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
- Congruity-Suitability_analysis-

COVER AND CONTROL PAGE OF DOCUMENT	
Document name:	**WP3.7_D3.7.2_SECTION_III_Suitability_analysis**
Document Short name:	**WP3.7Congruity_analysis**
Distribution level	**PU**
Status	**Final (QR)**
Author(s): **Organization:**	**Celia Varela, Gustavo Rojo, Mar Rojas** **CLM**

Dissemination level: PU = Public, PP = Restricted to other programme participants, RE = Restricted to a group specified by the consortium, CO = Confidential, only for members of the consortium.

ABSTRACT
WP3.7_D3.7.2_SECTION_III_Suitability_analysis **This paper provide a Draft for the epSOS Congruity & Suitability Analysis**

Change History					
Version	**Date**	**Status Changes**	**From**	**Details**	**Review**
V0.1-3	**-**	**Draft**	**CLM**		
V0.4	**18/11/2009**	**Draft**	**CLM**		
V0.5	**22/12/2009**	**Draft**	**CLM**		
V0.55	**13/01/2010**	**Draft**	**CLM**		
V0.6	**13/01/2010**	**Final (QR)**	**CLM**		
V0.7	**05/02/2010**	**Final**			

TABLE OF CONTENTS

1 Introduction

This paper analyses the congruity and suitability of the epSOS Security Services and Policies defined by WP3.7.
Consequently, the present analysis is developed following the security principles and objectives as described in the document *WP3.7_D3.7.2_SectionII_Security_Services*.

In this document five main security objectives with different importance degree are identified:

- **Confidentiality**
- **Integrity**
- **Accountability / Liability**
- **Availability**

In the next sections, the analysis will focus on these four objectives.

2 Scope

The scope assigned to this document is delimited by the following fields and dimensions of security:

- **Administrative: Integrity; Confidentiality.**
- **Technical: Integrity; Authenticity; Confidentiality.**
- **Physical: Integrity; Confidentiality.**

Therefore, in this document the elements to be analysed are approached within these limits provided by the WP3.7

3 Methodology

This document is structured in two main sections: Section 4, Analysis Elements and Section 5, Analysis Details.
In Section 4, the elements that will be deeply analysed in Section 5 are listed. These elements are an input from other Working Groups and the congruity and suitability analysis is done over them.
In section 5, the analysis is performed taking into account the elements of Section 4. No analysis or justification is done in Section 4.

4 Analysis elements

This section identifies the elements that will be deeply analysed in Section 5 in order to check the congruity and the suitability of the documents elaborated within WP3.7.

The main analysis elements can be classified in two groups: elements identified in the Working Groups of WP3.7 and the elements identified in Annex 1.

The first group includes the Security Policies and the Security Services. They are enumerated in the next subsections.

Second group includes the epSOS Actors and the Elements identified in Annex 1, which are enumerated in Sections 4.3 and 4.5.

Section 4.4, shows the relationship between the Security Policies and Services and the epSOS Actors.

Section 4.6 illustrates the relationship (if existing) between the elements in Annex 1 and the Security Policies and Services.

4.1 Security Policies.

WP3.7 has provided the security policies to be taken into consideration. Table 1 shows the security policies:

Security policies
Object & principles
Security infrastructure
Risk management strategy
Security services and measures
Physical security
Personnel security
Security checking

Table 1. Security policies

4.2 Security Services.

WP3.7 has provided the security services to be focused in. They are shown in the next table:

Security services
AC (Access Control)
AA (Auditing & Accounting)
Data-Exchange
Non Repudiation
Data-Confidentiality
Data-Integrity
PKI

Table 2. Security services

4.3 Actors

Both, policies and services described in the two precedent tables should be applied to the epSOS system component (from now on actors). The actors that have been identified by the WP3.7 are[1]:

- **POC (as part of country B HCPO)**
- **NCP-B**
- **NCP-A**
- **Repository (as part of country A HCPO)**

For all these actors, the policies and services can be either required to the actor by the epSOS, what means that the actor should define and implement them. Other policies and services are defined by epSOS, what means that the project will elaborate and implement them during the pilot phase. From now on, these two options will be identified in the tables by a capital letter: R stands for Required and D stands for defined.

[1] See the epSOS Glossary document for the Actors description

4.4 Relationship between Security Services and Policies and the epSOS Actors

Table 3 illustrates for which actors the security policies are required, defined or both.

