Co-funded by
the Health Programme
of the European Union

JASEHN

Joint Action to Support the eHealth Network

DISCUSSION PAPER

on

eHealth-specific eID framework across-borders

Document status:	For discussion by the members of the eHealth Network at their 10th meeting on 21 November 2016
Approved by JAseHN sPSC	Yes
Document Version:	V3.0
Document Number:	D5.2.1
Document produced by:	Joint Action to support the eHealth Network • WP5: Interoperability and standardization • Task 5.2: Electronic identification for eHealth
Author(s):	Beatrice Streit, GEMATIK (Germany) Jürgen Wehnert, GEMATIK (Germany)
Member State Contributor(s):	ASIP (France), HSE (Ireland), SOM (Estonia), ATNA (Austria), BHTC (Belgium), FRNA (France), NVD (Latvia), HDIR (Norway), SPMS (Portugal), SEHA (Sweden), AeS (Luxembourg), MFH (Malta)
Stakeholder Contributor(s):	CPME, e-SENS

TABLE OF CHANGE HISTORY

VERSION	DATE	SUBJECT	MODIFIED BY
0.2	2015-08-24	Original version	Beatrice Streit, Jürgen Wehnert (GEMATIK)
0.6	2015-09-09	Scope version	Beatrice Streit (GEMATIK)
1.0	2016-04-11	Draft version for sPSC review	Beatrice Streit, Jürgen Wehnert (GEMATIK)
1.2		Incorporation of reviewer's comments	Beatrice Streit (GEMATIK)
1.8	2016-10-13	Update Draft Version	Beatrice Streit (GEMATIK)
2.0	2016-10-14	Draft submitted "for review" by JaseHN WP3	Beatrice Streit (GEMATIK)
2.0	2016-10-17	Draft submitted for sPSC review	Beatrice Streit (GEMATIK)
3.0	2016-11-02	V3.0 created	Beatrice Streit (GEMATIK)

LIST OF ABBREVIATIONS

ACRONYM	DEFINITION
CBeHIS	Cross Border eHealth Information Services
CEF	Connecting Europe Facility
DSI	Digital Service Infrastructure
EC	European Commission
eHDSI	eHealth Digital Services Infrastructure
eHN	eHealth Network
EIF	European Interoperability Framework
eP	electronic Prescription
EU	European Union
IOP	Interoperability
HP	Health Professional
JAseHN	Joint Action for support the eHN
LOST	Legal, Organisational, Semantic, Technical
AA	Administrative Agreement former Multilateral Legal Agreement (MLA)
MS	Member States (of EU)
NCP	National Contact Point for cross border
NCPeH	National Contact Point for eHealth
NI	National Infrastructure
OFW	Organisational Framework
OFW-NCPeH	Organisational Framework for eHealth National Contact Point
PoC	Point of Care
PS	Patient Summary
ReEIF	Refined eHealth European Interoperability Framework
QSCD	Qualified Signature Creation Device

TABLE OF CONTENTS

1. Introduction

Electronic identification of citizens (e.g. being a patient or a healthcare professional) is key to setting up cross-border services in the European Union. Identification, authentication and authorization are prerequisites for cross-border use cases like ePrescription and Patient Summary and are managed differently in each Member State. For example some Member States have a comprehensive eID which is used for eHealth and other purposes at the same time while others have separate eIDs for different domains and purposes.

JAseHN's task T5.2 "electronic identification in eHealth" deals with the continuation of activities concerning identification in the context of cross-border care (directive 2011/24/EU) as decided in the multi-annual work plan 2015-2018 of the eHealth Network. The task T5.2 is in charge of preparing D5.2.1 eHealth-specific eID framework across-borders, which will address the mutual trust and recognition of citizens (e.g. being a patient or a health care professional) using electronic cross-border services. This is because the health care systems in the European Union have various organizational forms and thus a unified process for identification, authentication and authorization is not the objective.

