




Smart Open Services for European Patients

Open eHealth initiative for a European large scale pilot of
Patient Summary and electronic Prescription

D3.3.3 epSOS

epSOS Interoperability Framework

WORK PACKAGE	WP3.3
DOCUMENT NAME	D3.3.3 Interoperability Framework
SHORT NAME	D3.3.3
DOCUMENT VERSION	2.3 FINAL
DATE	15/04/2010

	D3.3.3 Interoperability Framework	Document Short name:	D.3.3.3
		Version:	2.3
	WP3.3: System architecture	Date:	15/04/2010

COVER AND CONTROL PAGE OF DOCUMENT

Document name:	D3.3.3 Interoperability Framework
Document Short name:	D3.3.3
Distribution level	PUBLIC
Status	D.3.3.3 epSOS interoperability framework FINAL
Author(s): Organization:	Didier Ambroise, Anne-Laure Janeczek, Patrick Ruestchmann, Gil de Béjarry ASIP SANTE

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

D3.3.3 Draft Interoperability Framework is the third and final deliverable of WP3.3 Architecture. Important: this deliverable might be revised after epSOS Pilot operations (WP4.4 and WP4.5). These experimentations may lead to make the choice of some standards that would be better than others.

Change History

Version	Date	Status Changes	From	Details	Review
V0.0	17/11/2009	Draft	ASIP Santé	Draft of Table of Content (TOC)	ASIP
V1.0	30/11/2009	Draft	ASIP Santé	Draft version release for pre-internal review + WP3.8 and WP3.9 WPL.	WP3.8, WP3.9.
V1.1	15/12/2009	Draft	ASIP Santé	Comments from ASIP	-
V2.0	18/01/2010	Final	ASIP Santé	Comments from Quality Reviewers	NHS, ELGA, THESS, FHGISST, GEMATIK
V2.1	20/01/2010	Final	ASIP Santé	Alignment with D.3.7.2	QR Reviewers
V2.2	28/01/2010	Final	ASIP Santé	Final adjustments	-
V2.3	15/04/2010	Final	ASIP Santé	Open Issues integration from TPM Taskforce	-




	D3.3.3 Interoperability Framework	Document Short name:	D.3.3.3
		Version:	2.3
	WP3.3: System architecture	Date:	15/04/2010

Table of contents

1. Introduction to the epSOS Interoperability Framework	5
1.1 Purpose	5
1.2 Definitions	7
1.3 EU Framework relevant to epSOS	7
1.3.1 Directive 1995/46/EC on the protection of personal data	7
1.3.2 Directive 1999/93/EC on a community framework for electronic signatures	10
1.3.3 Directive 2006/123/EC on services in the internal market	11
1.3.4 Directive 2005/36EC on the recognition of professional qualifications	12
1.4 Key Interoperability layers	13
1.5 Context Interoperability Frameworks	16
2. Underlying Principles	18
2.1 Underlying Principle 1: Security and Privacy	18
2.2 Underlying Principle 2: Transparency	18
2.3 Underlying Principle 3: Preservation of Information	19
2.4 Underlying Principle 4: Openness & Reusability	19
2.5 Underlying Principle 5: Technological Neutrality and Adaptability	20
3. epSOS Interoperability framework	21
3.1 Semantic interoperability	21
3.1.1 Data elements	21
3.1.2 Terminology	22
3.1.3 Structure	22
3.1.4 Transformation	23
3.1.5 Metadata	23
3.2 Technical interoperability	24
3.2.1 Transactions	24
3.2.2 Messages	25
3.3 Security interoperability	25

	D3.3.3 Interoperability Framework	Document Short name:	D.3.3.3
		Version:	2.3
	WP3.3: System architecture	Date:	15/04/2010

3.3.1	Web Services Security Standards	27
3.3.2	Secure communication.....	30
3.3.3	Security functionalities provided to epSOS.....	30
4.	Annex	34
4.1	epSOS Standards Catalogue (Semantic domain)	34
4.2	epSOS Standards Catalogue (Technical domain)	37
5.	References	38

	D3.3.3 Interoperability Framework	Document Short name:	D.3.3.3
		Version:	2.3
	WP3.3: System architecture	Date:	15/04/2010


1. Introduction to the epSOS Interoperability Framework

1.1 Purpose

This document is to be considered as a sister document to both D3.3.2 final epSOS System Technical Specification and D3.4.2 final epSOS Common Components Specification. It is not a stand-alone document as references are made to the above-mentioned deliverables that are the core specifications from a technical point of view. It gives, though, a guide to the various standards and protocols that are recommended in order to fulfil cross-border interoperability in epSOS. This document does not repeat architectural requirements that are found in D3.3.2 and D3.4.2 but complete them with underlying principles drawn mostly from the EU legal framework regarding interoperability (see Chapter 2).

Interoperability in the epSOS context: Interoperability is about operating in a heterogeneous environment in which policy priorities, business strategies, administrative procedures, information requirements and technology systems differ between organizations. As such, interoperability is about addressing multiple domains, which is a major issue for the epSOS Project: basically, a Gateway to Gateway exchange of data, which implies same interoperability profiles in each country.

Interoperability Framework for epSOS: As a general issue, such a framework is acting as an enabler for systems working together. It provides the shared vision and rules for instigating coordinated change to support complex, emerging interactions between organisations or individuals (HCP/HCPO). Technical, information and organisational viewpoints differentiate issues relevant to interoperability. Key aspects of these technical components include the use of open standards, a service-oriented approach to system design and the adoption of Internet technologies to ensure access to the latest in technology advances. Those aspects have been considered

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

for describing the common components of the epSOS architecture and proposing a full design (business – information system – technical views). This document provides a catalogue of standards used for epSOS interoperability.


The epSOS Interoperability Framework focuses on the interfaces or “glue” that enables distinct systems to work together: how national interfaces should interact with its epSOS national Gateway and how Gateways relates to each other at a technical level (transactions are described and assembled in D3.4.2 and D3.3.2).

epSOS Interoperability Framework does not seek to address the standards, policies and procedures that affect the information, business process and technical domains within MS. This is due to the context-specific nature of these domains in which agencies operate in different policy portfolios, engage different sets of stakeholders, and often have different information and business requirements.

This framework only applies to the epSOS cross border ePrescription / Patient Summary / eDispense exchange on the top of Web technologies.

