



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
- epSOS Security Policies -

WORK PACKAGE	3.7
DOCUMENT VERSION	0.7
DATE	16.06.2010

COVER AND CONTROL PAGE OF DOCUMENT

Document name:	The epSOS Security Policy
Distribution level*	PU
Status	Final
Author/ person responsible: Contributors:	George Pangalos (THESS)

* Distribution 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.

Sub-Project Identification	
Work Package	WP3.7 (Security)
Working Group	EWG B (Security Policy)

Abstract
<p>This document describes the epSOS security policy. Security is a critically important issue for epSOS. Without adequate security in place none of the epSOS services can be used in real-life environments. A security policy is therefore needed to define a secure operational environment for the epSOS service deployment and create a ‘chain of trust’ among all epSOS actors that will make possible the implementation of the cross border epSOS services. The epSOS security policy must be sufficient for protecting the epSOS data and processes, implementable and agreed upon by all partners. A security audit policy is also described in this document. The security policy must be periodically re-examined. It must also be periodically audited to ensure member’s conformance and compliance with its provisions. The document has been constructed in such a way, so that section 2 (Security Policy) can be directly annexed to the contractual agreement to be prepared by WP2,1 and signed by the participants in pilot epSOS implementations.</p>

History of Alteration				
Version	Date	Status Changes	From	Review
V0.1	23/07/2009	draft	G. Pangalos (THESS)	WP3.7/EWG B
V0.2	13/08/2009	Commented by WP3.7	WP3.7 members	WP3.7
V0.3	09/09/2009	Commented by WP3.7	WP3.7 members	WP3.7
V0.4	22/09/2009	Commented by WP3.7	WP3.7 members	WP3.7
V0.5	14/11/2009	Commented by QR (D.3.7.1)	Quality Reviewers (D.3.7.1)	QR
V0.6	21/01/2010	Pre-Final (QR)		QR
V0.7		Final (QR)		

1	NEED FOR SECURITY - epSOS SECURITY REQUIREMENTS	4
1.1	NEED AND SCOPE	4
1.2	epSOS SECURITY REQUIREMENTS	4
1.2.1	Security awareness requirements:	4
1.2.2	Organizational requirements:	4
1.2.3	Legal requirements:	5
1.2.4	Technical requirements:	5
1.2.5	Security Audit requirements:	6
2	THE epSOS SECURITY POLICY	7
2.1	NEED AND SCOPE	7
2.2	PRINCIPLE AND OBJECTIVES	7
2.2.1	Principle	7
2.2.2	Objectives	7
2.3	CONTEXT DESCRIPTION	8
2.3.1	Actors	8
2.3.2	Data exchanges	8
2.3.3	Legal basis	9
2.4	SECURITY RULES	10
2.5	TECHNICAL RECOMMENDATIONS	10
2.6	SECURITY AUDIT	11
2.7	REFERENCES	12
2.8	RECOMMENDATIONS	12
	THE epSOS SECURITY AUDIT POLICY	13

1 NEED FOR SECURITY - EPSOS SECURITY REQUIREMENTS

1.1 NEED AND SCOPE

Security is a critically important issue for epSOS. Without adequate security in place none of the epSOS services can be used in real-life environments. A security policy (SP) is therefore needed to create a secure operational environment for the service deployment. The epSOS security Policy must be sufficient for protecting the epSOS data and processes, implementable and agreed by all interacting partners. It must also contribute to create the necessary 'chain of trust' among all epSOS actors that will make possible the implementation of cross border epSOS services. Finally, the security policy must be periodically audited, to ensure member's conformance and compliance with its provisions.

1.2 EPSOS SECURITY REQUIREMENTS

The following list describes the epSOS security requirements that are identified as critical for the security of the epSOS system and processes and form the basis for constructing the Security Policy. These requirements are based on the security best practices in the field of health by epSOS beneficiaries.

1.2.1 Security awareness requirements:

- Make participants aware of the risks that threaten the epSOS data and processes, and the information and information systems of the epSOS partners, and the available means of protection.
- Make users aware about information security and train them using the authentication mechanisms in place. Also to understand the related standards and policies and recognise and accept the responsibility for protecting the passwords, smart cards, private keys, etc., by signing the related statements.
- To enhance user and patient' trust in the epSOS information system.

1.2.2 Organizational requirements:

- Create a general security framework / set of security principles adapted to the epSOS information system needs, to be followed by people that are in charge of epSOS processes and put in place appropriate measures and procedures in order to ensure the information and information system security.
- Facilitate the effective governance of shared information assets and effectively oversee the security management arrangements.
- Promote cooperation between various actors of the consortium in order to elaborate and put in place those measures, instructions and procedures.

