eHealth Governance Initiative:

Joint Action JA-EHGov & Thematic Network SEHGovIA

DELIVERABLE

D4.1.a. LPPD Contribution to the eU Roadmap: Towards a European eID Governance for eHealth

WP 4. Legal, Privacy and Protection of Data

Version:	Final
Date:	**20.12 2011**

Project co-funded by the European Commission within the ICT Policy Support Programme and the Health Framework Programme

COVER PAGE	
Project Acronym	**SEHGovIA**
Grant Agreement number	
Status*	**Final**
Dissemination level**	**PU**
Author(s) & Organization(s)	**Zoi Kolitsi, AUTH** **In co-operation with LPPD core group**
Contact	**kolitsi@vivodinet.gr**

* Status: Draft / In Progress / Final

** Dissemination level: PU = Public or
CO = Confidential, only for members of the consortium and the Commission Services

ABSTRACT

The aim of the document has been to provide input for the drafting of the eHGI Roadmap with a focus on the eID priority. It consolidates information from both the debriefing of this workshop and particularly its session focusing on legal and policy matters as well as an extensive desktop research. In its current form, it represents the result of a number of consultations within the LPPD core group by the end of 2011, when it was delivered to the Roadmap core group for further processing in Deliverable D2.1.

The document starts by proposing the scope of the work of the eHGI based on Article 14 of Directive 2011/24 EU and continues with a record of the main policy and legal background relevant to the topic of eID in general and for eHealth specifically. Of these emerge a number of agreed principles which should delimit the further elaboration with the eHGI group. The exercise is perceived as one of contextualising these in the eHealth domain. A number of legal issues are then identified for further consideration.

Change History					
Version	**Date**	**Status**	**Author**	**Details**	**Review**
01	25-11-2011	darft	Zoi Kolitsi	Following discusison in Tcon	Core group
02	29-11-2011	darft	Zoi Kolitsi	Following written comments	Core group
03	03-12-2011	darft	Zoi Kolitsi	Following discusison in Tcon	Core group
04	05-12-2011	draft	Zoi Kolitsi	Following written comments	Core group
05	19-12-2011	Final draft	Zoi Kolitsi	Following written comments	Core group
1	15-05-2012	Final	Zoi Kolitsi	Transferred to deliverable template	

ABBREVIATIONS

eHGI	eHealth Governance Initiative
eID	electronic Identification
eIDM	electronic Identification Management
ENISA	European Network and Information Security Agency
epSOS	European Patients Smart Open Services
EU	European Union
KA	Key Action
PRD	Patient Rights Directive
STORK	Secure Identity Across Borders Linked
WP29	Article 29 Working Party

LIST OF REFERENCES

Name of Author	Reverence / Source
Sources are cited in the text in footnotes	

TABLE OF CONTENTS

1. Scope of eID discussion within the eHGI

It should be understood that the scope of the work undertaken within the eHGI should be sufficient to support the implementation of the Directive 2011/24/EU , i.e. patient mobility.

The mandate and the legal basis for the work on eID within the eHGI is Directive 2011/24/EU. The specific reference to eID is made in Article 14 para2. Lit (c) according to which [one of the objectives of the voluntary network is to] *support Member States in developing* ***common identification and authentication measures*** *to facilitate transferability of data in cross-border healthcare*. However the objective of the voluntary Network is much broader [Article 14, para 2 lit (a)] ***"****work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to* ***achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality".*** It should be however noted that article 14 is non-mandatory and the eID in the Directive is voluntary and not subject to the 2013 transposition requirement.