Actors / Security policies	POC Country B	NCP-B	NCP-A	Repository Country A
Object & principles	R,D	R,D	R,D	R,D
Security infrastructure	R	R,D	R,D	R
Risk management strategy	R ,D	R,D	R,D	R, D
Security services and measures	R	R,D	R,D	R
Physical security	R	R,D	R,D	R
Personnel security	R	R,D	R,D	R
Security Checking	R,D	R,D	R,D	R,D

R – Must be required by epSOS

D – Must be defined by epSOS

Table 3 Security Policies vs epSOS Actors

Table 4 illustrates for which actors the security services are required, defined or both.

Actors / Security services	POC Country B	NCP-B	NCP-A	Repository Country A
AC (Access Control)	R	R,D	R,D	R
AA (Auditing & Accounting)	R	R,D	R,D	R
Data-Exchange		R,D	R,D	
Non Repudiation	R	R,D	R,D	R
Data-Confidentiality	R	R,D	R,D	R
Data-Integrity	R	R,D	R,D	R
PKI		R,D	R,D	

R – Must be required by epSOS

D – Must be defined by epSOS

Table 4. Security Services vs epSOS Actors

4.5 epSOS Elements in Annex1.

One of the objectives of this document is to match the aforementioned policies and services with the elements identified in Annex 1. After studying Annex 1, this is the list of the elements that should be taken into account for this congruity and suitability analysis:

- **Network Infrastructure**
- **Communication protocols and certificates**
- **Identification system (citizen and professionals)**
- **Data management (storage and protection)**
- **Audit Logs**

Additionally, the Service Availability remains outside of the competences of WP 3.7 as shown in the next table:

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

Table 6. WP 3.7 (work tasks).

4.6 Relationship between Security policies and services and epSOS Elements in Annex1.

Next tables, Table 7 and 8, show the matching between the security policies and services and the Elements in Annex 1.

"C" stands for Covered. That means that Element in Annex I is covered and protected by the Security Policy/ Security Services.

NC" stands for Not Covered. That means that Element in Annex I is not covered and protected by the Security Policy, but must be covered and protected by the principles of the Security Policy/Security Services.

"N / A" stands for Not Available. That means that there is not a relationship between the two elements. It doesn't make sense to perform the congruity and suitability analysis between the element of the Security Policy/Security Services and the element in Annex I.

Elements Annex 1 / Security policies	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audit and Logs
Object & principles	C	C	C	C	C
Security infrastructure	C	N/A	C	C	C
Risk management strategy	C	C	C	C	C
Security services and measures	C	C	C	C	C
Physical security	C	N/A	C	C	N/A
Personnel security	N/A	C	C	C	N/A
Security Checking	C	C	C	C	C

Table 7.Security Policies vs epSOS Annex I Elements Table

Next table shows the matching between the security services and the Elements in Annex 1.

Elements Annex 1 / Security servicies	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audit and Logs
AC (Access Control)	C	C	C	C	C

AA (Auditing & Accounting)	C	C	C	C	C
Data-Exchange	C	C	N/A	C	C
Non Repudiation	N/A	C	C	N/A	C
Data-Confidentiality	N/A	C	C	C	C
Data-Integrity	N/A	C	N/A	C	C
PKI	C	C	C	C	C

Table 8. Security Services vs epSOS Annex I Elements Table

Also the analysis must take into account the following requirements from the Annex I:

- **Federated system**
- **Reliability**
- **Safety**
- **Data Security**
- **Identification Security**
- **Transmission**
- **Receipt of data**
- **Trustworthiness of services**

Data-Availability service is not in the scope of the WP3.7

5 Analysis Details

In order to have an overall analysis including security policies, security services, the epSOS actors and the elements in Annex 1, each of the rows of the Tables 3,4,7 and 8 is analysed following this methodology: in first place, we summarize or refers to what the source document states and it follows the analyse or recommendation.

5.1 Security Policies vs epSOS elements:

i. Object & principles.

Actors / Security Policy	POC Country B	NCP-B	NCP-A	Repository Country A
Object & principles	R,D	R,D	R,D	R,D

Section 2.2.1 and Section 2.2.2 of the "WP3.7_D3.7.2_SECTION_I_Security_Policy" states the main principles and objectives that will rule over the epSOS project.

Analysis

Both, the objectives and the principles must be adopted (defined) by all actors involved in the epSOS, as outlined in paragraph 2.8 of the Security Policy.

ii. Security infrastructure.