Considering the epSOS time frame for implementation of the pilots, the existing experiences in industry and the strong demand for standardised security measures, a decision on the top-level messaging protocol has been made use the *W3C SOAP* protocol¹. Furthermore, major healthcare committees such as IHE and HL7 move in this direction by providing respective guidelines and (re)defining existing actors as web services.

¹ An alternative could be to use the REST (Representational State Transfer) architectural style which mainly relies on HTTP commands and URIs.

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

1.2 Definitions


- § *Interface*: a boundary at which interaction occurs between two systems or processes.
- § *Integration*: combination of diverse application entities into a relationship which functions as a whole.
- § *Interoperability*: a state which exists between two application entities when, with regard to a specific task, one application entity can accept data from the other and perform that task in an appropriate and satisfactory manner without the need for extra operator intervention^I.
- § *Functional and syntactic interoperability*: the ability of two or more systems to exchange information (so that it is human readable by the receiver)
 - *The most relevant articles with regard to*
- § *Semantic interoperability*: the ability for information shared by systems to be understood at the level of formally defined domain concepts (so that the information is computer processable by the receiving system)^{II}.

1.3 EU Framework relevant to epSOS^{III}

1.3.1 Directive 1995/46/EC on the protection of personal data

The Data Protection Directive (95/46/EC, 24 October 1995) was drawn up to address the need for pan-European flow of information and the need to have a minimum level of data protection when such information flows across borders. Hence, both the internal market (article 95 of the EC treaty) and the respect for privacy are core considerations of the Directive.

The Directive provides a set of legal requirements for personal data to be processed throughout private and public services in Europe and has been transposed into national regulation by all Member States.

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

Even though there are differences in the transposition of the Directive in the different Member States, it is likely that the principles laid down in the Directive are respected by all Member States.

The Directive comprises a set of principles/requirements which make data processing lawful. These principles are to a large extent elaborated in Article 6 of the Directive :

“(...) Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;


(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

(...)”

The Data Protection Directive has a direct link on the epSOS project. First of all, most of the data exchanged in patient-HCP interactions are to be considered personal

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

data and hence are covered by the Directive. This means that personal and medical data may only be processed if article 7 of the Directive is met:

“(...) Article 7

Member States shall provide that personal data may be processed only if

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or


(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

(...)”.

Given the conditions of previous article 7, one of the most important ground to make the processing of personal data across state borders legitimate is unambiguous consent of the data subject (the claimant).

This will not be too problematic when data is provided by the claimant directly (e.g., in an online form), or when data can be obtained from a certificate presented by the claimant (for instance, taken from a certificate on a smart card inserted into a reader attached to the device the claimant uses in the interaction). It becomes more

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

complicated when the service provider (relying party) needs to obtain additional data, such as (certified) attributes and these can be, or even have to be obtained, from other sources than the user. In some cases it may, for instance, be possible to collect the data from authentic registers in the claimant home member state.


In this case also consent of the user may be required in order to make the processing legitimate. Also the other requirements of the Data Protection Directive have to be met. The identity of the controller has to be specified, as well as the purposes for the data collection (articles 6 and 10, DPD). Data minimization has to be observed (art. 6) and data should be accurate and up to date. These requirements may be difficult to meet in cases where no direct access is available to reliable data sources (such as authentic registries). Data security will not be different from what is required in relation to the processing to data originating from the claimants in the service providers own member state.

1.3.2 Directive 1999/93/EC on a community framework for electronic signatures

The purpose of this Directive is to:

- § facilitate the use of electronic signatures and to contribute to their legal recognition and;
- § to establish a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market.

An electronic signature means data in electronic form which are attached to or logically associated with other electronic data. It is a technique by which it is possible to secure information in such a way that the originator of the information, as well as the integrity of the information, can be verified. This procedure of guaranteeing the origin and the integrity of the information is also called: authentication.

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

Although the European Directive deals mainly with the use of electronic signatures as a substitute for hand-written signatures produced by natural persons, it can be used in all circumstances where the origin and the integrity of computer data have to be secured.

Liability

Providers of qualified certificates are liable for information contained in the certificate and the accuracy of revocation lists. Article 6 provides for a minimum of Certification Authority (CA) liability but also certain limitations.

With respect to the epSOS LSP this leads to the question whether the certificates employed in different solutions are qualified or not. In Member States that require Qualified Certificates, a certain liability is placed upon the certification-service-provider, which may have arrangements with the MS government regarding damages. In other cases certification-service-provider may be able to waive liability in their terms of service.


1.3.3 Directive 2006/123/EC on services in the internal market

The directive on services in the internal market ('Services Directive') aims to creating a single market for services within the European Union by regulating cross-border services. It is necessary to remove barriers to the free movement of services between Member States and to guarantee recipients and providers the legal certainty necessary for the exercise in practice of the fundamental freedoms of the Treaty.

The most important article with regard to eHealth services is article 8:

Procedures by electronic means

- *Member States shall ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant point of single contact and with the relevant competent authorities.*

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010


- *The Commission shall, in accordance with the procedure referred to in Article 40(2), adopt detailed rules for the implementation of paragraph 1 of this Article with a view to facilitating the interoperability of information systems and use of procedures by electronic means between Member States, taking into account common standards developed at Community level.*

1.3.4 Directive 2005/36EC on the recognition of professional qualifications^{JV}

Directive 2005/36/EC provides for the recognition of professional qualifications in view of establishment in another Member State and in view of facilitating the provision of cross-border services in a Member State other than the one of establishment.

Some initiatives linked to the mobility of health professionals have been taken by professional organizations such as the Health Professionals Crossing Borders initiative and the professional card pilot initiative which both aim at improving access to information where conduct has been brought into question. The progress of these initiatives will need to be kept under review.

Citizens also enjoy rights to access healthcare in other Member States. The proposed Directive for cross-border healthcare aims to ensure application of common principles for cross-border healthcare in the EU. One pillar of the Directive is that of realizing the potential of European cooperation in areas where this is useful, including in border regions, through European reference networks of specialized centers, through EU network for Health technology assessment or through e-health.

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

1.4 Key Interoperability layers

Interoperability is frequently viewed as having three distinct dimensions: organizational, semantic, and technical. The EIF² extends this by adding political and legal dimension, resulting in Political – Legal – Organizational – Semantic – Technical, as shown on figure below.