As a first step towards defining the scope for the work LPPD WP recommends that eHGI works on defining one or more use cases. The following use cases may be considered for inclusion/exclusion

(a) a typical patient mobility use case: A patient receives care in a MS other than the MS of affiliation which requires access from abroad to his/her health data and sending a care reimbursement request to the country of afiliation.
(b) A typical professional and service mobility use case: Cross-border interoperability of eID in support of the mobility of health professionals and of health services

2. Background and Existing EU Policy

2.1 The cross Boarder Directive and the Digital Agenda

The Directive 2011/24/EU incorporates the relevant provisions of the Digital Agenda for seamless cross-border services, interoperability, mobility, better administrative cooperation, **mutual recognition and acceptance of e-Identification/Authentication and in** particular, Key Action 16: Propose a Council and Parliament Decision requesting Member States to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' by 2012. Additional KA to facilitate the adoption of an EU eIDM Framework include

> Key Action 6: Propose a Regulation to modernise the European Network and Information Security Agency (ENISA) and make proposals to set up certification for EU institutions by 2010
>
> Key Action 4: As part of the modernisation of the EU personal data protection regulatory framework, explore the extension of security breach notification provisions by 2010

Key Action 7**:** Propose rules on jurisdiction in cyberspace at European and international levels by 2013

Pilar I of the Digital Agenda on Digital Single Market aims to deliver future stability and growth, boost employment and get more out of single market enhancing policies and foresees **fast track** actions on a common legal base for mutual recognition/acceptance of e-identification, authentication and signature.

2.2 eGov Initiatives

Historically, MS commitment to establish a common EU framework for eID started with the Manchester Ministerial Conference Declaration 2005 for widely available, trusted access to public services across the EU, through mutually recognised electronic identifications. Member States agreed to strive for interoperability between the means of identification which were issued or relied on at the national level, with the goal of improving the efficiency and security of e-government services. This goal was to be achieved by relying on recognised international standards and on stable technologies, to be taken up and tested through pilots and the sharing of best practices.

The i2010 e government Action Plan: "Accelerating eGovernment in Europe for the Benefit of All **"** focused on user empowerment, Internal Market, efficiency/ effectiveness, provide pre-conditions and key enablers including the **Revision of e-Signature Directive, mutual recognition of e- identification/ Authentication** to be concluded by 2011?.

The eGov action plan foresees also the provision to agree with Member States on a roadmap setting measurable objectives and milestones on the way to a ***European eIDM framework*** by 2010 based on interoperability and ***mutual recognition of national eIDM***.

The **Signposts towards eGovernment 2010 Paper** [1] forsees that by 2010 "all European citizens, businesses and administrations shall benefit from secure means of electronic identification (eID) that maximise user-convenience while respecting data protection regulations. Such means shall be made available under the responsibility of Member States but be recognised across the EU".

The Paper also made several proposals to mitigate the inherent interoperability risks by 2010. Central among these is the need to adopt a model that **is both federated** (under the responsibility of each Member State in order to respect the autonomy of different administrations) **and multi-level** (to allow different levels of authentication that might be needed to face differing security and authentication requirements).

2.3 The EU eID Road Map

Foreseen as a priority of the eGov action plan, the eiD Road map [2]proposed action and measurable milestones towards a **common EU eID Management Framewor**k by 2010. However, in order to realise the vision on a pan-European eIDM system as expressed in the Ministerial Declaration and the Signpost Paper, minimal requirements to put in

[1] http://ec.europa.eu/information_society/activities/egovernment/docs/minconf2005/signposts2005.pdf

[2] http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

practice an eIDM infrastructure need to be agreed and followed by all parties involved. The following paragraphs are extracted directly from the EU eID Roadmap, as they set also a framework of principles that should also guide the discussion in the eHGI.

For this reason, the following principles should as a minimum be adhered to by the Member States, in order to come to an efficient and interoperable pan-European eIDM infrastructure:

1. Usability considerations should be the most pervasive design constraint when creating a pan-European eIDM framework. This means that the system must be secure, implement the necessary safeguards to protect the user's privacy, and allow its usage to be aligned with local interest and sensitivities.

2. Each Member State should be able to identify users within its borders, if it wishes to allow them access to eIDM services abroad. To this end, the consistent use of suitable identifiers is a necessity to allow the accurate identification and authentication of the entity involved, and to allow the exchange of information between administrations insofar as required for these purposes. The fundamental requirements for a system that addresses the needs of natural persons should be extensible to legal persons as well.