The proposal for the eHealth-specific eID framework across-borders will take the diversity of the European (e)health and ID systems into account while conforming to the legal framework in particular the eIDAS regulation. It is not intended to alter already existing national eID solutions in eHealth, but provides Member States with possible aspects for future enhancements and strategic orientation.

This first instalment serves as an up-to-date report on eID related activities, which sets the foundation of the future framework and includes a kind of check list for MS providing steps which need to be taken and achieved in order to implement it. The upcoming final instalment of the eHealth-specific eID framework across-borders will be ready for eHN's adoption in May 2017.

2. Conceptual basis and rationale for action

2.1 Basis and rationale

The main foundation of the future eHealth-specific eID framework across-borders are the eIDAS regulation and the General Data Protection Regulation, which applies to several domains including eHealth. The following chapter thus identifies and discusses the important and critical elements of both regulations, the specific needs of eHealth and enabling initiatives, which are still working on finding appropriate solutions on not only technical level. Afterwards the findings are turned into action proposals for Member States to undertake in anticipation of the eHealth-specific eID framework across-borders.

2.2 eIDAS regulation

On the 23rd of July 2014 the EC published a regulation on the electronic identification and trust services for electronic transactions in the internal market (eIDAS regulation 2014/910/EU). While the regulation explicitly mentions the existence of eHealth requirements (compare recital 10 of the eIDAS regulation) the statements are very general and not specific for domains like eHealth.

There are, however, significant aspects of the eIDAS regulation which are of special interest concerning eHealth:

- It is entirely up to the member states to decide if and which national eID system(s) will be notified to the EC (compare Art. 7 as well as recitals 12 – 15 of the eIDAS regulation).
- Processing of personal data is subject to the Directive 95/46/EC (compare recital 11 of the eIDAS regulation and Art. 5 of the eIDAS regulation). The subsequent General Data Protection Regulation should be taken into account as it repeals Directive 95/46/EC.
- There is a description of assurance levels for electronic identification schemes; the mutual recognition obligation is just given for assurance level substantial/high (compare Art. 8 of the eIDAS regulation and its commission implementing regulation 2015/1502/EU).
- Mutual recognition is a topic (compare Art. 6 of the eIDAS regulation), which deserves special attention.
- There are articles on the topics security breach and liability (compare Art. 10 and 11 of the eIDAS regulation), which are to be considered.
- The eIDAS eID mechanisms and their specific regulatory, liability, IT security, trust establishment, and operation environment provisions may impact the operation/fitness of existing and new cross-border electronic services.
- Repealing the eSignature Directive by eIDAS may impose new requirements (such as the "qualified" property) onto existing and new cross-border electronic services.

Cooperation of member states and interoperability of the notified electronic identification schemes shall be facilitated e.g. by establishing an interoperability framework (compare Art. 12(7) of the eIDAS regulation and its commission implementing decision 2015/296/EU and Art. 12(8) of the eIDAS regulation and its commission implementing regulation 2015/1501/EU).

The recitals 10 and 12 of eIDAS made clear explicitly that the domain eHealth was taken in consideration:

Recital 10: cross-border directive 2011/24/EU and eHN

"Directive 2011/24/EU of the European Parliament and of the Council set up a network of national authorities responsible for e-health. To enhance the safety and the continuity of cross-border healthcare, the network is required to produce guidelines on cross-border access to electronic health data and services, including by supporting 'common identification and authentication measures to facilitate transferability of data in cross-border healthcare'. Mutual recognition of electronic identification and authentication is key to making cross-border healthcare for European citizens a reality. When people travel for treatment, their medical data need to be accessible in the country of treatment. That requires a solid, safe and trusted electronic identification framework."

Recital 12:

"One of the objectives of this direction is to remove existing barriers to the cross-border use of electronic identification means used in the MS to authenticate, for at least public services. This regulation does not aim to intervene with regard to electronic identity management systems and related infrastructures established in MS. The aim of this Regulation is to ensure that for access to cross-border online services offered by MS, secure electronic identification and authentication is possible."