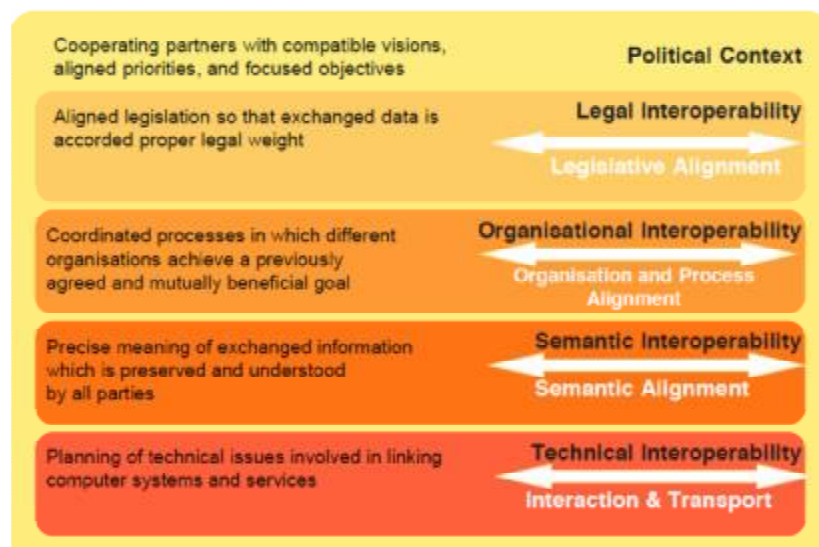



Figure 1: Interoperability levels

- § **Political context** denotes the alignment of missions, policies, and business processes.
- § **Legal interoperability** provides the legislative foundation for interoperability, for example, by providing compatible regulations concerning privacy and access control.
- § **Organizational interoperability** denotes the ability of two or more organizations to interact with each other.
- § **Semantic interoperability** denotes the ability of entities to share information meaningfully and to engage in meaningful collaborative activities in order to perform collaborative business processes.

² European Interoperability Framework for Pan European eGovernment Services

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010


§ **Technical interoperability** denotes the ability of systems to exchange data, perform collaborative processing, synchronize transactions, and coordinate their interactions.

Although these dimensions interact with each other, the mechanisms that are appropriate to fostering interoperability in each dimension are quite different. **Political** interoperability involves the ways that the missions, policies, and business processes of an enterprise interact with those of other enterprises. **Legal** interoperability involves the promotion of consistent legal policies and the possible creation of legislation to enable appropriate interoperation among organizations and enterprises. **Organizational** interoperability is a matter of organizational structure, culture, and procedure, which may be affected by oversight, legislation, reorganization, interagency agreements, etc. **Semantic** interoperability requires that business processes be analyzed and potentially re-engineered to be consistent and compatible, that terminology and ontology be harmonized, that metadata be created, etc. Finally, **technical** interoperability requires that communication and interaction protocols be standardized, that processing and transaction mechanisms be implemented consistently across systems, those wrappers or “adapters” be created to transform data and translate among different eService interfaces, etc.

In the epSOS project, layers of interoperability are:

- § *Political* interoperability layer follows Grand Agreement;
- § *Legal* interoperability layer is contained in WP2.1, notably through the Framework Agreement documents;
- § *Organizational* interoperability is defined within WP3.1, WP3.2, WP3.3, WP3.6³, and WP3.7;

³ The choice of standard for encoding security token is the SAML 2.0 (*Security Assertion Markup Language*). SAML assertions can be integrated within *SOAP security headers* and are compatible with *WS Security* and the *WS** family of specifications. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject to other entities, such as a NCP or a HCP/O. See WP3.6 and WP3.7 deliverables.

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

§ *Semantic & Technical* interoperability layers have their roots defined in WP3.5 (semantic) and WP3.7 (security) and provided by WP3.4 (common components) in the definition of the epSOS Interoperability Profiles Groups aligned with the WP3.3 (architecture) technical blocks.

As a conclusion, it is not the scope of current document to develop political, legal and organizational interoperability. But it is in scope to describe **semantic and technical** interoperability among:

- § **Medical application level** (semantic and syntactic): it addresses exchanged contents: data objects, terminology, structures, transformation and metadata
- § **Exchange level**: it addresses transactions rules and parameters rules
- § **Transport level**: it addresses exchange protocols specifications

Figure below illustrates the scope of epSOS Interoperability framework stated in the current section.