3. Each Member State should issue the means to each user to identify and authenticate himself electronically, if it wishes to allow him access to benefit from eIDM services abroad. A user has the ability to act autonomously and to make use of the offered services.

4. With regard to mandate/representation authorisations, each Member State should provide the means to manage the competences of the identified users within its borders, insofar as these authorisations are not subject to approval by or on the authority of another Member State.

5. Each Member State should support online validation mechanisms of identities, competences and mandates, if it wishes to provide eIDM services.

6. High-level consensus must be established between Member States on an eIDM terminology in order to guarantee conceptual/semantic interoperability. Appropriate policy and legal measures can be used to corroborate this consensus.

From these basic principles, a number of design criteria for a pan-European eIDM system can be derived, which were also included in the Signpost Paper. Most notably, in order to achieve eIDM interoperability, the pan-European eIDM system would need to be:

a. federated, in a policy sense, i.e. allowing administrations to mutually trust each other's identification and authentication methods, accepting these methods on the basis that they were considered acceptable by the administration of origin.

b. multilevel, in the sense that Member States should be permitted to provide multiple security levels for eIDM services, so that the authentication requirements for each eGovernment service can be tailored to the security needs of that service. Member States determine at which level they choose to offer authentication services, and which level of authentication is required for each eGovernment service (although they must accept as valid any authentication methods of the required level from other Member States). This implies that a set of criteria must be defined on a European level which must be met for each authentication level.

c. Relying on authentic sources: to ensure data quality and eGovernment efficiency, a single authentic source should be available for each piece of data regarding each registered entity in the Member State of origin. This does not necessarily imply the use of databases, as the

authentic source might be a unique token. Additionally, commonalities in the eIDM approach among Member States can be encouraged to provide assurance on the quality of source eIDM data.

d. Permitting a context/sector based approach where this is deemed desirable by the Member State of origin (i.e. this is a logical extension of the federated model). Such context can be determined by the application framework or the conceptual framework within which eIDM is used.

e. Enabling private sector uptake, where Member States choose to rely on private sector partners (e.g. financial institutions) for the provision of eIDM services.

2.4 STORK

The STORK project (www.eid-stork.eu) is a 20 million euro project co-financed by the Competitiveness and Innovation Programme (CIP) of the European Commission and 14 Member States.

The objective of STORK is "to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID". This project is also in its second year and has a planning similar to epSOS.

To work out towards this objective, STORK will develop several pilot services, including a pilot for a "Cross border authentication platform - for electronic services", another one to support student mobility "to help people who want to study in different Member States" and another one on electronic delivery "to develop cross-border mechanisms for secure online delivery of documents". One can also add that STORK is currently working with epSOS to seek solutions for solving epSOS's identification management questions appearing when a patient is in need of care in another Member State.

The project has also started in 2008 and has been extended and enlarged. It has delivered most of the necessary functional and technical specifications and is currently preparing their use in specific applications, i.e. the above-mentioned pilots.

From this, one can understand that STORK may propose technologies and a legal framework to all those projects which have to address cross-border electronic identification and authentication of individuals. Some elements of STORK could therefore help making personal identification data electronically available with the necessary security and privacy constraints being taken care of. Hence, this could be of value to EESSI as well as to eEHIC, when phase 3 of the eEHIC roadmap will be launched.

2.5 Connecting Europe Facility

A proposal of the European Commission to the council and the European Parliament: 50 billion worth of investment to improve European transport, energy and digital networks, 9,2 billion for Connecting Europe ICT (broadband – 8 billions - and digital service infrastructures - 1.2 billions), **ensure cross-border delivery of eGovernment services**: **eHealth, eID for secure transactions**, setting up a business across Europe.

2.6 Public Authorities Initiative – the Porvoo Group

Public Authorities have taken initiative towards transnational interoperable eID. The **Porvoo group** has a goal to achieve this based on PKI technology (Public Key Infrastructure) and smart cards and chip ID cards, in order to help ensure secure public and private sector e-transactions in Europe. The Group also promotes the introduction of interoperable certificates and technical specifications, the mutual, cross-border acceptance of identification and authentication mechanisms, as well as cross-border, online access to administrative services. The Thomas Myhr´s report[3] on a legal study sponsored by the group concluded that despite the fact that the Directive on Electronic Signatures covers also entity authentication, **there is a need for a legal framework for entity authentication and pan European eID** . The possibility to use regulation for passports as one building block for legal framework for pan European eID could be considered.