- Ensure that the epSOS IT infrastructure and software on which the system is running is up to date, provides all the necessary security updates and is compatible with national domain systems.
- Ensure that epSOS processes do not require unacceptable changes to the local (national competency) systems already in place.
- Ensure the separation of duty among epSOS actors (identity providers, data service providers, etc).
- Ensure that an effective information security incident management process for the epSOS infrastructure exists and contracting parties, as defined later in this document, will cooperate in investigating security incidents.

1.2.3 Legal requirements:

- Ensure that the information system in place respects all related National and European laws on privacy and data protection in force. This is based on the following principles:

§ For the NATIONAL dataflow, the actors should respect the respective national legislation on privacy and data protection in effect.

§ For the CROSSBORDER (interstate) dataflow, as a pan European network, the EPSOS actors will respect at least:

- the European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- the European Directive 2002/58/EC on privacy and electronic communications
- the related legal requirements identified in the 'Legal and regulatory constraints on epSOS' document, prepared by epSOS WP2.1 (3)

1.2.4 Technical requirements:

- All epSOS data flows must be adequately protected, covering both the member state requirements and the agreed epSOS minimum standards
- End Users (patients, HCPs, etc.) must be clearly identified by the National Contact Point (NCP) providers before being able to enter the system.
- Mutual authentication between End Users and the National Contact Point providers (NCPs) is needed when connecting to the system
- Mutual Authentication between National Contact Point providers of different Member State is needed, when initiating a crossborder information flow.
- The national portal server is located in a safe environment, according to current standards (e.g. physical access is controlled and allowed only to authorized staff, based on written and accepted statements, following the general design).
- Administration access to the National Contact Point is limited to appropriate staff only (e.g. administrators, security officers). Administrative users are using appropriate means of authentication (e.g. strong passwords, or an equivalent means like smart cards, electronic signatures etc.).

issued and used according to a suitable Certificate Policy. Digital certificates are issued by a Certification Authority(ies) which is appropriately accredited by the national authorities or equivalent (e.g. the “Webtrust programme for Certification Authorities”, the standard framework of AICPA/CISA, tScheme, or equivalent)

- The system is using appropriate procedures to ensure data for audit trail
- Special attention must be given to the Root Certificate Authority, which is issuing the certificates for the National Portal/NCP (Portal to Portal certificates), in order to ensure that this Certification Authority can be trusted and can be accepted as root authority. For this purpose the root Certification Authority must be certified by the national authorities or equivalent (e.g. the “Webtrust programme for Certification Authorities”, the standard framework of AICPA/CISA, tScheme, or equivalent).

1.2.5 Security Audit requirements:

- End user identification and authentication means must have been audited and certified by an independent organization which is certified by the national authorities or equivalent (e.g. the “Webtrust programme for Certification Authorities”, the standard framework of AICPA/CISA, tScheme, or equivalent)
- National contact point provider authentication means must have been audited and certified by an independent organization which is CERT^{*} certified according to the state of the art.
- National Contact Point provider Data and Privacy protection procedures in place must have been audited and certified by the responsible national data protection supervisory body.
- Each National epSOS Portal (NCP) must pass through a security audit according to international standards. The security audit must be repeated yearly.
- Security audits must be conducted yearly to audit the systems by ISO/IEC27001, ISO/IEC 17799 / ISO/IEC 27002, or equivalent level standards, according to the above listed requirements and the technical recommendations provided by the consortium in this respect. Security audit should also cover risk management issues. (see also appendix 1).
- Audit must approve the fulfilment of the application installation and operation of security principles and guidelines.

The above security requirements will be reviewed each year by the consortium and updates will be made according to the state of the art.

(*) For further information see <http://www.cert.org/csirts/> and <http://www.cert.org/certification/>

2 THE epSOS SECURITY POLICY

2.1 NEED AND SCOPE

Security is a critically important issue for epSOS. Without adequate security in place none of the epSOS services can be used in real-life environments. The epSOS security Policy (ESP) aims to create a secure operational environment for the service deployment which will be sufficient for protecting the epSOS data and processes, implementable and agreed by all participants. The epSOS security policy provides a secure operational environment for epSOS, helps develop a 'chain of trust' among epSOS actors and has been developed according to the provisions of the Technical Annex of the project and the contract. The security policy also specifies the obligations of service providers and users and must be approved, implemented and periodically audited by all epSOS partners, as described below.