Actors / Security Policy	POC Country B	NCP-B	NCP-A	Repository Country A
Security infrastructure	R	R,D	R,D	R

Section 2.5 of the document "WP3.7_D3.7.2_SECTION_I_Security_Policy" describes the technical recommendations that should be respected by all the actors in the epSOS project, and considered as a minimum, regarding the security.

Section 3 of the Appendix 1 of the document "WP3.7_D3.7.2_SECTION_I_Security_Policy" also specifies two audit aspects about security infrastructure:

- **Communication and operation management.**
- **Information system development and maintenance.**

Analysis

The security infrastructure should be adopted by all actors in the epSOS LSP, as stated in section 2.8 of the Security Policy. However, actors should respect their respective national legislation and other provisions, like security rules defined in section 2.4 of Security Policy. For this reason, security infrastructure must be

defined for NPC´s, and should be required for National Dataflow (PoC and Repository).

iii. Risk Management Strategy

Actors / Security Policy	POC Country B	NCP-B	NCP-A	Repository Country A
Risk management strategy	R,D	R,D	R,D	R,D

In order to establish a uniform approach throughout the project scope, the Risk Management Strategy, should be defined for each PoC.

Analysis.

This overall strategy would provide policies to reduce the risk level of the epSOS project. However, mechanisms and the way to implement them would be responsibility of each POC. This global strategy would allow to compare consistency within the different POCs risk management mechanisms.

iv. Security Services and measures

Actors / Security Policy	POC Country B	NCP-B	NCP-A	Repository Country A
Security Services and measures	R	R,D	R,D	R

Section 2.5 of the document "WP3.7_D3.7.2_SECTION_I_Security_Policy" describes the technical recommendations that should be respected by all the actors in the epSOS project, and considered as a minimum, regarding the security.

Analysis

In our opinion, the proposed Security Policy establishes, sometimes, repeated guidelines that involve the same aspects, namely: Access Control. We miss aspects such as availability, (not only of data, but of the applications that support it), the

management of security incidents and disaster recovery, for example. We understand the Security Policy as a statement of good purposes, that identifies general attributes that must guide epSOS safety principles, without overlooking any security dimension.

v. Physical Security

Actors / Security Policy	POC Country B	NCP-B	NCP-A	Repository Country A
Physical Security	R	R,D	R,D	R

Section 2.5 of the document "WP3.7_D3.7.2_SECTION_I_Security_Policy" specifies a recommendation about the physical security of the NCP.

Section 3 of the Appendix 1 of the document "WP3.7_D3.7.2_SECTION_I_Security_Policy" also mentions an audit aspect about the physical and environmental security

Analysis

The Security Policy gives the guidelines to protect information, focusing in the physical security on controlling access to determinate secure areas.

vi.Personnel Security

Actors / Security Policy	POC Country B	NCP-B	NCP-A	Repository Country A
Personal Security	R	R,D	R,D	R

Section 2.5 of the document "WP3.7_D3.7.2_SECTION_I_Security_Policy" specifies three recommendations about personnel security. Spec 2, 3 and 4.

Section 3 of the Appendix 1 of the document "WP3.7_D3.7.2_SECTION_I_Security_Policy" also mentions audit aspects about personnel security:

- **Human resources policy.**
- **Access control.**

Analysis

Regarding personal safety, the proposed Security Policy provides guidelines that, from our point of view, do not completely cover the problem. This is illustrated in Section 2.5, spec 4, where aspects like staff selection and recruitment, or staff dismissal and termination are not discussed. This security feature is very relevant, since a large number of security threats are associated to employees inside the organization.

vii. Security Checking

Actors / Security Policy	POC Country B	NCP-B	NCP-A	Repository Country A
Security Checking	R,D	R,D	R,D	R,D

Section 2.5 of the document "WP3.7_D3.7.2_SECTION_I_Security_Policy" specifies three recommendations (number 9, 10 and 11) about security checking.

Section 3 of the Appendix 1 of the document "WP3.7_D3.7.2_SECTION_I_Security_Policy" develops all aspects to consider about Security Checking.

Analysis

It satisfies the purpose and schema of the Audit Policy. However, we can't found a total congruence between the Audit Policy and the Security Policy, since the first one has been created based on the principles of ISO 27002, while the Security Policy is not based in this standard.