An issue that would merit discussion is whether pan European eIDs on different security levels be accepted.

2.7 epSOS

epSOS has concluded a first phase of development and has made the start of the pilots possible. A first set of recommendations has been forwarded to the eHGI. epSOS has also performed an analysis of Directive 2011/24/EU and has identified a number of legal issues that need to be addressed. Those relevant to eID are summarized in the table below.

Legal Reference	**Open Issue**	**When**
Art. 10 para. 2 and 3 as well as Art. 14 PRD epSOS Recommendation	**International Agreements?** The legal framework of the PRD creates conditions for sustainable international (interoperability) legal agreements for sustainability of epSOS services. Acc. to Art. 14 PRD Member States shall facilitate cooperation in cross-border healthcare provision at regional and local level as well as through ICT and other forms of cross-border cooperation. The European Commission shall encourage Member States, particularly neighbouring countries, to conclude agreements among themselves. The Commission shall also encourage the Member States to cooperate in cross-border healthcare provision in border regions. The epSOS Consortium, developed a Framework	**2013**

[3] www.fineid.fi.

	Agreement (FWA) to address the organisational and legal issues around the health system. This should not be a project-specific matter, however, and we believe the eHGI should progress, with the Commission, a robust legal basis to support cross-border healthcare in Europe. This would need to include aspects such as recognition and reimbursement of e-prescriptions.	
Art. 1 para. 2 and Art. 17 DPD Art. 14 PRD	The Member States – through the voluntary Network acc. to Art. 14 PRD – shall work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare. From a European perspective, security requirements vary considerably in Member States. However, different levels of security in national legislations must not impose an obstacle to intra-EU exchange of data (Art. 1 para. 2 DPD). Such requirements might be found in international standards or national laws. What should be then pursued is the specification of a realistic appropriate security level, which can be gradually enhanced, that will allow MS to implement basic cross-border services and continue to optimize, align and gradually improve them. Furthermore article 1 DPD requires that appropriate technical and organisational measures are taken to protect data.	
Art. 14 PRD para 2, lit.c Incorporating Key Action 16 of the Digital Agenda epSOS Recommendation	**eID and Authentication Measures** KA 16/DA foresees that a Council and Parliament Decision requesting Member States to ensure mutual recognition of e-identification and eauthentication across the EU based on online 'authentication services' by 2012. Art. 14 PRD for the voluntary network shall support Member States in developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare. epSOS has recommended that an interoperable, eGovernment-wide approach for electronic, real time, checking of identity, right to practice and	**2012** **2013**

	access is needed to improve trust and acceptability of cross border eHealth and would welcome the leadership of eHGI in co-ordinating progress in this area.	
Directive 2005/36/EC on recognition of professional qualifications (PQD) Art. 10 para. 4 PRD epSOS Recommendation	**Authorisation** Member States of treatment shall ensure that information on the right to practise of health professionals listed in national or local registers established on their territory is, upon request, made available to the authorities of other Member States for the purpose of cross-border healthcare. The exchange of information shall take place via the Internal Market Information system established pursuant to Commission Decision 2008/49/EC of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data, See also epSOS Recommendation above adn patient consent in emergency situations below.	**2013**
DPD art7 (a) and Art 8 2 (a)	**Patient Consent** Purpose and manner of the data processing need to be covered by the patient's consent. The two step approach of epSOS – i.e. full, general information at the time of participation (epSOS Privacy Information Notice & Terms and Conditions) plus individual information at the time of access (either by the epSOS healthcare provider or for example a message box with regard to this use case) have been well accepted in epSOS. In Emergency situations patient consent (specific) cannot be acquired. In such cases it is imperative to secure the health professional role of the individual requesting access to person data from abroad.	**2011 in piloting**
DPD	**Traceability** All transactions shall be logged and an audit trail created and stored for audit and litigation purposes. Retention periods for logs must be agreed. Art 10 DPD also requires the identification of the data processor and data controller?	**2011 in piloting**

2.8 Identification in the Social Security sector[4]

The Patient Rights Directive 2011/24/EU adds additional clarity as to the right of reimbursement for care received abroad. Co-ordination of social security rights are regulated in Europe by Regulation 883/2004 of 2004 and 987/2009.