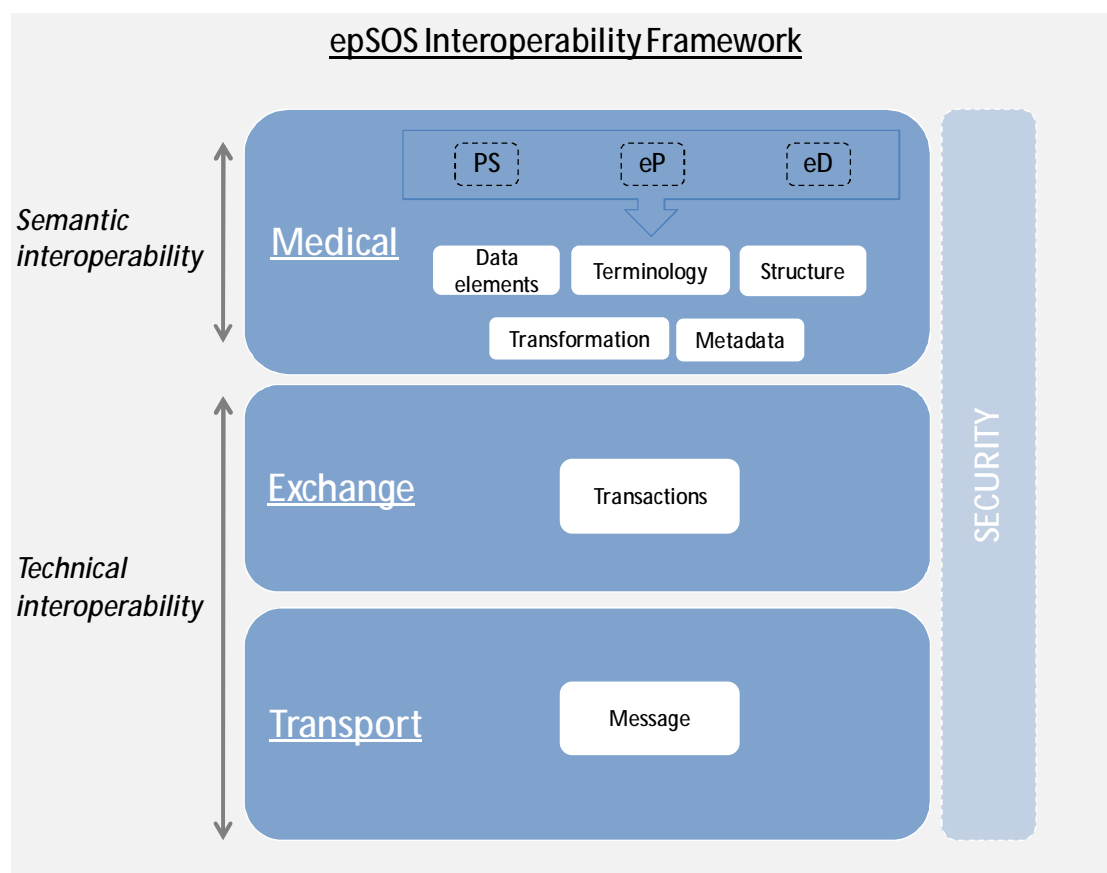



Figure 2 : epSOS interoperability Framework Layers

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

1.5 Context Interoperability Frameworks

Many public administrations already have or are in the process of developing frameworks addressing interoperability issues within their national, regional or local domains. The scope of these frameworks is restricted to the jurisdictions within which they have been developed.

The epSOS Interoperability Framework is to provide support and resources as necessary to enable the consistent and interoperable implementation of epSOS LSP specifications. This document considers that Standards implementation needs to be approached from two angles:

- § Interaction with existing standards organisations – locally and internationally;
- § Interaction with industry including jurisdictions, international equivalents and vendor community;


As a consequence, the relevant bodies implied here are:

Official Standardisation bodies are:

- § ISO: International Standards Organisation,
- § EIC: International Electro-technical Commission,
- § ITU: International Telecommunication Union,
- § UN/CEFACT: United Nations Centre for Trade Facilitation and Electronic Business,
- § ETSI: European Telecommunications Standards Institute.
- § HL7: Health Level Seven.
- § CEN: European Committee for standardization
- § IHTSD : International Health Terminology Standards Development


Main bodies relative to the electronic exchange are:

- § OASIS: Organization for the Advancement of Structured Information Standards,

	D3.3.3 Interoperability Framework	Document Short name:	D.3.3.3
		Version:	2.3
	WP3.3: System architecture	Date:	15/04/2010

- § W3C: World Wide Web Consortium,
- § IETF: Internet Engineering Task Force,
- § ECMA: European Computer Manufacturers Association,
- § OMG: Object Management Group,
- § WS-I: Web Services Interoperability Organization.

In the field of health, the standards supporting initiatives is IHE: Integrating the Healthcare Enterprise,

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

2. Underlying Principles

As a consequence of the above frameworks (Chapter 1) a number of principles^V can be announced in relevance to the process of establishing interoperability in the epSOS context. Those principles acted as constraints when it came to decide the level of interoperability to impose in epSOS.

2.1 Underlying Principle 1: Security and Privacy


Patients and Health care professionals must be assured that they interact with e-health systems in an environment of trust and in full compliance with the relevant regulations, e.g. on privacy and data protection. This means that e-health services must guarantee that the privacy of patients and the confidentiality of information provided by businesses are respected.

This principle is enforced most specially by WP3.6 (identity management) and WP3.7 (security) specifications in regards to the usage of technological standards and protocols, notably with specifications of the Audit trail.

2.2 Underlying Principle 2: Transparency

Within the necessary security constraints, patients and HCPs should have the right to verify the information national and/or European systems have collected about them and to decide whether this information may be used for purposes other than those for which it was originally supplied.

Patients and HCPs should be able to understand administrative and business processes. They should have the right to track procedures that involve them and have insight into the rationale behind decisions that could affect them.

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

2.3 Underlying Principle 3: Preservation of Information

Medical records and information in electronic form held by national and/or European infrastructures for the purpose of documenting procedures and decisions must be preserved. The goal is to ensure that medical records and other forms of information keep their legibility, reliability and integrity over time and can be accessed taking into account security and privacy.

In order to guarantee long-term preservation of all electronic records and information, formats should be selected so as to ensure long-term accessibility, including preservation of associated electronic signatures and other electronic certifications.


For medical information sources owned and managed by national infrastructures, the preservation is a purely national matter. For European e-Health Services like epSOS and for information that is not purely national preservation should become an European issue and the necessary "preservation policy" has to be foreseen, notably towards codes and translations for semantic mapping.

2.4 Underlying Principle 4: Openness & Reusability

Interoperability involves the sharing of information and knowledge between organisations, hence implies a certain degree of openness.

Specifications, software and software development methods that promote collaboration and the results of which can freely be accessed, reused and shared are considered open and lie at one end of the spectrum while non-documented, proprietary specifications, proprietary software and the reluctance or resistance to reuse solutions lie at the other end.

Re-use is key to the efficient development of European e-Health Services. Re-use means that organisations confronted with a specific problem seek to benefit from the work of others by looking at what is available, assessing its usefulness or relevancy

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010


to the problem at hand, and decide to use solutions that have proven their value elsewhere.

Implementations tasks for upcoming work in epSOS (pilots preparation) can enforce this principle by development of common tools (testing and/or software components) based on epSOS interoperability specifications (from WP3.3-4-5-6-7) that can be shared / re-used among the different pilots on a free basis, with no royalties (open source).

2.5 Underlying Principle 5: Technological Neutrality and Adaptability

When establishing European e-Health Services, organisations should focus on functional needs and defer decisions on technology as long as possible in order to avoid imposing specific technologies or products on their partners and to be able to adapt to the rapidly evolving technological environment.

epSOS LSP participants should render access to e-Health services independent of any specific technology or product. This is the purpose of choosing standards and protocols when deciding the interoperability framework.

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

3. epSOS Interoperability framework

3.1 Semantic interoperability

Many integration approaches concentrate on the delivery of connectivity technologies to enable system interoperation. This approach is subject to technology and solution changes as new standards and technologies permeate the market. The semantics of information provide a more concrete proposition on which to base evolutionary, collaborative interactions.

Agreement on shared semantic understanding is the basis for all communication and is informed from an agreed national E- Health Information Domain such as epSOS.