2.2 PRINCIPLE AND OBJECTIVES

2.2.1 Principle

All epSOS data and processes must be adequately protected. The network build among the epSOS partners should also not add any unacceptable new risk within any partner organization. Appropriate technologies and procedures must be used to ensure that data is stored processed and transmitted securely over the network build among the epSOS partners and is only disclosed to authorized parties.

Information security is generally characterized as the protection of (a) *Confidentiality* (information is protected from unauthorized access or unintended disclosure - only authorized users have access to the information and other system resources), (b) *Integrity* (information is protected from unauthorized modification), (c) *Availability* (resources are available, without unreasonable delay - authorized users are able to access information and the related means when they need it).

The epSOS security policy should help to ensure and enforce the above. It should also provide means of proof and essential checks which give users trust in the given information.

2.2.2 Objectives

The objective of the epSOS security policy is to establish the basic security provisions that must be satisfied in order to ensure the security of data and system continuity and to prevent and minimise the impact of security incidents by implementing a stable, reliable and secure infrastructure.

More specifically, the epSOS security policy objectives are:

1. To make actors sensitive in the operated means of protection and in the risks which they cover.
2. To create a general security framework adapted to the epSOS information system needs, to be followed by those in charge of epSOS processes, and to put in place measures and procedures in order to ensure the epSOS information and epSOS information system and infrastructure security.

elaborate and put in place those measures, instructions and procedures.

4. To enhance user and patient' trust in the information system.
5. To ensure that the information system in place respects the National and European legislation on privacy and data protection in force.

The epSOS security policy is constructed under the principle of well-proportioned answer to the incurred risk.

2.3 CONTEXT DESCRIPTION

2.3.1 Actors

The actors that interact in the epSOS system are:

1. The epSOS End Users: patients (individuals who visit a health care provider or pharmacist in the country of their temporary stay and request an epSOS service), other users participating in the epSOS processes (Health Care Professionals, System Administrators, Ps-summary / e-prescription data controllers, etc).
2. The requesting party: the Health Care Professional (HCP) or Health Care Professional Organization (HCP-O) in the country of temporary stay of the patient, who currently has an epSOS related care relationship with a patient, or a pharmacists providing an epSOS service
3. The release party: the Health Care Professional (HCP) or Health Care Professional Organization (HCP-O) in the country of origin of the patient who has previously made an epSOS related care or has written an e-prescription to the patient.
4. The epSOS Point of Care (PoC) and epSOS NCP: the epSOS service providing points and IT infrastructure systems created for the crossborder request and disclosure of the epSOS patient summary and/or the execution of e-prescriptions of the patient.

2.3.2 Data exchanges

There are two dataflow levels to be distinguished in the epSOS system (figure 1):

- a. The NATIONAL dataflow level (national domain dataflow):
Between the End User (PoC), the National Contact Point (NCP) / IT service supplier, and the National Repository, or, any other epSOS related national dataflows.
- b. The CROSSBORDER - INTERSTATE dataflow level (crossborder domain dataflow):
Between the National Contact Point (NCP) service supplier of the Member State of patient's Temporary Stay and the National Contact Point (NCP) service supplier of the patient's Member State of Origin.

The exchange of data in the epSOS context can be modelled as follows (figure 1):

- 1- **Authentication and administration Data:** Exchanged from End User's point of care (POC) to National Contact Point (NCP) Providers, and vice versa. Authentication data clearly identify the End User, and document its entitlement for the service. Part of this data is added to the logs.

NCP of the Member State of Temporary Stay, and the National Contact Point (NCP) service supplier of the Member State of Origin.

3- Patient e-prescription Data: Exchanged between the End User's point of care (POC) /NCP of the Member State of Temporary Stay, and the National Contact Point (NCP) service supplier of the Member State of Origin.