A person insured in one Member State when in need of care during his/her journey in another Member State, is entitled to social protection, i.e. to get the care at the same financial condition as a person insured locally. The local institution covers the costs of the care and ask reimbursement to the institution where the person is insured. The health care provider needs to

- ☐ Collect the EHIC data set and verify its validity
- ☐ Verify the identity of the person
- ☐ Request payment for the care to the local institution

Therefore the communication for reimbursement purposes with the payers will always be at national level while the internal communication will be between health insurance organisations. However, a health care provider is required to verify entitlement which is not always straight forward. For this part of the process, communication involving the health care provider at the EU level may be also necessary.

The EU level communication between insurance institutions is facilitated by EESSI , linking national networks for social security estimated to link 15000 institutions connected through National Access points (67 to 150) and exchanging 10 million messages per year. It's full operation is estimated to be in mid 2014. Provisions for privacy may be found in Article 78 of Regulation 883/2004 on "Data processing".

Article 4(2) of Reg. 987/2009 foresees that the transmission of data between the institutions or the liaison bodies shall be carried out by electronic means either directly or indirectly through the access points under a common secure framework that can guarantee the confidentiality and protection of exchanges of data."

In the present-day system, identification of a patient for reimbursement purposes is based on a Patient Identity Number together with a name and surname printed on an EHIC. There is no technical (electronic) authentication process involved in this procedure. The health care provider should simply verify these data against an official patient's ID document containing the photo (passport, driver's license etc.), but adherence to this process cannot be verified.

The electonification of the EHIC aims at better integration of the EHIC handling into the computerised administrative processes at the point of care and within the social security institutions.

Improvement in the identification process of an insured person will also benefit the social security institutions the health care providers. A common approach with other eGov domains and with eHealth can be a key success factor from an economic viewpoint as well as improve user acceptance and accelerate deployment.

---

[4] including input from epSOS D1.4.3.

Authentication for the purposes of verifying eligibility of the reimbursement claims by health insurance institutions should:

- ensure that the patient is the actual EHIC holder and that the EHIC is not shared fraudulently, or stolen and used by another person.
- ensure that the claims correspond to health services offered to the insured individual i.e., make sure that no reimbursement request are made fraudulently for services that were not actually provided.
- Provide for remote access to the patient's entitlement status. In some countries, personal protection regulations require patient's consent for such an access. In these cases, the authorization of the health care provider is needed and may require a sort of patient's authentication first.

These requirements could be fulfilled by the use of electronic cards carried by patients, but the price of such a system (with card readers infrastructure), that would have to be implemented in all EU countries, was deemed to be too high. On the other hand, sticking to the present solution, where the reimbursement procedure relies on an assumption that a paper copy of the patient's EHIC is a proof of his/her presence at the HCP and a proof of entitlement validity seems to be already not satisfying. Depending on the internal regulations, experiences, and priorities in implementation of e-Administration systems, some member states express their interest in looking for more convenient solutions for the cross border reimbursement.

The health insurance organizations estimate that the first two problems, related to the fraudulent behaviour, are not crucial now (from the financial point of view), and their solution has probably to wait for the mass implementation of a person authentication tool (e.g. eID cards, SMS confirmation, other tokens or new concepts). Until then, responsibility for patient's authentication may be left on the HCPs. In many countries there is now a new additional tool for verification of the treatment provision – patients' internet access to the list of all medical services delivered to them. If they discover the reported treatment that didn't take place, a checking procedure can be initiated.