The eIDAS regulation applies on cross-border patient data exchange with online-services such as Patient Summary and/or ePrescription services despite the fact that the eIDAS regulation was created intentionally to be not specific for any domain and its needs. Nevertheless the eIDAS set-up allows for optional agreed extensions based on domain's needs on domain's request.

2.3 General Data Protection Regulation

On the 27th of April 2016 the EC published a regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). This will also have an influence on the eIDAS regulation, which currently refers to Directive 95/46/EC in the following way:

Recital 11: protection of personal data 95/46/EC

"This Regulation should be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council. In this respect, having regard to the principle of mutual recognition established by this Regulation, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. Furthermore, requirements under Directive 95/46/EC concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies."

The General Data Protection Regulation made clear explicitly that personal data concerning health and health care services as referred to in the cross-border directive 2011/24/EU were taken in consideration:

Recital 35: personal data concerning health and cross-border directive 2011/24/EU

"Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (1) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test."

There are several definitions relevant for eHealth, nevertheless the definition of 'data concerning health' is the most important one as it is the first time that such data is defined in a legal context being a special category of personal data. According to Art. 4 (15) General Data Protection Regulation 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. Art. 9 of the Regulation is about the processing of special categories of personal data, which includes data concerning health. Art. 9 (4) states that 'MS may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health'. 'cross-border processing' is defined in Art. 4 (23) either as

> (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
>
> (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

It has to be analysed if this definition of cross-border processing applies on cross-border patient data exchange with online-services such as Patient Summary and/or ePrescription services and if so which are possible consequences out of this.

2.4 Open Issues

The eIDAS regulation and the General Data Protection Regulation repealing Directive 95/46/EC are the legal boundaries for eID in eHealth. The *Administrative Agreement between National Authorities responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Services* (AA) will put this on a more concrete level to serve the eHealth specific needs of cross-border patient data exchange with online-services such as Patient Summary and/or ePrescription services. Relying on the referred legal framework D5.2.1 eHealth-specific eID framework across-borders will be added, which will to be fully aligned with the overall legal framework and especially to the Administrative Agreement. Both documents – the Administrative Agreement and D5.2.1 eHealth-specific eID framework across-borders – will be tabled to the eHN in May 2017 for adoption.

Several questions concerning eID in eHealth are addressed within the following different initiatives on diverse levels but not sufficiently solved by now. The busy work is still on going and will bring a lot of relevant results. According to this an overall solution as to be laid out in D5.2.1 eHealth-specific eID framework across-borders is still pending.

The current eIDAS technical specification limits itself to the core requirements from eIDAS, while preserving a certain degree of extensibility for the needs of other sectorial requirements such as encoding and transporting additional attributes. This shall allow the domains governance over domain-specific needs, without changing the eIDAS core specs and eIDAS reference software implementation. From the eHealth perspective it is currently unclear in detail how feasible and sustainable a solution with a singular reliance on the eIDAS core specification and implementation with the use of only additional (optional) attributes is in the medium/long-term. The European project e-SENS and an eHealth eID Study will generate first-hand knowledge and experience.

The to be taken decision on the choice of assurance level(s) appropriate for eHealth shall be strict enough to fully protect medical data exchange (article 12 §3 and §7 of eIDAS). The decision could be that only the highest assurance level of eIDAS would match the requirements of sensitive medical data. This would force each participating MS into strictly adhering to the minimum requirements as assigned to the Assurance Level 'high' as regulates by the eIDAS regulation. Each MS is requested to consider this carefully by investigating their national situation and possible consequences to fulfil the minimum requirements of the highest eIDAS Assurance Level.

The eIDAS Cooperation Network will enhance the adoption and operation of eIDAS regulation and its reference implementation as its highest decision-taking body. It is up to DG SANTE and the eHealth Network as equally positioned bodies to stand up aligned for the specific matters and requirements of eHealth concerning especially data protection and identification of roles. On working and technical level the following initiatives concerning eHealth eID take place and will help to guide the policy level decision making as best as possible.

2.5 e-SENS findings

The aim of the e-SENS project is to facilitate the deployment of cross-border digital public services through generic and re-usable technical components, based on the building blocks of the Large Scale Pilots. The consolidated technical solutions, with a strong focus on e-ID, e-Documents, e-Delivery, Semantics and e-Signatures, aim to provide the foundation for a platform of "core services" for the eGovernment cross-border digital infrastructure foreseen in the regulation for implementing the Connecting Europe Facility (CEF).

The eID parts of the services Patient Summary and ePrescription/eDispensation are addressed in WP5.2 which is in charge of the eHealth pilot. The e-SENS eHealth eID architecture describes two suitable technical solutions for eID. One focuses on a strictly smartcard-based approach as a qualified signature creation device (QSCD) in conjunction with the contained qualified certificates, which is essentially consolidating the diverging smartcard eID means of different MS into one streamlined solution (e-SENS way 0). The other approach focuses on virtual authentication schemes (such as eIDAS, legacy STORK 2.0, etc.) as well as an optional mobile eID, which is feasible for MSs with a software token-based (non-physical eID carrier) eID solution (e-SENS way 1). Both solutions are fully interoperable and combinable with each other to enable seamless identification and authentication processes of patients and health professionals.

However, any combinatory approach with eIDAS eID requires the capability to encode and transport an additional attribute[1] patient identifier. This attribute will be added to the eIDAS SAML Assertion outside of the eIDAS minimum data set, meanwhile the minimum dataset stays absolutely unchanged. The inclusion and processing of additional attributes is MS responsibility. Nevertheless, to gain an interoperable solution it is recommended that the highest decision making body in that domain takes the decision and informs the eIDAS Cooperation Network accordingly. The latter has to acknowledge the entire notified eID scheme of each MS including the additional attributes within the eIDAS SAML Assertion at time of notification. In the eHealth domain the eHealth Network is the responsible body to start this process for an additional attribute patient identifier. This might happen when eHN adopts D5.2.1 eHealth-specific eID framework across-borders in May 2017.

e-SENS is currently carrying out an eHealth eID Pilot with Austria, Greece, Italy, Portugal and Spain participating in it, which should bring up more detailed results and experiences on technical level. This will enhance D5.2.1 eHealth-specific eID framework across-borders with aspects on readiness and

[1] No additional attribute is needed for MS that merged the eGovernment and patient identifier into one singular property (such as PT, IT, etc.).

maturity of the e-SENS technical solutions as well as lessons learned concerning future implementations and long-term sustainability. The eHealth eID Pilot is expected to end by beginning of 2017.

2.6 Deloitte Study 'The use of CEF eID in the CEF eHealth DSI'

An eHealth eID Study was contracted by DG SANTE and is produced by a Deloitte team in cooperation with DG DIGIT. The eHDSI Solution Provider is the unit within DG SANTE responsible for the study, which should gain results based on an analysis of the use of the CEF eID building block under eIDAS for the eHDSI Patient Summary and ePrescription services. The study takes into account the national setup in terms of existing systems and infrastructures for both national eID schemes and eHealth related ones as well as future plans for notification under eIDAS of the following six MSs in an exemplary manner: Austria, Finland, Italy, Luxembourg, Portugal and Sweden. On this basis future implementation scenarios of cross-border identification/authentication of patients for eHealth should be identified and described.

The Deloitte Study on eID in eHealth has reached a more mature status. Nevertheless it is currently under a revision process. Until now a new date of delivery for the final version of the study could not be given. The beforehand mentioned extension of the study with more MSs' experiences was prioritised of secondary importance and therefore put off meanwhile.

The results of the Deloitte Study are crucial input for D5.2.1 eHealth-specific eID framework across-borders as prerequisites also on policy level are considered to be addressed. The laid out implementation scenarios with its pros and cons will have a strong impact on the decision making of MSs in preparation of CEF eHealth and are essentially for moving on to a successful operation of cross-border patient data exchange.

3. Principles and requisites for action

MSs are currently preparing the operation of cross-border patient data exchange with online-services such as Patient Summary and/or ePrescription services which are supported by the EC under the CEF eHealth call for proposals (2015 CEF-TC 2015-2). To address the open questions on eIdentification under eHealth Digital Service Infrastructure (eHDSI) the following steps are proposed provided that the e-SENS eHealth eID pilot and the Deloitte Study 'The use of CEF eID in the CEF eHealth DSI' will finish their ongoing work latest by beginning of next year.

Steps to be performed by eHN in the preparation phase before cross-border eHealth operation:

- Discuss and decide on an assurance level according to 2015/1502/EU
- Discuss and decide on an additional attribute for patient identifier in addition to the eIDAS minimum dataset according to 2015/1501/EU

Steps to be performed by DG SANTE, DG DIGIT and the eIDAS Cooperation Network in the preparation phase before cross-border eHealth operation:

- Be informed about and acknowledge eHN's decision on assurance level and patient identifier
  If applicable, incorporate it into the eIDAS Node, CEF BBs

Steps to be performed by each MS in the preparation phase before cross-border eHealth operation:

- Decide whether to notify MS's national eHealth related eID system to the EC (in any case your solution needs to accept notified national eHealth related eIDs)
- Choose e-SENS way 0 or 1 (corresponding to e-SENS business levels 4 and 5) appropriate for your MS's solution;
- Implement the eIDAS compliant solution for your patient's eID in the MS.

In future also;

- Implement your national electronic health professional register according to the eHN guidelines to be adopted in May 2017

or

- Check if MS's existing electronic health professional register is coherent with the eHN guidelines (if not, change it accordingly)
- Register your national electronic health professional register to the MS's eIDAS node
- Implement the eIDAS compliant solution for your health professionals' eID in the MS

Steps to be performed by JAseHN's task T5.2 eID for eHealth until the next eHN meeting in May 2017:

- Proposal for an eID specific Framework for eHealth, for adoption by the eHN
- Proposal for Guidelines on the interoperability of electronic health professional registries, for discussion by the eHN

4. Conclusion

The present document gives an up-to-date overview on the activities of multiple initiatives concerning eID in eHealth. At this point of time there is not enough detailed analysis and synthesis carried out by the mentioned multiple initiatives to compose D5.2.1 eHealth-specific eID framework across-borders which will guide MSs on how to address eID nationally based on their individual situation in order to ensure an interoperable eID mechanism.

Therefore MSs are kindly asked to discuss if they are able to commit to the laid out direction concerning eHealth eID which is based on eIDAS and will probably take into account to notify at least one eID scheme which will be used for identifying patients for cross-border patient data exchange with online-services such as Patient Summary and/or ePrescription services. MSs shall also take into consideration how long it will take themselves on national level to be ready for cross-border patient data exchange including eID schemes. When estimating this MS should keep in mind that they need to fulfil at least the minimum requirements on Assurance Level 'substantial' of the eIDAS regulation on national level.

5. References

5.1 Legal references

- 2011/24/EU directive on the application of patients' rights in cross-border healthcare (cross-border directive)
- 2014/910/EU regulation on the electronic identification and trust services for electronic transactions in the internal market (eIDAS regulation) and delegated acts
- 2015/296/EU Commission implementing decision establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of eIDAS regulation
- 2015/1501/EU Commission implementing regulation on the interoperability framework pursuant to Article 12(8) of eIDAS regulation
- 2015/1502/EU Commission implementing regulation on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of eIDAS regulation
- 95/46/EU directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- 2016/679/EU regulation on the protection of natural persons with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation)

5.2 Content-related references

- eHGI documents
    - D2.1 eID for eHealth: towards EU governance
    - D2.2 eID for eHealth: towards coherence with the proposal of the Commission for eID regulation
- e-SENS documents
    - WP5.2 eID general architecture
        - WP5.2 eID eIDAS Integration Approach: e-SENS eHealth eID with eIDAS Approach and Pilot (work in progress)
    - WP4 Implication of eIDAS Regulation for eHealth (work in progress)