Semantic interoperability implies that data exchanged in a pan-European context needs to be translated to the receivers' own language and individual data structure. Hence, the data exchanged as part of epSOS communication has to be mapped from the originating data format of the sender to the data format of the receiver. Furthermore, the terminology and vocabulary has to be translated from the source to the target language. The data exchange has to be semantics-preserving, i.e. sender and receiver must have a common and ideally identical understanding of the meaning of the data in all languages involved, and any incompleteness and ambiguity have to be adequately addressed.

3.1.1 Data elements

This section addresses standards for basic data elements and types which are the foundation for any information model. International efforts through both ISO TC 215^{VI} and CEN TC/251^{VII} are underway to define these clinical and business elements.

epSOS standards for code system, addressed in D3.5.2, are :

- **UCUM** (Unified Code for Units of Measures) (See chapter 6.2.3)
- **HL7 code system** (See chapter 6.2.7)

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

3.1.2 Terminology

This section presents standards for terminologies, vocabularies, dictionaries, code-sets, catalogues, and classifications allow common clinical understanding.

epSOS **terminology** standards described in D3.5.1, are :

- **EDQM** : Standard Terms of European Directorate of Quality in Medicine (see chapter 6.2.1)
- **LOINC** : Logical Observation Identifiers names and codes (see chapter 6.2.2)
- **ATC** : Anatomical Therapeutic Chemical classification system (see chapter 6.2.4)
- **ICD** : International Statistical Classification of Diseases and Related Health Problems (see chapter 6.2.5)
- **SNOMED CT** : Systematized Nomenclature of Medicine-Clinical Terms (see chapter 6.2.6)


epSOS standards encoding languages for **controlled vocabulary** is Web Ontology Language (OWL).

3.1.3 Structure

Foundation elements and value domains are brought together to form more complex structures including data structures/groups, schemas and archetypes. These mechanisms must enable complex elements to be combined and separated.

Electronic health records exchanged in epSOS are to be consistent with HL7 Clinical Documents Architecture, release 2.0 (CDA R2)⁴. This standard is based on xml syntax. Those xml Medical documents must be valid according to CDA.xds schema. A CDA document is parted in two sections a “header” and a “body”.

⁴ May 2005 edition.

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

Those epSOS syntax standards are exhaustively described in D3.5.2 (Chapter 6.1 Pivot Documents Syntax Standards) and thus not transcribed here.


3.1.4 *Transformation*

Transformation between messages, information elements and terminologies allows different systems to interact through common transformations. Core semantic services standards covering data transformation are based on HL7 Common Terminology Services^{VIII} (**HL7 CTS**). It is an Application Programming Interface (API) specification that is intended to describe the basic functionality that will be needed by HL7 Version 3 software implementations to query and access terminological content. **HL7 CTS 2^{IX}** is intended to ex-pose a single or multiple terminology sources for use by various applications that may or may not be within the same organization, providing a standardized method for terminology access. D3.5.2 (Chapter dedicated to epSOS Semantic Services) presents a complete view of these standards.

3.1.5 *Metadata*

Standards for the classification of information itself are captured through metadata. Standards described in current section enable to make service descriptions accessible to service requesters, service registries for publication of service descriptions by service providers and discovery of services by service requesters are required.

epSOS metadata standard based on web service technology is **Web Service Description Language^X** (WSDL). It allows describing the interface of a Web service on a technical (i.e. functional) level; they describe the operations the service offers to Web service clients along with a description of the format of the messages the service consumes and produces.

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

3.2 Technical interoperability

Organisation of interoperability in epSOS is IHE orientated (i.e. profiles in epSOS are comparable to IHE integration profiles) and covers cross-border data exchange. As a reminder to the reader, the interoperability profiles are organised into 6 groups (grey boxes).

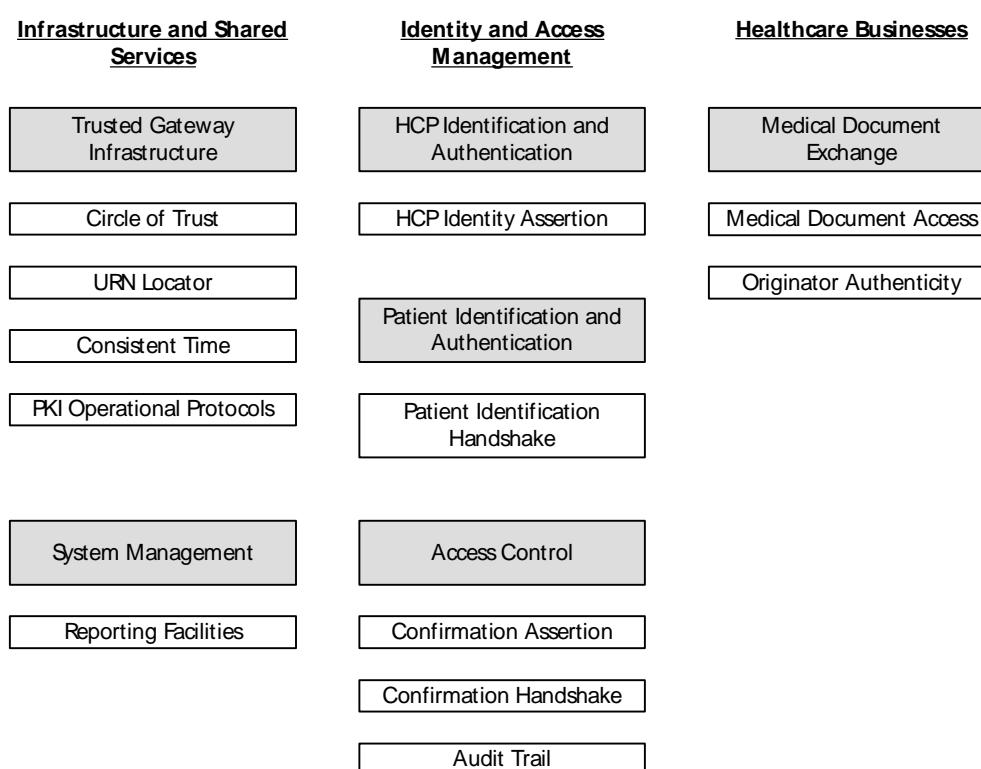



Figure 3: epSOS Profile Groups and Interoperability Profiles (source: D3.4.2)

3.2.1 Transactions

This section addresses service interoperability which end user's perception of the services to be aligned. Common profiles and transaction specified in D3.4.2 are to be used as reference standards for epSOS.

epSOS transactions standards are XDS.b based. Following epSOS transactions are fully defined in D3.4.2.