Therefore, at present, the issue of the patient's authentication in the EESSI system could be considered mainly in the context of entitlement verification in an on-line (real time) solution. This is also the only way to re-use the identification process in eHealth services (e.g. those resulting from the epSOS scope).

***Thus, to make the future systems at health care providers consistent, it is necessary to establish cooperation on this issue between all regulatory bodies dealing with electronic exchange of information in healthcare field on EU level (DG EMPL, DG SANCO, DG INFSO*).**

In the long term, this should lead to the creation of the common standards in the identification process of the patients or in a broader sense – EU citizens. One of the possible outcomes of this cooperation could be the CWA based standard for the electronic cards. However we must avoid focusing on a card-centric approach and examples such as the STORK approach offering flexible solutions of the identification process ***with different possible authentication and authorization levels for different applications' needs. Each county may adjust requirements towards the requests sent through STORK in accordance with the national regulations [and common EU level agreements].***

2.9 WP 29 Opinion on epSOS

The WP 29 Working Document on epSOS is intended to provide guidance on data protection issues in relation with the epSOS project. The WP29 working document is

- The result of an academic of review of available documentation and not a review of implementations
- A working document, not to be understood as a supervision
- Based on a common understanding among the European DPA

The relationship of epSOS to WP29 subgroup will be through the national DPAs. WP29 subgroup on has now delivered and any further consultation will need to take place at national level. PNs are encouraged to discuss further with their national DPAs for additional guidance. Any further future opinions of WP29 will be stimulated through questions arising from its members; epSOS is encouraged to take these questions to the national DPAs.

The main Conclusions may be summarized as follows:

a. epSOS has made the right choices in terms of the legal basis and the legal approach for data exchange. No further action is needed notwithstanding the need for additional clarifications (see point 4 below)

b. The FWA is an appropriate instrument for the purposes of the pilot but sustainability beyond the pilot will require agreements and possibly EU level legal interventions.

c. epSOS has a role in providing Recommendations on the need and appropriate instruments for such agreements but also on retention periods of epSOS access logs for sustainability beyond epSOS.

3. Agreed Principles for EU eIDM [5]

This section provides a list of basic principles on which there is already a consensus in the eID community. They are generic and one should however review them in light of the eHealth requirements.

3.1 Key Messages

From the Athens workshop, one can retain the following principles to serve as basis for this briefing paper on eID interoperability:

- All citizens, businesses and administrations have the right to benefit from a secure eID (see also the Signpost section in annex II of this document);

- eID interoperability is to be understood as interoperability between the means of identification which were issued or relied on at the national level (see the

[5] Debriefing Athens Workshop and initial desktop research

Manchester declaration); a contrario, eID interoperability is not based on a common eID means;

- A first step towards eID interoperability is ensuring a mutual recognition and acceptance of e-Identification/Authentication (See the Manchester declaration, and the EC plan for submitting a legislative proposal in 2012);

- eID interoperability system should be a federated and multi-level system. STORK is demonstrating the feasibility of this.

3.2 Prerequisites for eID systems

The EU eID Roadmap[6] has already identified prerequisites to be fulfilled by the eID systems of the Member States. The following principles should as a minimum be adhered to by the Member States, in order to come to an efficient and interoperable pan-European eIDM infrastructure:

a. Usability considerations should be the most pervasive design constraint when creating a pan-European eIDM framework. This means that the system must be secure, implement the necessary safeguards to protect the user's privacy, and allow its usage to be aligned with local interest and sensitivities.

b. Each Member State should be able to identify users within its borders, if it wishes to allow them access to eIDM services abroad. To this end, the consistent use of suitable identifiers is a necessity to allow the accurate identification and authentication of the entity involved, and to allow the exchange of information between administrations insofar as required for these purposes. The fundamental requirements for a system that addresses the needs of natural persons should be extensible to legal persons as well.

c. Each Member State should issue the means to each user to identify and authenticate himself electronically, if it wishes to allow him access to benefit from eIDM services abroad. A user has the ability to act autonomously and to make use of the offered services.

d. With regard to mandate/representation authorisations, each Member State should provide the means to manage the competences of the identified users within its borders, insofar as these authorisations are not subject to approval by or on the authority of another Member State.

e. Each Member State should support online validation mechanisms of identities, competences and mandates, if it wishes to provide eIDM services.

f. High-level consensus must be established between Member States on an eIDM terminology in order to guarantee conceptual/semantic interoperability. Appropriate policy and legal measures can be used to corroborate this consensus.