4- Validation data: Exchanged between the National Contact Point Provider (NCP) and the End Users (POC). Validation data may contain patient administrative data, validation decision data, additional data qualifying the transactions, etc. (existence and content based on general design)

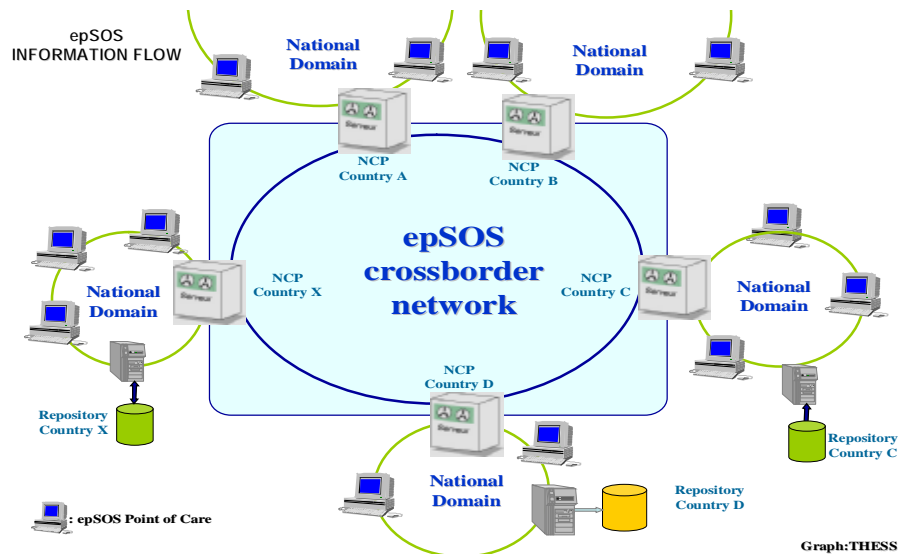


Figure 1: General information flow - exchanges of data in the epSOS context

2.3.3 Legal basis

The following principle applies:

- For the NATIONAL dataflow, the actors should respect the respective national legislation on privacy and data protection and other related national legal provisions in effect.
- For the CROSSBORDER - INTERSTATE dataflow (as a pan European network), the epSOS actors will respect at least the following:
 - The European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
 - the European Directive 2002/58/EC on privacy and electronic communications
 - The relevant EU Directives and Recommendations, as identified in the 'Legal and regulatory constraints on epSOS' document, prepared by WP2.1 (3)

The following general security rules are specified and apply for the epSOS data exchange model:

SR 001	epSOS dataflows must be adequately protected, as specified in international standards.
SR 002	End users must be clearly identified by national contact point providers (epSOS NCP portals) before being able to enter the system.
SR 003	Mutual authentication between End Users and the national contact point providers is needed when connecting to the system
SR 004	End user identification and authentication means must have been audited and certified by an independent organization which is certified by the national authorities according to the state of the art and international standards.
SR 005	National contact point provider Data and Privacy protection procedures in place must have been audited and certified.
SR 006	National contact point provider authentication means must have been audited and certified by an independent organization which is CERT* certified according to the state of the art and international standards.
SR 007	Mutual Authentication between national contact point providers (NCPs) of different Member State is needed, when initiating a trans European (cross border) information flow.

Rules SR002, SR003, SR004 are a national (national level) competency, while rules SR005, SR006, SR007 are a pan European (epSOS level) competency.

In addition, epSOS actors and processes must also take into account the relevant security provisions of:

- The security recommendations of the 'draft recommendation of the commission on e-health interoperability' (section 4.1: security), EU, July 2007.
- The 'Legal and regulatory constraints on epSOS' document, prepared by WP2.1 (3)

2.5 TECHNICAL RECOMMENDATIONS

Following the abovementioned provisions and security rules defined in section 2.4 above, the following minimum set of technical recommendations must be respected by all actors in the epSOS LSP. Compliance will be proved by the security audit procedure, as specified in section 2.6 below.

1. The national contact point (NCP) server is located in a safe environment, where physical access is controlled, monitored and allowed only to authorized staff, based on written and accepted statements, following the general design and international standards.
2. Running and administration access to the national contact point (NCP) is limited to appropriate staff only (e.g. administrators, security officers). Administrative users are using for this purpose strong passwords or an equivalent means of authentication (e.g. smart cards, etc.).
3. Logical Access to the National contact point (NCP) is protected by personal digital certificates, which are issued by a Certification Authority which is appropriately accredited by the national authorities or by the "Webtrust programme for Certification Authorities", the standard framework of AICPA/CISA, tScheme, or equivalent.
4. Users are adequately aware about information security and trained in using the authentication means in place. They have also accepted the responsibility for protecting the passwords, smart cards, private keys, etc., by signing an official statement.
5. The system is using appropriate logging procedures to ensure data for audit trail.
6. An adequate separation of duty between the identity providers and the data service providers within the epSOS processes is required.
7. Special attention must be given to the Root Certificate Authority, which is issuing the certificates for the National Portal/NCP (Portal to Portal certificates), in order to ensure that this Certification Authority can be trusted and can be accepted as root authority. For this purpose the root Certification Authority must be certified by the "Webtrust programme for Certification Authorities", the standard framework of AICPA/CISA, tScheme, or equivalent.
8. The software on which the system is running should be up to date and include all the necessary security updates.
9. Actors will respect the Security Services Definitions, as defined by the epSOS security workpackage (1).
10. Contracting parties will cooperate in investigating security incidents.
11. Security Audits must approve the fulfilment of the application installation and operation guidelines.
12. The above technical security recommendations will be reviewed each year by the consortium and updates will be made according to the state of the art.

2.6 SECURITY AUDIT

1. Each National epSOS Portal (NCP) must pass through a security audit.
2. 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

respect. Audit will be based on the epSOS security audit policy, described in annex I of this security policy.

2.7 REFERENCES

1. WP3.7 D3.7.2, Security Service, V02.doc, REGLOM, epSOS, 2009
2. epSOS Annex I – “Description of Work”, EMP/S.O.S. LSP-eHealth team, 2008-06-30
3. D2.1 Legal and regulatory constraints on epSOS, WP2.1, epSOS, 2009-01-31
4. The epSOS trusted domain. Consolidation of concepts, WP2.1, epSOS, 2009-06-28
5. WP3.7 Organization & working methodology, REGLOM, epSOS, 2009

2.8 RECOMMENDATIONS

All epSOS actors must respect the provisions of the above security policy.

APPENDIX 1

THE epSOS SECURITY AUDIT POLICY

In compliance with the provisions of the EpSOS Security Policy (SP), an epSOS security audit procedure is implemented. The basic characteristics of the epSOS security audit procedure are outlined below.

1. MAJOR CHARACTERISTICS OF THE epSOS SECURITY AUDIT POLICY

The epSOS security audit policy and procedure has the following major characteristics:

- It is based and covers both the epSOS security policy and the ISO27002 standard requirements.
- The epSOS security audit policy underlines mainly confidentiality and integrity needs more than availability needs.
- The epSOS security audit procedure is conducted by accredited security experts (e.g. by national authorities), using ISO based procedures.

2. BASIC PROVISIONS FOR THE epSOS SECURITY AUDIT PROCEDURE:

The epSOS security audit procedure is based on the following basic provisions:

- An epSOS security audit group made up of experts will be constituted to coordinate the audit procedure and decide if a partner fulfils the epSOS security requirements. The group decision will be based on the epSOS audit results.
- Some of the security measures specified in the epSOS security policy can be defined as critical because they concern either some fundamental items of the EpSOS system and processes, or because of legal requirements.
- A minimum acceptable mark is to be defined by the epSOS security experts for each measure depending on its importance.
- A measure mark under the minimum mark is considered as a non compliance.
- Compliance to critical security measures is required under any circumstances.
- Compliance monitoring procedures will be applied in case of failure. These will include appropriate management procedure or sanctions, requirements for improvements, etc.

- ISO27001 certified lead auditors
- Certified Information System Auditors, or equivalent.

- Audit validity is limited in time. After one year, a new audit must be conducted.
- Security audit must have been completed by all partners before the start of the epSOS pilot services.

3. SCOPE OF THE SECURITY AUDIT POLICY – AREAS COVERED

The epSOS security audit policy and procedure should cover and certify compliance with at least the following items:

- **Security Policy**
 - Existence of an Information security policy
- **Organization of security policy**
 - Structure / organization of the existing information security policy
- **Asset management**
 - Information classification
- **Human resources policy**
 - Employment security
 - Information security awareness, education, and training
 - Management of information security incidents and improvements
- **Physical and environmental security**
 - Secure areas
 - Physical security
- **Communication and operation management**
 - Operational procedures and responsibilities
 - Exchanges with external systems
 - Protection against malicious and mobile code
 - Network security
 - Media handling
 - Exchange of software and information
- **Access control**
 - Business requirements for access control
 - User access management
 - User responsibilities
 - Network access control
 - Operating system access control
 - Application and information access control
 - Recording of security events
 - Mobile computing and teleworking
- **Information system development and maintenance**
 - Security requirements of epSOS information systems
 - Project development security process
 - Cryptographic controls

- maintenance
- **Business continuity management**
 - Backup plan
 - Emergency plan
 - Disaster recovery plan
- **Compliance**
 - Compliance with legal requirements
 - Compliance with security policies and standards, and technical compliance
 - Information systems control and supervisory considerations

The above audit areas cover the requirements of both the epSOS security policy and the ISO27002 (or equivalent) security standard.