroups);
  - Proposed uses:
    - § Reflections and agreement about the different contents of the Deliverables.

### 11.2.3 Methodology for generation of consensus report

- WP leader generated a draft template with main content topics, the person responsible for the contributions of each topic and the deadline: *after the meeting the draft updated TOC, was placed in projectplace*;
- The TOC circulated for at least one week for revision;
- The final TOC was approved in a Telco;
- The final TOC circulated among the partners and each of them worked on its contributions;
- WP leader received contribution from each responsible partner and consolidated document;
- WP leader identified weak or missing points and required refinements, updates or modifications on document submitted;

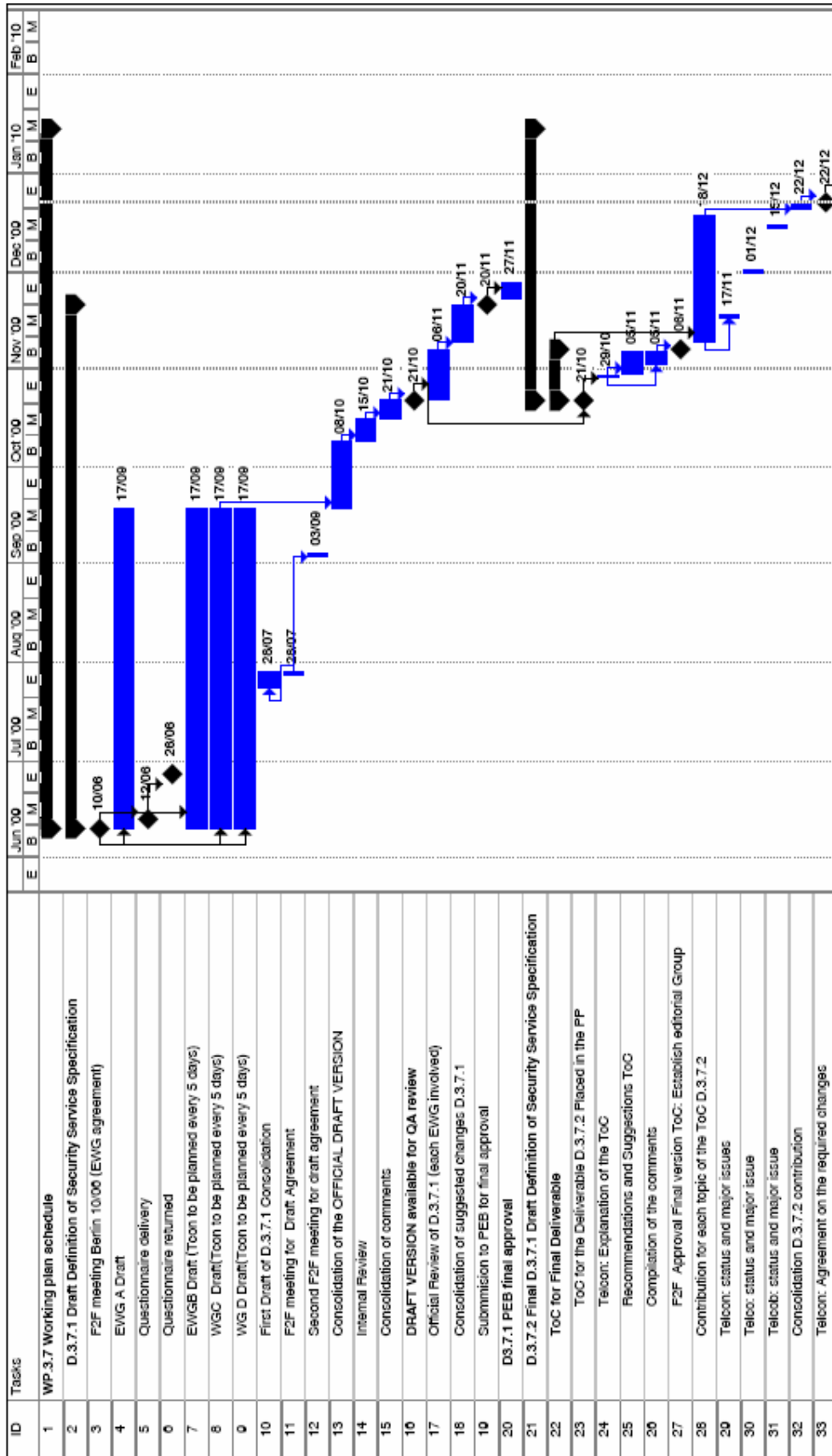
- WP leader circulated the second version of the consolidated draft among the partners;
- Depending on the document quality, the WP leader could require a Telco to discuss and to agree on the required changes and to assign responsibilities for them;
- The changes made were sent to WP leader;
- WP leader consolidated the final version of the Consensus Report and submitted the final version of the document to review by the rest of the beneficiaries and by the Quality manager;
- The final document was discussed and approved by the TPM and submitted for formal approval by the PEB.

#### **11.2.4 Methodology for conflicts resolution**

- Conflicts resolution (*Coordination and Management handbook*):
  - Agreement were reached first by informal contact at WP level.
  - Inform on possible delay via:
    - E-mail to [projectmanagement@epsos.eu](mailto:projectmanagement@epsos.eu).
    - Letter to the Project Coordinator.
    - Adding an Issue under the Issues Tab at [www.projectplace.com](http://www.projectplace.com) (all such issues were entered under the Issues tab at Projectplace so that they could be officially followed up on).
- Potential conflict identified: WP Leader had to mediate between the parties and PC. TPM was to be informed in case the solution affects the work plan and expected results;
- If no solution was reached, the TPM and PC had to mediate, involving if necessary the PEB. An extraordinary PEB meeting could be called;
- In case the PEB could not solve the conflict, the issue was referred to the PSB;
- Should a consensus not be achieved in PSB, decisions were reached by simple majority vote, each delegate having one vote.
  - The PSB could not make a decision binding a participant which would be seriously affected without such a participant's consent.
  - Should a conflict not be resolved by this mechanism, the PC and APM had to consult with the EC Project Officer.

### **11.3 WP3.7 Final timing**

In the following two pages the final timing of the WP3.7 is shown.



Project: WP.3.7 0.1	Tarea		Tareas externas	
	División		Hito externo	
	Progreso		Fecha límite	

Figure 11-1 WP 3.7 Activities Plan