[6] http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

3.3 Design criteria for a pan-European eIDM system (also from the eID Roadmap)

From these basic principles, a number of design criteria for a pan-European eIDM system can be derived, which were also included in the Signpost Paper. Most notably, in order to achieve eIDM interoperability, the pan-European eIDM system would need to be:

a) **Federated**, in a policy sense, i.e. allowing administrations to mutually trust each other's identification and authentication methods, accepting these methods on the basis that they were considered acceptable by the administration of origin.
b) **Multilevel**, in the sense that Member States should be permitted to provide multiple security levels for eIDM services, so that the authentication requirements for each eGovernment service can be tailored to the security needs of that service. Member States determine at which level they choose to offer authentication services, and which level of authentication is required for each eGovernment service (although they must accept as valid any authentication methods of the required level from other Member States). This implies that a set of criteria must be defined on a European level which must be met for each authentication level.
c) **Relying on authentic sources**: to ensure data quality and eGovernment efficiency, a single authentic source should be available for each piece of data regarding each registered entity in the Member State of origin. This does not necessarily imply the use of databases, as the authentic source might be a unique token. Additionally, commonalities in the eIDM approach among Member States can be encouraged to provide assurance on the quality of source eIDM data.
d) **Permitting a context/sector based approach** where this is deemed desirable by the Member State of origin (i.e. this is a logical extension of the federated model). Such context can be determined by the application framework or the conceptual framework within which eIDM is used.
e) **Enabling private sector uptake**, where Member States choose to rely on private sector partners (e.g. financial institutions) for the provision of eIDM services.

4. Open Legal Issues

POLICY AND LEGAL BASIS: The review of the current status reveals that there is adequate policy and legal basis for a common EU eID framework for the purposes of supporting the implementation of Directive 2011/24/EU; however, challenges exist in the form of contextualizing the eGov policies and Roadmap to the domain of cross border healthcare. The eGov eIDM model would require the Member States to put in place a framework and policies which respect and interconnect national infrastructures, and which are based on the **mutual recognition of electronic identities** for the purposes of ehealth between countries.

As stated also in the ENISA study on EU eIDM initiatives,[7] *this mutual recognition will then require* ***the definition of specific security levels****, with each means of*

[7] http://www.epractice.eu/files/media/media2552.pdf

identification/authentication being accorded a specific security level ***based on its characteristics and each application*** *stating which security level would be needed. The Member States would then accept each means of identification/authentication as valid provided that it meets the security requirements of the application being accessed. Such policies could be implemented without any specific EU-level infrastructure being established.*

Appropriate ***governance principles*** *will be developed in order to facilitate trust and security in line with Member States specific needs and as such provide the basis for the equal treatment of electronic identities throughout the EU, irrespective of the originating Member State.*

Open Issue: What form will such definition of minimum requirements and Governance take or legal instrument be used? What legislative tool works best may be deduced from: experiences and current motivation of parties involved, parties involved, feasibility of legislative process.

There is a variety of legislative tools to choose from: generally (regulations, directives, intergovernmental, open method of coordination), competences (principal of conferral and principle of subsidiarity art. 5 TFEU). Possibly adoption of measures of the commission (see Article 11 of Directive 2011/24 EU on the application of patients' rights in cross border healthcare). See also Article 114 (approximation of laws) in connection with Art. 168 of the Treaty on the Functioning of the European Union (TFEU.

LEGAL BARRIERS: An approach to identifying open issues may be served through identifying legal barriers. The following elements have been so far flagged:

- **Mutual recognition of eID applied to healthcare if:** Assurance of a secure and reliable (electronic and/or paper based) patient identification process in the Member State of origin of the patient; Assurance of a secure and reliable mechanism for electronically and/or visually authenticating the patient in the Member State were the care is being sought; agreements of appropriate levels e.g. of authentication suitable to the service to access; need for an EU level eID Management Governance. Mutual recognition implies both operation legal interoperability and technical operability – ie the legal right and or obligaiton to recognise the eID issue sin another counrty and the tecnhical capacity to do so through a common tehcnical infrastrucutre.
- **Privacy**: Providing assurance that cross-border identification cannot create a security hole in the access to medical data
- **cross-border access to patient data by an authorised party:** legal basis is patient consent In case of emergency assurance is needed that about the role of the health professional (Authorisation) and the related rights of patients to limit such access.
- **cross-border access to patient data by the patient : the** legal basis identification and authentication of the patient and the requested access.
- **Link with the issue of mutual recognition of health professionals:** Mutual recognition of their roles and their right to access medical data, if the patient gives his/her consent . For this to be achieved we need semantic precision and common definition of roles (healthcare professionals, insurance, administrators..)
- **eID for health only? For health and social security? For eGov with health sector provisions?**

ANNEX 1

Core concepts definitions: draft and open questions

Identity

Data sufficient to identify an entity over time.

Identity of a person

Data sufficient to identify a person over time. May include the person's name, date of birth, identifiers issued by a national body or an organisation etc.

[Proposed by Torbjørn based on the definition of identity]

Alternative definition:

The common sense notion of personal identity. A person's name, personality, physical body and history, including such personal attributes as address etc, of an individual person.

legal identity of a person

Identity awarded by the relevant administration in a country.

Identifier

Identity information that unambiguously distinguishes one entity from another one in a given domain.

Trait

Distinguishing quality or characteristic, typically one belonging to a person.

Identity document

Document which may be used to verify aspects of a person's identity.

[Proposed by Torbjørn based on the Wikipedia description of identity document]

Identification

The process of obtaining information about whom the requester claims to be without considering the "trustability" of this information.

authentication

Provision of assurance of the claimed identity of an entity.

Alternative definitions:

Corroboration that an entity is the one claimed

The process of validating an identity token inclusive of its attributes in the context of a healthcare or social service, both in the Member State and the cross-border setting.

Authorization

The process by which rights are granted, e.g. the right to access or use a given service.

[Proposed by Torbjørn as an amalgamation of the two candidate definitions below. (In my opinion the STORK definition is to narrow since we in our future work may need to describe other kinds authorisation, e.g. authorisation to provide health care.)]

Alternative definition:

granting of rights

> [Definition from ISO 13606-1:2008 Health informatics -- Electronic health record communication -- Part 1: Reference model]
>
> [Definition from ISO 15782-1:2009 Certificate management for financial services -- Part 1: Public key certificates]

The process by which entitlement of a requester, to access or use a given service, is determined

> [Definition from STORK Glossary and Acronym]

eHealth Interoperability

The ability of two or more ICT systems to interact with one another and exchange health-related information according to a prescribed method in order to achieve predictable results.

[Proposed by Torbjørn based on the definition of *interoperability* in ISO/TR 16056-1:2004 Health informatics -- Interoperability of telehealth systems and networks -- Part 1: Introduction and definitions]

Alternative definition:

A characteristic of an ICT enabled system or service in the healthcare domain that allows its users to exchange, understand and act on citizens/patients and other health-related information and knowledge in a commonly interpreted useable way. In other words it is a means of crossing linguistic, cultural, professional, jurisdictional and geographical border in eHealth. In CALLIOPE, interoperability is addressed within the conceptual framework of the EC Recommendation on cross-border interoperability of electronic health record systems[8].

EU Governance

Refers to the rules, processes and behaviour that affect the way in which powers are exercised at European level [European Governance: a White Paper]9.

8 Commission Recommendation on cross-border interoperability of electronic health record systems, Brussels, COM(2008)3282, http://ec.europa.eu/information_society/activities/health/docs/policy/20080702-interop_recom.pdf

9 Commission of the European Communities. European Governance: a White Paper. Brussels, 25 July 2001 (COM(2001) 428 final)