	D3.3.3 Interoperability Framework	Document Short name:	D.3.3.3
		Version:	2.3
	WP3.3: System architecture	Date:	15/04/2010

- epSOS-1: Establish Mutual Trust
- epSOS-2: Get Resource URL
- epSOS-3: Maintain Time
- epSOS-4: Get Resource
- epSOS-5: Format Audit Trail
- epSOS-6: Provide Identity Assertion
- epSOS-7: Query Medical Data
- epSOS-8: Retrieve Medical Data
- epSOS-9: Notify Medical Data Processing
- epSOS-10: Attest Authenticity
- epSOS-12: Patient ID Discovery
- epSOS-13: Provide Confirmation Assertion
- epSOS-14: Request Confirmation Assertion

3.2.2 Messages


Since the goal of Web service technology^{xi} is to provide an inter-operable platform that facilitates distributed computing based on the messaging paradigm, a standardized messaging platform is an essential requirement.

The foundation for the standards is the SOAP Messaging Framework^{xii} which defines an XML based message format and rules for message processing.

3.3 Security interoperability

The epSOS LSP will be implemented by combining business functions, in this case national existing e-health infrastructures, implemented in different Member States.

Therefore the cross-border service involves allowing external access to national base registers, hence requiring a high degree of security and trust. Even when personal information is exchanged across borders, national data protection legislations apply.

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

The security exchange layer implements and enforces the security requirements for the aggregate service. As data originating from different Member States may have attached to them different data protection requirements, a set of common requirements for data protection should be agreed in order to implement the aggregate service.

This document does not repeat security requirements given in D3.7.2, section II Security Services


Secure data exchange layer

Security is one the most important barriers for interoperability if not applied in a harmonized and agreed way among organizations. This part intends to highlight this fact and draw the attention of all service providers to consider the security issues head-on and to collaborate on a common framework to meet their respective security needs via compatible mechanisms and commonly agreed specifications, as well as to reach common understanding on essential characteristics such as authorization levels and authentication strength.

A key requirement for implementing the functionality expected in the secure data exchange layer involves leveraging the national identification and authentication infrastructures in the Member States into a working cross-border scheme. This scheme should establish which ICT architectures and data are needed in a cross-border context in order to make existing Member States' electronic identity infrastructures interoperable.

Secure communications management

The provision of secure, i.e. signed, certified, encrypted and logged, data exchange also requires several management functions, including:

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

- *Service Management* to ensure oversight of all communication activities relating to identification, authentication, and authorization, data transport, etc., including e.g. access granting, revocation, and audit.
- *Service registry*: given the small numbers of NCPs the LSP will distribute metadata out-of-band. Verification of the trustworthiness of a service is not a responsibility of the service registry.
- *Service Logging* to ensure that logging of all data exchanges for future evidence is adequately performed, including archiving when necessary.

3.3.1 Web Services Security Standards


The Web Service Security family of standards includes different building blocks that can be used to achieve a complete security solution for Web Service communication.

The next sections consider the following standards:

- *WS-Security*, which defines the basic mechanisms for providing secure messaging, i.e. integrity and confidentiality of a single message, and for the exchange of security tokens;
- *WS-Trust*, which provides methods for issuing, renewing, and validating security tokens as well as establishing, detecting, and brokering trust relationships;

3.3.1.1 WS-Security

WS-Security^{xiii} is an OASIS standard specification that describes enhancements to SOAP messaging to provide message integrity and confidentiality and provides a general purpose mechanism for associating “security tokens” with message content. WS-Security is not a complete security solution for Web Services, but rather a basic building block that can be used in conjunction with other Web Service standards and higher-level application-specific protocols to accommodate a wide variety of security models and security technologies.


	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

In the point-to-point situation that is epSOS, confidentiality and data integrity can also be enforced on Web Services through the usage of Transport Layer Security (TLS 1.0). WS-Security however operates at a higher level, on a message basis, thus addresses the wider problem of maintaining integrity and confidentiality of messages even if they have to go through intermediate nodes. WS-Security can therefore provide end-to-end security, whereas TLS can usually provide only point-to-point security.

A core concept in WS-Security is the security token. A security token is a set of one or more claims, i.e. declarations about one entity (e.g. username, capability, role, etc.). A token can be signed by an authority that vouches for its validity; for example an X.509 certificate is a token that claims a binding between an identity and a public key, signed by a certificate authority.

WS-Security specifies an abstract message security model in terms of security tokens combined with digital signatures to protect and authenticate SOAP messages. Security tokens assert claims and can be used to assert the binding between authentication secrets or keys and security identities, whereas signatures are used to verify message origin and integrity. Signatures are also used by message producers to demonstrate knowledge of the key used to confirm the claims in a security token, and thus to bind their identity (and any other claims occurring in the security token) to the messages they create.

WS-Security provides also a means to protect a message by encrypting and/or digitally signing the message body and/or header. Message integrity is provided by XML Signature in conjunction with security tokens to ensure that modifications to messages are detected. Message confidentiality leverages XML Encryption in conjunction with security tokens to keep portions of a SOAP message confidential. WS-Security is focused on single SOAP messages, thus it does not provide mechanisms to establish a security context or any sort of secure "session".

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010


Moreover, it does not address the problem of key exchange and derivation, and does not provide a mechanism to establish a trust relationship between parties.

3.3.1.2 *WS-Trust*

WS-Trust^{XIV} is an OASIS standard that extends WS-Security in order to provide a framework for requesting and issuing security tokens, and to broker trust relationships. WS-Security defines the concept of security tokens and way to use them, but does not address the problem of how these tokens can be obtained. WS-Trust then defines the concept of a security token service, i.e. a Web Service that issues security tokens. Such service makes assertions based on evidence that it trusts, to whoever trusts it (or to specific recipients). A service itself can generate tokens or it can rely on a separate security token service to issue a security token with its own trust statement (this forms the basis of trust brokering). WS-Trust defines also the formats of the messages used to request security tokens and the responses to those messages.

In WS-Trust model a Web Service can require that an incoming message proves a set of claims, using appropriate security tokens. If the requester does not have the necessary token(s) to prove required claims to a service, it can contact appropriate authorities and request the needed tokens with the proper claims. These authorities play the role of security tokens services, and may in turn require their own set of claims for authenticating and authorizing the request for security tokens. The requester then demonstrates authorized use of the token to the Web Service. The Web Service will analyze the token and decide whether it trusts it or not (possibly relying on an external validation service).