In our opinion, the Audit Policy should be defined as a document assessing the validity and the degree of effectiveness of the implemented measures to achieve the objectives defined by the Security Policy. Therefore, in order to audit based on certain principles, these principles should be previously adopted as main guidelines.

5.2 Security Services vs epSOS Elements:

i. AC (Access Control)

Actors / Security Service	POC Country B	NCP-B	NCP-A	Repository Country A
AC (Access Control)	R	R,D	R,D	R

Access Control security service is described in chapter 2 of WP3.7_D3.7.2_SECTION_II_Security_Services document. The service description states the objectives of the Access Control security services and specifies four main paradigms regarding the access control methodologies, suggesting an epSOS approach based on a mixed RBAC and Context-aware.

The Access Control Security Service meets all the requirements demanded by the epSOS Project. These are:

- **epSOS-Req#3.7.04 (Access Control)**
- **epSOS-Req#3.7.05 (Access Control, privilege management and HCP authorization)**
- **NCP-Req#3.7.04 (Access Control)**

In the case of the "*emergency access*", the use case is detailed in a specific section of the access control security service.

Analysis

Thus, every time each MS complies with the previously exposed, in a controlled way by an agency of the NCP, the principles of security demanded by the epSOS Project will be satisfied.

ii. AA (Auditing & Accounting).

Actors / Security Service	POC Country B	NCP-B	NCP-A	Repository Country A
AA (Auditing & Accounting)	R	R,D	R,D	R

The objective of Audit and Accounting security service is to provide a history of transactions and to ensure that it is possible to trace who has performed any action involving an epSOS-NCP transaction. The service MUST also ensure to be tamper-proof to avoid the historical data to be deleted or tampered even by system administrators:

Auditing & Accounting security service is described in chapter 6 of WP3.7_D3.7.2_SECTION_II_Security_Services document.
In the service description, there are two subsections "Security Service Scope" and "Requirements and constraints" that describe main guidelines

<u>Analysis</u>
The implementation of the above safety guidelines can ensure traceability and auditability of the system defined by the epSOS project.

iii. Data-Exchange.

Actors / Security Service	POC Country B	NCP-B	NCP-A	Repository Country A
Data -Exchange		R,D	R,D	

Data Exchange security service is described in chapter 5 of WP3.7_D3.7.2_SECTION_II_Security_Services document.

End-to-End security is among the most important concepts for epSOS security and for the scoping and definition of epSOS security services.

To achieve this objective, in the service description, a classification regarding the trust zones and their associated criticality level is proposed.

In the same document, four levels of End-to-End security are defined.

The security on different layers of the OSI Reference Model is also analysed and the mechanisms for implementing end-to-end security are compared.

As a conclusion, the service description, point out that:

- **epSOS data exchange security services should be primarily focused on web service security mechanisms.**

- **To reach the required level of liability, audit trails MUST be written to accompany the reliable transmission of data.**

- **To support the security objectives of access control and HCP authenticity respective security token MUST be exchanged securely as part of the SOAP Security Header.**

Analysis

Thus, once determined the fully solution to implement, we can confirm that the NCP-A to NCP-B data exchange is compliant with epSOS safety requirements.

iv. Non Repudiation.

Actors / Security Service	POC Country B	NCP-B	NCP-A	Repository Country A
Non Repudiation	R	R,D	R,D	R

Non repudiation security service is described in chapter 7 of WP3.7_D3.7.2_SECTION_II_Security_Services document.

The service description explain the service and the main objective. This is to provide a mechanism for the member states to be able to prevent parties from claiming not to have requested certain information.

Analysis

As shown in the service description to establish the accountability for the actions of originator and recipient, the following non repudiation services are required.

- **Non-repudiation of Origin (NRO) is intended to protect against the originator's false denial of having originated the message.**

- **Non-repudiation of Receipt (NRR) is intended to protect against the recipient's false denial of having received the message.**

In an indirect communication model, like epSOS model, a delivery agent (NPCs) is involved to transfer a message from originator to recipient. In order to support the settlement of possible disputes between originator and delivery agent or between originator and recipient, the non repudiation service on the delivery agent must be required and defined.

v. Confidentiality.

Actors / Security Service	POC Country B	NCP-B	NCP-A	Repository Country A
Confidentiality	R	R,D	R,D	R

Data Confidentiality security service is described in chapter 4 of WP3.7_D3.7.2_SECTION_II_Security_Services document.

The objective of the epSOS confidentiality security service is to provide confidentiality to data stored by the epSOS-NCP in its persistent memory (e.g. hard-disks, tapes) for a (un)limited amount of time.

The combination of all the measures explained in the service description, will ensure compliance with the security requirements imposed by epSOS Project wich are.

- **EpSOS-Req#3.7.06 (Confidentiality)**
- **NCP-Req#3.7.05 (Confidentiality)**
- **NCP-Req#3.7.07 (Protecting Data Storage)**

Analysis

However, the technique to perform the anonymisation of data it should be specified in more detail.

vi. Integrity

Actors / Security Service	POC Country B	NCP-B	NCP-A	Repository Country A
Integrity	R	R,D	R,D	R

Data Integrity security service is described in chapter 3 of WP3.7_D3.7.2_SECTION_II_Security_Services document.

In the service description, solutions are proposed for safety protection in nodes NCP-B and NCP-A, and a classification of information has been made in order to understand the importance of integrity for each type of data (healthcare-related, critical meta data, non-critical personal data and administrative data)

Analysis

The measures proposed in the service description for the integrity must be tuned as the project progresses. The data handled by each process should be identified, and thus determine which technical measures must be implemented to ensure the required level of integrity.

vii. PKI.

Actors / Security Service	POC Country B	NCP-B	NCP-A	Repository Country A
PKI		R,D	R,D	

PKI security service is described in chapter 8 of WP3.7_D3.7.2_SECTION_II_Security_Services document.

The service describes how defined Public Key Infrastructure meets satisfactorily the intended objectives.

- **Identification, authentication, and confidentiality objective**
- **Integrity and non-repudiation objective**

As outlined in the epSOS Project, each MS is responsible for implementing their own PKI's.

Analysis

The objective of PKI security service is to supply certificates and validation services that will be used to ensure the confidentiality and the integrity of the services of epSOS Patient Summary and ePrescription.

We alert that the implementation of PKI Service is complex, and if not handled correctly it could mean a significant expenditure of resources, without obtaining the benefits associated with this service. Thus, PKI service implementation should be done in an extremely carefully way.

5.3 Security Policies vs epSOS Annex I Elements:

i. **Object&principles.**

Elements Annex 1 / Security Policy	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
Object & principles	C	C	C	C	C

Section 2.2. of "The epSOS Security Policy.doc" identifies the main principles and objectives regarding the security policies.

Analysis

The set of Objectives & Principles defined by the Security Policy meets security requirements of the epSOS project and they can be extended to all the elements.

ii. Security Infrastructure

Elements Annex 1 / Security Policy	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
Security Infrastructure	C	N/A	C	C	C

Section 2.5 of "The epSOS Security Policy.doc" provides detailed technical recommendations, especially number 1, 6 and 7 regarding the security infrastructure.

Section 3 explaining the security audit policy, covers specially the following audit aspects regarding security infrastructure:

- **Communication and operation management**
- **Information system development and maintenance**

Analysis

The implementation of these measures, allows us to assure that the security infrastructure will be correctly managed.

We assume that each MS has a Security Infrastructure that meet security requirements and audit points.

iii. Risk management strategy

Elements Annex 1 / Security Policy	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
Risk Management strategy	C	C	C	C	C

Analysis

There is no reference in the document "The epSOS Security Policy.doc" about Risk Management Strategy and contingency plans, meaning, transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk or accepting some or all of the consequences of a particular risk.

Risk management must be done in all the elements of Annex I, as a proper risk management should include the whole of the elements involved in the epSOS project. This is a key premise when defining guidelines to mitigate risks related to the system, that would condition the project behaviour since the beginning.

We assume that each MS has a Risk Management Strategy according to these audit points.

In the other hand, these aspects are properly addressed in the "WP3.7_D3.7.2_Security_Services", section 3.2.

iv. Security services and measures

Elements Annex 1 / Security Policiy	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
Security Services and measures	C	C	C	C	C

Section 2.5 of "WP3.7_D3.7.2_SECTION_I_Security_Policy" provides detailed technical recommendations.

Analysis

Security measures and services depicted in the Security Policy protects to all the elements defined in Annex I.

v. Physical Security.

Elements Annex 1 / Security Policy	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
Physical security	C	N/A	C	C	N/A

Section 2.5 of "WP3.7_D3.7.2_SECTION_I_Security_Policy" specifies technical recommendations regarding the physical security:

1. ***The national portal server (NCP) is located in a safe environment, where physical access is controlled and allowed only to authorized staff, based on written and accepted statements, following the general design.***

Section 3 explaining the security audit policy, covers specially the following audit aspects regarding security infrastructure:

- **Physical and environmental security**

Analysis

As a consequence of the precedent paragraphs, the elements concerned by the physical security seem to be correctly managed from a security point of view.

vi. Personnel security.

Elements Annex 1 / Security Policy	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs

Personnel security	**N/A**	**C**	**C**	**C**	**N/A**

Section 2.5 of "WP3.7_D3.7.2_SECTION_I_Security_Policy" provides detailed technical recommendations, especially number 2, 3 and 4 regarding the personnel security.

Section 3 explaining the security audit policy, covers specially the following audit aspects regarding security infrastructure:

- **Human resources policy**
- **Access control**

Analysis

Personnel security covers to all elements of Annex I affected

vii. Security Checking

Elements Annex 1 / Security Policy	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
Security Checking	**C**	**C**	**C**	**C**	**C**

Section 2.5 of "WP3.7_D3.7.2_SECTION_I_Security_Policy" provides detailed technical recommendations, specially number 9, 10 and 11 regarding the Security Checking.

In section 1.2.5 about security audit requirements it states:

- **Each National epSOS Portal (NCP) must pass through a security audit.**
- **The security audit must be conducted yearly to audit the systems by ISO/IEC 17799 or ISO/IEC 27001, or equivalent level standards, according to the above listed requirements and the technical recommendations**

provided by the consortium in this respect. Audit will be based on the epSOS security audit policy, described in annex 1 of this security policy.

Finally, Section 3 explaining the security audit policy covers specially the audit aspects regarding security checking.

Analysis

All the elements involved in the epSOS Project are included in the validation of the control effectiveness and the implemented of security measures, as well as, the degree of reducing the associated risks.

5.4 Security Services vs epSOS Annex I Elements:

i. AC (Access Control)

Security services \ Elements Annex 1	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
AC (Access Control)	C	C	C	C	C

Analysis

In order to meet the following security requirements as stated in the Access Control chapter of WP3.7_D3.7.2_SECTION_II_Security_Services document.

- ***EpSOS-Req#3.7.04 (Access control): The confidentiality and integrity of epSOS information assets must be protected by preventing unauthorised access and use.***

- ***EpSOS-Req#3.7.05 (Access Control, privilege management and HCP authorization): 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 in respect to the data and services.

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

The Access Control Security Service fulfils EpSOS-Req#3.7.04 because it is enforcing an access control decision prior to give access to a resource. The EpSOS Req#3.7.05 is satisfied because the access control decision is based upon the role played by the HCP (as per PBAC/RBAC mechanism). The NCP-Req#3.7.04 is satisfied because the actors involved in the ACS are grouped within the epSOS-NCP, so the epSOS-NCP is providing an Access Control mechanism.

ii. AA (Auditing & Accounting)

Elements Annex 1 / Security services	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
AA (Auditing & Accounting)	C	C	C	C	C

Analysis

A&A Security Service is intended as a service that covers all elements of epSOS Project as stated in the whole list of the requirements defined in the Auditing & Accounting chapter of WP3.7_D3.7.2_SECTION_II_Security_Services document.

- **EpSOS-Req#3.7.10 (Accounting)**
- **EpSOS-Req#3.7.11 (Auditing)**
- **EpSOS-Req#3.7.12 (Fraud detection)**
- **NCP-Req#3.7.11 (Accounting and Control)**
- **NCP-Req#3.7.12 (Auditing)**
- **NCP-Req#3.7.13 (fraud detection):**
- **NCP-Req#3.7.14 (Continuously Logging)**

- **NCP-Req#3.7.15 (Securing Access to Audit/Account Logs)**
- **NCP-Req#3.7.16 (Logging Transactions)**
- **NCP-Req#3.7.18 (Minimum Content of Accounting Logs)**
- **NCP-Req#3.7.19 (Reporting Every Access medical information – notifications included)**

More details are provided, justifying this global A&A strategy in the same document explaining the technical requirements that the system devoted to audit collection must meet:

In order to design such a system the following technical requirements must be met:

- *1*. **the PHYSICAL system(s) hosting the audit collection processes and the audit data (logs)must be physically protected (closed environment, access control,)**
- **2. the MACHINE(s) hosting the audit collection processes and the audit data (logs) must be UNACCESSIBLE by Technical staff users;**
- **3. users allowed/entitled to access the audit system will ONLY have the right to access in READING the logs, without having access to other system functions**
- **4. audit data (logs) must be stored on non-modifiable supports (WORM)**
- **5. The communication between epSOS-NCP and the Audit trails secure storage should be secured and both systems should also authenticate each others.**

iii. Data-Exchange

Elements Annex 1 / Security services	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
Data-Exchange	C	C	N/A	C	C

Analysis

The epSOS topology of epSOS-NCPs is a peer-to-peer network of autonomous application level gateways. Each gateway corresponds to a set of service endpoints which mediate requests into the national healthcare infrastructure. Data exchange security services provide message exchange end-to-end security between the sender and the receiver of a message which are both located on the application level (ISO layer 7). In case of epSOS these are the epSOS-NCP gateways of the two countries where the patient is insured and where he is receiving medical care. However, the Element "Audit & Logs" is a factor covered by the Data-Exchange Service, because the solution shown in Data Exchange chapter of *WP3.7_D3.7.2_SectionII_Security_Services* just applies to the message payload level.

- **To reach the required level of liability, audit trails MUST be written to accompany the reliable transmission of data.**

iv. Non Repudiation.

Elements Annex 1 / Security services	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
Non repudiation	N/A	C	C	N/A	C

In chapter 7 of *WP3.7_D3.7.2_SectionII_Security_Services*, the Non-repudiation services are explained and also their main objective. This is to provide a mechanism for the member states to be able to prevent parties from claiming not to have requested certain information.

Analysis

In the service description, in order to establish the accountability for the actions of originator and recipient, the following non repudiation services are presented:

- **Non-repudiation of Origin (NRO) is intended to protect against the originator's false denial of having originated the message.**

- **Non-repudiation of Receipt (NRR) is intended to protect against the recipient's false denial of having received the message.**

Moreover, when a delivery agent is involved to transfer a message from originator to recipient, in order to support the settlement of possible disputes between originator and delivery agent or between originator and recipient, the following non repudiation services are presented:

- **Non-repudiation of Submission (NRS) is intended to provide evidence that the originator submitted the message for delivery. Evidence of Submission (EOS) is generated by the delivery agent, and will be held by the originator.**

- **Non-repudiation of Delivery (NRD) is intended to provide evidence that the message has been delivered to the recipient. Evidence of Delivery (EOD) is generated by the delivery agent, and will be held by the originator. Similarly, we should be aware that evidence provided by this service cannot be used to make further deductions about the delivery status without some sort of assumption on the communication channel.**

For this purpose, the Non-Repudiation Service establishes a set of evidences and phases (generation, transfer, verification, storage, and dispute resolution) that allow us to confirm that all Elements of Annex I are covered by the aforementioned service.

v. Confidentiality.

Elements Annex 1 / Security services	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
Confidentiality	N/A	C	C	C	C

Objective of the epSOS Confidentiality Security Service is to provide confidentiality to data stored by the epSOS-NCP in its persistent memory (e.g. hard-disks, tapes) for a (un)limited amount of time.

Analysis

The encryption (of messages and data) addressed by the Confidentiality Security Service, allows us to ensure compliance with the requirements demanded by epSOS:

- **EpSOS-Req#3.7.06 (Confidentiality)**
- **NCP-Req#3.7.05 (Confidentiality)**
- **NCP-Req#3.7.07 (Protecting Data Storage)**

This means that all Elements of Annex I are covered by this Security Service.

vi. Integrity.

Security servicies \ Elements Annex 1	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
Integrity	N/A	C	N/A	C	C

Guaranteeing the integrity of data means to introduce the measures against undetectable modification of data. In a broader sense the integrity must covers the technical systems consistency/robustness.

Analysis

Both solutions proposed (use of documents fingerprints and use of digital signatures), covers Elements of Annex I.

vii. PKI.

Security servicies \ Elements Annex 1	Network Infrastructure	Communication protocols and certificates	Identification system	Data management	Audits and Logs
PKI	C	C	C	C	C

The objective of PKI security service is to supply certificates and validation services that will be used to ensure the confidentiality and the integrity of the services of epSOS Patient Summary and ePrescription.

Analysis

As the PKI Security Service provides certificates and a service to validate them, the proposed solution covers all Elements in Annex I.

6 Conclusions

The epSOS project is extremely complex with direct implications in patient privacy, legal requirements and technical measures. So, we wish to note that the whole dimension of the project should be subjected to a continuous improvement process regarding the information security.