WS-Trust is focused on the issuing and validation of security tokens, and does not address the problem of managing a trust policy. Moreover, it does not deal with the problem of using a security token to establish a security context or session.

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

3.3.2 Secure communication

The two mechanisms use to secure communications are SSL and IPsec. IPsec and SSL are security provided by networking protocols.

3.3.2.1 Regarding SSL

SSL is usually implemented by configuring the web service in Internet Information Services (IIS). A certificate, with the subject name matching the web site, is passed to the client. The client then generates a symmetric key, which is sent back to the web server, encrypted with the public key from the certificate. Only the web server, with its private key matching the public key of the certificate, can decrypt this symmetric key. The symmetric key is then used for secure communications during the request.


3.3.2.2 Regarding IPsec

IPsec uses the Diffie-Hellman key exchange algorithm. Each of the two servers communicating passes key material to contribute to the secure creation of a symmetric key. This key is then used to encrypt specific types of traffic passing between the two servers. Security Associations are created on each server – if there are matching Security Associations on each server, then security is applied.

3.3.3 Security functionalities provided to epSOS.

3.3.3.1 Integrity

If it's necessary to ensure that data has not been tampered with during transit, then cryptography is used to provide integrity. IPsec, SSL and WS-Security all provide this. IPsec uses Authentication Headers (AH) mode, which adds a hash of the data to the packet. SSL securely generates and shares a symmetric key when negotiating the connection and so no other party can decrypt what is being sent. This means it

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

cannot be altered without the receiving party being aware. WS-Security can be used to digitally sign either a part or the whole of a message.

3.3.3.2 Confidentiality

IPSec uses Encapsulating Security Payloads to encrypt all data sent with the symmetric key generated during the Diffie Hellman exchange. SSL, as stated before, securely passes a symmetric key between client and server for every request. This means that each request is encrypted with a unique key. WS-Security can encrypt the entire contents of the <body> or <header> elements, or both. It is also able to encrypt only part of the message.


There are an increasing number of networks using Intrusion Detection Systems . These systems monitor the type, source and destination of packets moving across the network, inspecting their contents.

WS-Security gives the benefit of allowing small parts of the data (name, patientID) to be encrypted, leaving the rest of the communication in the clear. This would leave the Intrusion Detection Systems able to perform its functionality while still giving the necessary level of confidentiality.

3.3.3.3 Non-Repudiation

Non-repudiation means that someone cannot deny having done something (see D3.7.2). In this case, if a message has been sent by one party to another (across a network), it may be necessary to hold the originating party to what they have communicated. This is the case for epSOS transactions (eP, PS).

Digital signatures not only provide integrity, they can provide non-repudiation when PKI certificates are used. Neither SSL nor IPSec offer this service. However, WS-Security does, allowing you to sign all or just a part of a SOAP message.

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

The implementation of digital signature will be configured via web service policy (see D3.7.2).


3.3.3.4 *Authentication*

IPSec functions at the network layer of the TCP/IP stack, and so it only authenticates hosts, rather than users. When SSL is used with a web server, credentials can be passed, allowing users to be identified. Credentials can also be passed via WS-Security, authenticating users. IPSec authenticates computers using certificates or shared password. SSL have a richer authentication mechanism username/password, certificates, digest. WS-Security has all of the authentication mechanisms available to SSL, but the authentication model is pluggable. Custom providers can be written to handle checking of passwords, for instance. WS-Security and custom providers add this type of flexibility to web services.


3.3.3.5 *Overview of the security functionality*

The table below gives an overview of the security functionality provided by each of IPSec, SSL and WS-Security.

	IPSec	SSL	WS-Security
Integrity	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes – allows fine grain encryption
Non-Repudiation	No	No	Yes – fine grain addition of digital signatures to document
Authentication	Yes	Yes	Yes – Custom schema

	D3.3.3 Interoperability Framework	Document Short name:	D.3.3.3
		Version:	2.3
	WP3.3: System architecture	Date:	15/04/2010

WS-Security, although it is quite verbose, offers non-repudiation and a customizable security database, which the other two technologies do not. It also allows fine-grain security to be applied to individual sections of the SOAP document.


	D3.3.3 Interoperability Framework	Document Short name:	D.3.3.3
		Version:	2.3
	WP3.3: System architecture	Date:	15/04/2010

4. Annex


4.1 epSOS Standards Catalogue (Semantic domain)

Current Standard catalogue is a consolidated view of references made in D3.3.2, D3.4.2, D3.5.2, D3.6.2, D3.7.2. Correspondence with epSOS Profiles and transaction from WP3.4 are made in columns six and seven. Those references apply mostly on technical domain.


Nr.	Name & version	Overview	Custodian	Reference
1	ISO TC 215	International Standards Organisation (ISO) Health Informatics Technical Committee (TC) 215	ISO	http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=4720
2	CEN TC/251	European Standardization of Health Informatics	European Union	http://www.cenitc251.org/
3	UCUM	Unified Code for Units of Measures is a system code for unambiguously representing measurements units to both humans and machines	Regenstrief Institute, Inc	http://www.regenstrief.org/medinformatics/ucum
5	HL7 Version 3 Standards : transport specification - web services profile release 2	Application Protocol for Electronic Data Exchange in Healthcare Environments	ANSI	http://www.hl7.org/implement/standards/ansiapproved.cfm , http://www.hl7.org/implement/standards/index.cfm
6	HL7 Common Terminology Services 2 Service Functional Model (SFM) 19.02.2009	The SFM provides a Service Interface specification. It is the methodology followed to define HSSP specifications	ANSI	http://informatics.mayo.edu/LexGrid/downloads/CTS/cts2/HL7_Common_Terminology_Services_2_Service_Functional_Model_(SFM).htm
7	Lexicon Query Service version 1.0	Specify a set of common, read-only methods for accessing the content of medical terminology systems	ANSI	http://www.omg.org/technology/documents/formal/lexicon_query_service.htm