Analysis and recommendations about the Security Policy related to the epSOS Actors

In a general way, the relationship between the guidelines provided by the Security Policies and the epSOS Actors respects the desired degree of congruity.

However, there could be an improvement regarding the strategy of the management risk. In our opinion, the acceptable level of risk for each POC should be commonly defined by the epSOS project whereas, risk management, protection implementation and reducing risk mechanisms could be under the responsibility of each POC, but being supervised by the corresponding NPC. From a Security Policy point of view, we think that is interesting to propose a Risk Management methodology based in formal risk analysis. This methodology is actually mentioned in the WP3.7_D3.7.2_SECTION_II_Security_Services document, but it is NOT in the Security Policy. This can lead to a lack of congruence between the principles of security required by the Project epSOS and content of the Policy Security

Regarding the Security Services and Measures, Security Policy defines reiterative guidelines that would affect the same aspects, namely: Access Control. We recommend to include aspects such as availability, (not just data, but the related applications), security incidents management and disaster recovery, for example.

Personnel security covers important aspects, since a large number of security threats are related to the employees within the organization. We recommend to include guidelines regarding recruitment and contract ending in the Security Policy.

The strategy to validate the effectiveness of the implemented security measures is described in the Audit Policy (Annex I of the Security Policy). However, in our

opinion, there is a lack of consistency in the Audit Policy as the audit is based on the standard ISO / IEC 27001, rather than on the principles agreed in the Security Policy.

Analysis and recommendations about the Security Services related to the epSOS Actors

Regarding the Security Services, we want indicate that both, I & A (Identification and Authentication) and Data Availability, should not be referenced in this analysis, as they are not the responsibility of the WP 3.7. The same can be applied to the column of "Service Availability" included among the epSOS Elements.

AC Security Service is one of the main points to be determined by the safety principles of the epSOS Project, since it is closely related to patient safety and to compliance with demanded legal requirements. A priori, the proposed methodology (mix between RBAC and Context-aware access control methodologies) seems to be a perfectly consistent solution to bring the optimal security level required by existing health regulations.

A & A appears as a fundamental Security Service to guarantee the tightness of the system against unauthorized access and for avoiding misuse of the epSOS components. As we mentioned in the corresponding section, Audit & Accountability should be understood as a Security Service that must cover all elements of epSOS. After analyzing the congruence of this Service with the epSOS security principles, we don't detect security objectives that might be neglected.

Data-Exchange is one of the most complete Services, and its correct implementation will ensure the integrity, confidentiality and authenticity of the system. The approach made over this service seems to be the most appropriate.

About Non-repudiation Service, in principle, it seems to be important to maintain this security dimension between the NCP transactions, as required in the security services prerequisites.

The measures defined by the Data-Confidentiality Service, fully satisfy the safety objectives. The adoption of the AES algorithm seems the better solution. However, the technique to perform the anonymisation of data it should be specified in more detail.

Regarding to the Data-Integrity Service, we will have to assess which of the proposed solutions are the most effective from the security point of view, and to update the technical aspects involved. Anyway, the congruity between this service and the epSOS Actors seems to be assured.

For the proper establishment of the PKI Service, we must take into account the complexity associated with implementing an infrastructure of such dimension, so the proposed solution meets satisfactorily the intended security objectives and consequently the required level of congruity.

Analysis and recommendations about the Security Policy related to the elements of Annex I

Same analysis and recommendations apply for the relation between the Security Policy and the Elements of Annex I and the Security Policy and the epSOS Actors, see above.

Analysis and recommendations about the Security Services related to the elements of Annex I

The only aspect that can be stressed is the reaching of the level of congruity desired between security services related to elements of Annex I.
Finally, just as a reminder, the I&A and Data-Availability are out of the scope of the WP3.7 whereas PKI service has been included.

Other recommendations

We recommend to implement Security Policy guidelines based in continuity and contingency plans, incident management and delegating and accepting responsibilities.

We also recommend to include in the Security Policy two other security mechanism:

- **A continuous improvement process based on periodic reviews of the principles and safeguards in place,**
- **The adoption of preventive and corrective measures to correct security deficiencies.**

To this end, as already stated previously, we believe that the elements that are going to be audited should follow the main Security Policy guidelines.

- **Moreover, from our point of view, we miss some uniformity about the approaching that describes each of the Security Services.**