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

8	SNOMED_CT Technical Implementation Guide Chapter 6 "Terminology Services Guide" 31.01.2009	Systematized Nomenclature of Medicine-Clinical Terms. SNOMED CT is a comprehensive terminology, created to cover the whole patient record and medical documentation	IHTSDO – International Health Terminology Standards Development Organization, a non-for-profit association based in Denmark.	http://www.ihtsdo.org/fileadmin/user_upload/Docs_01/SNOMED_CT_Publications/SNOMED_CT_Technical_Implementation_Guide_20090131.pdf
9	EDQM standards	Standard Terms of European Directorate of Quality in Medicine The List of Standard Terms covers dosage forms, routes of administration and containers used for medicines for human and veterinary use	EDQM	http://www.edqm.eu/en/Homepage-628.html
10	LOINC	Logical Observation Identifiers names and codes. The scope of the LOINC effort includes laboratory and other clinical observations	Regenstrief Institute, Indiana	http://loinc.org/
11	ATC	Anatomical Therapeutic Chemical (ATC) classification system In the ATC-classification pharmacological substances are divided into different groups according to the organ or organ system which they affect and their chemical, pharmacological and therapeutic properties	WHO Collaborating Centre for Drug Statistics Methodology - Norwegian Institute of Public Health	http://www.who.int/classifications/atcddd/en/


	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

12	ICD	International Statistical Classification of Diseases and Related Health Problems. The ICD is the international standard diagnostic classification of diseases (signs, symptoms, conditions) for all general epidemiological, health management and statistics (death) and clinical use (health records).	WHO	http://www.who.int/classifications/icd/en/
13	OWL	Web Ontology Language. OWL is a family of knowledge representation languages for authoring ontologies endorsed by the World Wide Web Consortium.	W3C	http://www.w3.org/2004/OWL/
14	CDA	CDA is an architecture that defines structure and semantics of medical documents for the purpose of exchange	HL7	http://www.hl7.org/implement/standards/cda.cfm
15	XML Schema	Description language for XML document	W3C	http://www.w3.org/XML/Schema
16	XSL version 1.0	eXtensible Stylesheet Language - A family of recommendations for describing stylesheets for XML document transformation and presentation.	W3C	http://www.w3.org/Style/XSL/
17	XSL version 1.0	XSL Transformations - a language for transforming XML documents into other XML documents.	W3C	http://www.w3.org/Style/XSL/

	D3.3.3 Interoperability Framework	Document Short name: D.3.3.3
		Version: 2.3
	WP3.3: System architecture	Date: 15/04/2010

1 4.2 epSOS Standards Catalogue (Technical domain)

Nr.	Name & version	Overview	Custodian	Reference
1	SAML v2.0	Security Assertions Markup Language (SAML) is an XML-based framework for Web services that enables the exchange of authentication and authorization information	OASIS	http://saml.xml.org/saml-specifications
2	TLS 1.0	Transport Layer Security.	IETF	http://www.ietf.org/rfc/rfc2246.txt
3	TLS 1.1	Transport Layer Security.	IETF	http://www.ietf.org/rfc/rfc2246.txt
4	TLS 1.2	Transport Layer Security.	IETF	http://www.ietf.org/rfc/rfc2246.txt
5	IHE - XDS.b	Cross Document Sharing standard	IHE	http://www.ihe.net/TechnicalFramework/index.cfm
6	IHE - XDM	Cross Enterprise Media Interchange Standard	IHE	http://www.ihe.net/TechnicalFramework/index.cfm
7	SOAP version 1.1	Simple Object Access Protocol - A lightweight, XML-based messaging protocol that is the encoding standard for web services messages.	W3C	http://www.w3.org/TR/soap/
8	WS-Security (WSS)	Ensures security of messages transmitted between web services component	OASIS	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
9	WS-Trust v1.3 March 2007	Provide a framework for requesting and issuing security tokens and broke relationship	OASIS	http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html
10	Web Services Business Process Execution Language v2.0	Define business process that interact with external entities through Web services operations defined using WSDL.	OASIS	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel
11	WSDL 1.1	Web Services Description Language - an XML-based language used to describe Web services.	W3C	http://www.w3.org/2002/ws/desc/
12	XSPA Cross-Enterprise Security and Privacy Authorization	Specify healthcare profiles of existing OASIS standards to support reliable, auditable methods of confirming personal identity, official authorization status, and role attributes	OASIS	www.oasis-open.org/committees/xspa/
13	IPSec Security Architecture for the Internet Protocol	IPsec is a protocol which sits on top of the Internet Protocol (IP) layer. It allows two or more hosts to communicate in a secure manner	IETF	http://www.ietf.org/old/2009/ids.by.wg/ipsec.html

	D3.3.3 Interoperability Framework	Document Short name:	D.3.3.3
		Version:	2.3
	WP3.3: System architecture	Date:	15/04/2010

3

4 5. References

^I CEN Report CR 14300:1999 "Interoperability of health care multimedia report systems", and CEN/TC 251 "Short Strategic Study: Health Information Infrastructure", 2000

^{II} Report from the CEN/ISSS eHealth Standardization Focus Group "Current and future standardization issues in the e-Health domain: Achieving interoperability", draft August 2004

^{III} STORK "D2.2 – Report on Legal Interoperability", Final version, February 2009

^{IV} http://www.hprocard.eu/images/stories/memo_hpro_card_en_nov_08.pdf

^V European Interoperability Framework for European Public Services (EIF) Version 2.0, draft October 2009

^{VI} International Standards Organisation (ISO) Health Informatics Technical Committee (TC) 215, <http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=4720>,

^{VII} European Standardization of Health Informatics, <http://www.centc251.org/>

^{VIII} HL7 Common Terminology Services 2 Service Functional Model (SFM)". 19.02.2009

^{IX} HL7 Common Terminology Services" from November 2005

^X R. Chinnici, M. Gudgin, J. J Moreau, J. Schlimmer, and S. Weerawarana. Web Services Description Language (WSDL) Version 2.0

^{XI} S. Weerawarana, F. Curbera, F. Leymann, T. Storey, and D. F. Ferguson. Web Services Platform Architecture: SOAP, WSDL, WS-Policy, WS-Addressing, WS-BPEL, WS-Reliable Messaging and More. Prentice Hall PTR Upper Saddle River, NJ, USA, 2005

^{XII} M. Gudgin, M. Hadley, and J. J. Moreau. SOAP Version 1.2 Part 1: Messaging Framework. W3C Recommendation 27 April 2007

^{XIII} Web Services Security: SOAP Message Security 1.1 http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

^{XIV} WS-Trust 1.3. OASIS Standard, Mar 2007 <http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf>