eHealth Network

POLICY PAPER

on

eID specific framework for eHealth

RELEASE 1

The eHealth Network is a voluntary network, set up under article 14 of Directive 2011/24/EU. It provides a platform of Member States' competent authorities dealing with eHealth. The Joint Action supporting the eHealth Network (JAseHN) provides scientific and technical support to the Network.

Adopted by consensus by the eHealth Network, Saint Julian's, Malta, 9 May 2017

-Keep this page free-

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
MLA/Agreement	Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross Border eHealth Information Services 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

One of the main challenges in supporting the eHN (eHealth Network) ambitions for sustainability policies regarding assets in the field of eHealth cross-border interoperability is the bond between policies and service provision by Member States (MS).

In order to establish the bond and allow it to grow and endure a set of simple but well-aligned instruments needs to be prepared. One of the crucial instruments is an Organisational Framework which describes, in a commonly understandable language, the principles and requirements for National Contact Points for eHealth (NCPeH). Another important instrument is the eHealth-specific eID framework across borders, which will address the mutual trust and recognition of means to identify citizens (e.g. being a patient or a health care professional) using electronic cross-border services under the Cross Border eHealth Information Services (CBeHIS). CBeHIS stands for the infrastructure and the operations used to exchange real patient related data, in particular health data, between its Members.

1.1 Purpose of this document

The purpose of this document is to propose an eID specific framework for eHealth to support the establishment of an interoperable eID mechanism in MSs for the provision of Cross-Border eHealth Information Services (CBeHIS). Introduction of the eID framework is to be done in two steps which correspond to two releases. This document addresses only the first release of the eID framework.

The Policy Paper on the eID specific framework for eHealth was prepared based on accomplished activities and in close alignment with still ongoing activities, namely (but non-exhaustively):

- Organisational Framework for eHealth National Contact Points (OWA-NCPeH) adopted by eHealth Network
- Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross Border eHealth Information Services (Agreement) to be adopted by eHealth Network and to be signed by the competent national authorities.
- eSENS' T5.2 and eHealth eID Pilot through several Joint Workshops[1]
- eSENS' WP4 Implication of eIDAS Regulation for eHealth[2]

[1]An e-SENS JAseHN Joint Workshop took place on the 30th January 2017 in Berlin. At the end of that day the open question remained how to make the NCPeH ready for eIDAS in time for eHDSI implementation (second wave in February 2019).
The JAseHN eID Workshop on the 31st January 2017 tried to find a way forward concerning eID by sharing expertise and sketching a composition of next steps on the basis of a common understanding. This resulted in a revised concept and scope for D5.2.1 eID framework for eHealth which accounts for the joint assessment that an interim solution for eID seems to be most appropriate. In the workshop strong concerns about the possibility to finalize the eID framework in May 2017 were raised. Due to the complexity of the topic and the identified tasks which have to be addressed but are mainly not in scope of JAseHN the participants of the workshop preferred to have an eID framework with a provisional nature for eHealth Network meeting, which would be finalized at a later stage for instance November 2017. This would also take into account the results of the identified tasks, which should be done until then.

[2] One view on the Implications of the eIDAS Regulation for eHealth is laid down in the eponymous document from the legal expertise center of e-SENS, which was presented and discussed in the e-SENS JAseHN Joint Workshop which took place on the 30th January 2017 in Berlin. Both parts of the eIDAS Regulation were equally addressed in the document.

1.2 Scope

The eID specific framework for eHealth lays down requirements to identify a patient and a health professional in an interoperable manner by electronic means - considering the legal basis for CBeHIS provision in Europe. It does not aim to alter already existing national eID solutions in eHealth, but to provide Member States with viable aspects for future enhancements and strategic orientation.

The eID framework will help MSs to overcome the common challenges regarding electronic identification, by providing a common approach to tackle this matter from a structural perspective as well as framing a set of actions to leverage the joint adoption of this innovative instrument. Not in the immediate focus of the eID framework but closely related and equally important is electronic signature to name just one of the trust services under eIDAS Regulation. In short and only if applicable the eID framework will take into account trust services as subordinated theme.

The eID specific framework for eHealth considers the current situation of eID, proposes a number of actions and next steps and considers known concerns, challenges and, where applicable, provides recommendations and requirements. It will show the boundaries of eID without limiting the scope of technical options. The full eID framework will contain sustainable eID measures and requirements for eID implementation in CBeHIS. The document at hand addresses the first release of the eID framework with a second release planned for November 2017.

This eID framework will only consider and thus apply to the Patient Summary (PS) and ePrescription/eDispensation (eP/eD) use case. However, specific adaptions of the framework for additional use cases may be necessary at a later time.

1.3 Objectives

A plan for the revision of the eID framework is proposed and shall consist of the following releases:

Release 1 (Document at hand)
Provide an eID framework Release 1, which

- lays down the past and current situation on eID in eHealth to build a common understanding
- gives guidance on identification and authentication for the first wave of eHDSI and
- frames a set of actions necessary for establishing an interoperable eHealth-specific eID solution for CBeHIS.

Release 2 (in November 2017)
Provide an eID framework Release 2, which

- adds concrete measures and requirements to be included in the eHDSI specifications for March 2018 Release[3] and
- sets up sustainable principles and requirements for an interoperable eHealth-specific eID solution for CBeHIS.

1.4 Initial considerations

The overall structure presented in the Guideline on an Organizational Framework for eHealth National Contact Point (OFW-NCPeH) foresees several instruments to support CBeHIS in its preparation, deployment and operation phase. Each Member State aiming to participate in the eHDSI shall undergo all three phases. For every phase JAseHN provides supportive documents. The eID specific framework for eHealth is one of these documents which in its Release 1 addresses the Preparation and Deployment Phase.

[3] This release is the basis for going live in February 2019 (second wave of CEF eHealth).

The proposal for an eID specific framework for eHealth was designed in reference to the refined eHealth European Interoperability Framework (reEIF).

2. eID specific framework for eHealth

The following sections lay down concerns, challenges and known possibilities or recommendations regarding eID in eHealth taking into account the specific e-SENS recommendations. They are structured following the LOST approach according to re EIF complemented by additional sections where needed.

2.1 The wider remit of eHealth eID

At that time the epSOS pilot was implemented and operated not the eIDAS regulation but the e-signature Directive 1999/93/EC applied and was hence taken into account by the epSOS specifications and OpenNCP reference implementation. Changes to epSOS specifications or the OpenNCP reference implementation are still made in order to maintain or to enhance the existing content, e.g. for piloting purposes such as the e-SENS eHealth eID pilot.

Regulation (EU) N°910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (hereinafter the eIDAS Regulation) repealed the e-signature Directive 1999/93/EC and introduced new concepts to build or strengthen trust in electronic transactions in the internal market. The eIDAS regulation consists of two parts: one on Trust Services, the other on eIdentification. The Trust Services part is already fully applicable whereas for the mandatory recognition of notified eID Schemes there is a transition period until September 2018.

As of today there are no notified eID Schemes from Member States and specific information on their notification plans are rare[4]. Due to a lack of experience it is also unclear how long the notification process will take. Notification of an eID scheme comprises of several steps: Pre-notification by submitting necessary materials for the notification, peer review of the to-be-notified eID scheme by the other MSs and the formal step to publish the now notified eID scheme. A minimum time of six months for the notification process is expected, yet it may take longer.

An eHealth eID Study should gain results based on an analysis of the Member States' current and planned use of the CEF eID building block under eIDAS for the eHDSI Patient Summary and ePrescription services. It was contracted by DG SANTE and is produced by a Deloitte team in cooperation with DG DIGIT. Within DG SANTE the eHDSI Solution Provider is the unit responsible for the study. The study takes into account each 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. eID of Health Professionals (HPs) are out of scope. A final draft version of the Deloitte Study on eID in eHealth was shared in November, 2016; it is currently under revision and will be extended to include additional MSs' experience. To do so, several Member States received questionnaires on eID regarding their specific national situation and whether the Member State considers one of the described scenarios applicable for their national eID Implementation in CBeHIS.

[4] At the time of the release of this document it was announced by the EC that Germany is the first MS starting the notification process on 20th February 2017 for the German eID card and the electronic residence permit. Both eID schemes do not apply to the eHealth domain. The German eID card is handed in general to a German citizen aged 16 or older, whereas the e-residence permit is given to nationals of non-EU countries with an existing residence permit.

Above mentioned scenarios draw on the very specific scenarios implemented by the e-SENS eID eHealth Pilot under the vast resource and time restrictions of a non-operational EU pilot project. An economic analysis of the chosen scenarios or an approach for a sustainable solution for eHDSI was neither part of e-SENS nor done by Deloitte. Thus the economic impact of the proposed scenarios or any additional scenarios beyond the scope of the study will need to be analysed in support of the decision making in the Member States. For example, the cost per transaction may vary between some Cents and several Euros.

The date of delivery for the final version of the study is end of April.

2.2 General Considerations, Responsibilities and Duties

eIDAS can be seen as a system and a tool box for establishing trust which sets new rules and provides solutions not available at the time of epSOS. The epSOS specifications or the OpenNCP reference implementation are not adapted for eIDAS as of today. This statement refers to both parts of eIDAS: trust services as well as eIdentification. In order to bridge this gap and provide a sustainable eID solution towards CBeHIS provision it is necessary to take a look at the following general considerations especially towards responsibilities and duties of the diverse relevant actors.

- eID eIDAS profile and the sample implementation of it called eIDAS-Node will be provided by the European Commission trough DG DIGIT, specific national implementations will be carried out by each national eIDAS competent authority. There is no correlation between the notification of an eID Scheme and the existence of an eIDAS-Node implementation in MS. MS will have an eIDAS-Node even if they do not intend to notify any eID Scheme in order to be able to recognize the notified eID means of other MSs.
- Due to the ongoing transition period until September 2018 for the mandatory recognition of notified eID Schemes a stable release of the eID eIDAS profile and the eIDAS-Node will only be finalized and published by DIGIT in the summer of 2018. Additional changes to and releases of the eID eIDAS profile and the eIDAS-Node may happen afterwards but due to a necessary rechecking and implementing processes in MS this will result in a service suspension of approximately half a year. The eIDAS Cooperation Network as the highest decision-taking body of eIDAS will enhance the adoption and operation of eIDAS regulation with the eID eIDAS profile and the eIDAS-Node. 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.
- The solution provider of DG SANTE is the responsible unit for the eHDSI specifications (based on the epSOS work) and the OpenNCP reference implementation of NCPeH. Maintenance, updates and add-ons of the NCPeH take place under the guidance of DG SANTE taking into account the specific DSI Owner's perspective from a policy viewpoint.
- The first wave of eHDSI (go live in February 2018) will operate without electronic identification in practise. Patients and HPs will be identified and authenticated as described in the epSOS use cases of PS and eP/eD[5]. For the second wave (go live in February 2019) and onwards the sustainable eID solution will be available for the use of MS. However, MSs remain free to decide if they will use identification and authentication with electronic or non-electronic means. Electronic means hereby includes one of the options: notified or not notified eID schemes. The Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross Border eHealth Information Services (Agreement) is the basis

[5] Further details are originally led out in epSOS Common Components Specifications (see http://www.epsos.eu/uploads/tx_epsosfileshare/D3.4.2_epSOS_Common_Components_Specification_01.pdf) but are outdated due to the NCPeH Release 'Wave 1 – Release Candidate', which was published on 28th March 2017 (see https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+Artefacts+Releases).

for this (refer to Agreement clause II.1.1.2 on identification and authentication of patients, health professionals and healthcare providers) clearly stating that the identification and authentication of the HP and HCP is the responsibility of Country B, and is performed according to national procedures (refer to Agreement clause II.1.1.3 Authorization of health professionals).

2.3 Legal Environment

This section provides a non-exhaustive description of the legal environment on European level for the eID framework.

The main foundation of the eID specific framework for eHealth is the eIDAS Regulation and the General Data Protection Regulation, which applies to several domains, not specifically to eHealth. The eIDAS Regulation and General Data Protection Regulation shall be followed by all Member States and shall be transferred into national legislation regardless of whether they participate in CBeHIS or not.

Here are 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). However, the recognition of notified eID schemes is mandatory from September 2018 on.
- 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 (compare Art. 6 of the eIDAS regulation) is just given for assurance level substantial/high (compare Art. 8 of the eIDAS regulation and its commission implementing regulation 2015/1502/EU).
- 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 explicitly state that the domain eHealth has been taken into consideration. The eIDAS regulation applies for cross-border patient data exchange with online-services such as Patient Summary and/or ePrescription services even though it is intended to serve needs beyond domain boundaries. The eIDAS set-up allows for optional agreed extensions based on the individual domain's needs upon the domain's request.

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). The General Data Protection Regulation made it explicitly clear that personal data concerning health and health care services as referred to in the cross-border directive 2011/24/EU were taken into consideration, see recital 35.

The Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross Border eHealth

Information Services (Agreement) is currently prepared by JAseHN task T6.2 and lays down legal boundaries for the CBeHIS provision on the grounds of eIDAS regulation and several other applicable laws. The agreement is to be adopted by the eHealth Network in May 2017 and to be signed by the competent national authorities.

Among several other clauses the Agreement refers to the identification and authentication of patients, health professionals and healthcare providers as well as to the authorization of a health professional. These clauses on eID leave the decision to use electronic identification (notified under eIDAS or not notified) or to use identification with non-electronic means with each Member State. A guidance paper on eID will also be prepared by T6.2 but was not available at the time of writing.

The legal foundation of the eID specific framework for eHealth consists of eIDAS regulation, GDP Regulation and Agreement. However, the overarching question which services of eIDAS (Trust Services and eIdentification) will need to be used to reach the goal of secure data exchange across borders still remains open.

To be able to come to an answer the following points need to be carefully considered:

- Member States are obliged to recognize notified eID Schemes after September 2018 with a transition period until then where recognition is on voluntary basis. There is no obligation for Member States to notify eID Schemes neither now nor in the future. The consequences in practical terms or interoperability of the large variety of possible implementations in MSs cannot be foreseen at the moment.
- Electronic signatures are now regulated under eIDAS (part on Trust Services) which repealed the eSignature Directive 1999/93/EC and are to be implemented for the Patient Summary and ePrescription/eDispensation use cases of CEF eHealth but new a new concept and consequently new requirements have been introduced. They are to be analysed and further actions for implementations initiated.
- The Agreement prepared by the T6.2 of JAseHN states requirements to be fulfilled by eIDAS Regulation and GDP Regulation (Agreement clause II.4.1). An according eHDSI implementation and CBeHIS provision ("*confidentiality, integrity, authenticity, availability and non-repudiation according to Regulation 2014/910/EU and Regulation 2016/679/EU*") shall be analysed in order to incorporate them not only on a technical level.

2.4 Organisational and Policy Requirements

Building on the legal environment the following organisational and policy related considerations and requirements are identified.

The Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross Border eHealth Information Services (Agreement) lays down the eHealth specific rules for cross-border patient data exchange with online-services such as Patient Summary and/or ePrescription. For CBeHIS implementation the following two requirements concerning the Agreement shall be fulfilled:

1) **The eHealth Network shall adopt the Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross Border eHealth Information Services (Agreement).**
2) **Each National Authority responsible for the NCPeH and taking part in CBeHIS shall sign the Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross Border eHealth Information Services (Agreement).**

There is a need for specific requirements concerning ID for the first wave of eHDSI (go live in February 2018) and afterwards.

3) **The eHealth Network shall adopt that the first wave of eHDSI (go live in February 2018) will operate patients' and HPs' identification and authentication non-electronically with reference to the 'Wave 1 – Operation Ready' Release of the NCPeH[6].**
4) **The eHealth Network shall adopt that from the second wave of eHDSI (go live in February 2019) on patients' and HPs' identification and authentication will be operated according to the clauses of the Agreement and the productive Releases of the NCPeH for Wave 2 and following.**

For cross-border purposes, a unique patient identifier is a necessary requirement for each individual patient to be linked to the patient record in the country of affiliation. Additionally concerning eIDAS assurance level the e-SENS project recommended:

> "The eHealth Network should consider, in the relevant guidelines, appropriate assurance levels for electronic identification and authentication for the purposes of cross border eHealth services supported by the eHealth DSI balancing the risks associated to individual or groups of health services and existing national laws and infrastructure capabilities."

The following decisions of the eHealth Network have to be achieved in order to implement eID for eHealth in MSs as part of CBeHIS.

5) **The eHealth Network shall adopt common additional attributes[7] for a patient identifier in addition to the eIDAS minimum dataset according to 2015/1501/EU.**
6) **The eHealth Network shall adopt an agreed level of electronic identification and authentication for CBeHIS.**

The decision to be taken regarding adequate 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 to securely exchange sensitive medical data across-borders. This would force each participating MS into strictly adhering to the minimum requirements as assigned to the Assurance Level 'high' defined 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.

Additionally there is a need for a policy alignment concerning requirements on the interoperability of electronic professional registries as laid down in the JAseHN guidelines.

7) **The eHealth Network shall adopt the Guidelines on Interoperability of Electronic Professional Registries.**

2.5 Semantic Requirements

At the time of the release of this document no semantic requirements are known.

[6] The NCPeH Release 'Wave 1 – Operation Ready' will be published by eHDSI Solution Provider 1st of June 2017.
[7] The inclusion and processing of additional attributes is in the MS responsibility. Nevertheless, to gain an interoperable solution it is recommended that the highest decision making body of the respective domain (eHealth network in case of eHealth) 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. Its use is optional by MS implementing CBeHIS. For more details refer to section 2.6 Technical Requirements

2.6 Technical Requirements

As of today the epSOS specifications and the OpenNCP reference implementation are not ready for eIDAS. As recommended by e-SENS:

> "It is proposed that a thorough review of the OpenNCP reference implementation is performed in the light of the eIDAS Regulation and the tools it provides. The list of issues presented in this document[8], though not exhaustive, is indicative of the breadth of issues that need to be examined."

Technical consequences of eIDAS on CBeHIS have to be analysed in detail and taken into account for the eID framework Release 2. Consequently epSOS specifications and the OpenNCP reference implementation have to be updated accordingly to make the NCPeH ready for CBeHIS provision.

This above identified task also applies to Trust Services, which are not in the scope of JAseHN's T5.2 eID for eHealth. If needed for CBeHIS, Trust Services shall be addressed through new activities as lay out in section

3. Closing remarks.

The current eID eIDAS profile limits itself to the core requirements of eIDAS, while preserving a certain degree of extensibility for the needs of other sectors such as encoding and transporting additional attributes. This allows domains some governance over domain-specific needs, without changing the eID eIDAS profile and its sample implementation called eIDAS-Node. From the eHealth perspective it is currently unclear how feasible and sustainable in the medium/long-term a solution can be which solely relies on the eID eIDAS profile and eIDAS-Node, under use of only additional (optional) attributes.

The eID aspects of the services Patient Summary and ePrescription/eDispensation are addressed in the EU-project e-SENS[9] and there in WP5.2 which is in charge of the eHealth pilot[10]. 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 essentially consolidates the diverging smartcard eID means of different MS into one streamlined solution. QSCD and qualified certificates are also specified and ruled by the eIDAS Regulation and are primarily meant to be used for creation of electronic signatures, and not for authentication. 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. Both solutions are fully compatible and enable seamless identification and authentication of patients and health professionals.

[8] eSENS's WP4 *Implication of eIDAS Regulation for eHealth*

[9] 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).

[10] e-SENS is currently carrying out an eHealth eID Pilot with Austria, Greece, Italy, Portugal and Spain participating in it, which will bring up more detailed results and experiences on technical level. This enhances eID specific framework for eHealth with aspects on readiness and 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 in the first quarter of 2017.

However, any combined approach with eIDAS eID requires the capability to encode and transport an additional attribute[11] patient identifier. This attribute will be added to the eIDAS SAML Assertion outside of the eIDAS minimum data set[12], while the minimum dataset remains unchanged.

The inclusion and processing of additional attributes is in the MS responsibility. Nevertheless, to gain an interoperable solution it is recommended that the highest decision making body of the respective 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.

However, it remains to be the responsibility of the eHealth Network to take the required decision (see recommendation #5) and take together with the European Commission immediate action to ensure that the eIDAS technical subgroup and the eIDAS Cooperation Network will add the patient identifier attribute outside of the eIDAS minimum data set as a domain specific attribute. Its use is optional by MS implementing CBeHIS.

8) **Each Member State participating in CBeHIS shall use the agreed additional attribute(s) for patient identifier in addition to the eIDAS minimum dataset according to 2015/1501/EU if applicable for its national implementation.**
9) **Each Member State participating in CBeHIS shall implement the agreed level of electronic identification and authentication for CBeHIS.**

Each Member State is responsible to set up and maintain electronic register(s) of health professionals according to the adopted guidelines on the interoperability of electronic Professional Registries.

10) **Each Member State participating in CBeHIS shall implement electronic register(s) of health professionals according to the Guidelines on Interoperability of electronic Professional Registries.**
11) **Each Member State participating in CBeHIS shall maintain electronic register(s) of health professionals.**

For an unequivocal identification of healthcare professionals a registration with at least one national healthcare professional organisation or health authority is required. A possibility to check the attributes of the data requester needs to be provided as well.

3. Closing remarks

The present document outlines the first release of the eID specific framework for eHealth and

- lays down the past and current situation on eID in eHealth to build a common understanding,
- gives guidance on identification and authentication for the first wave of eHDSI and
- frames a set of actions necessary for establishing an interoperable eHealth-specific eID solution for CBeHIS.

The proposed eID specific framework for eHealth shall be revised and enhanced as necessary, taking into consideration the lessons learnt and experience gained from the emergence of CBeHIS. A way forward for the revision of the eID framework was proposed and shall be followed to establish interoperable eID measures and implementation in CBeHIS.

[11] No additional attribute is needed for MS that merged the eGovernment and patient identifier into one singular property (such as PT, IT, etc.). Consequently the use of it will remain optional depending on the MS's decision.
[12] Sector specific attributes can be added under 2.7 Sector Specific Attributes of eIDAS SAML Attribute Profile v1.1 and future versions.

In order to successfully create the eID framework in its full version the following tasks were identified by JAseHN and e-SENS along with a proposal who should address those:

- Technical analysis of the NCPeH (epSOS specifications and OpenNCP reference implementation). This task should be carried out by eHDSI Solution Provider. Results are needed in order to provide the Release 2 of the eID framework.
- Economic analysis of eID implementation scenarios (this includes the Deloitte scenarios but is not limited to). This task should be carried out by eHDSI Owner giving further guidance to the eHealth Network and the eHMSEG.
- Results of both analyses need to be incorporated into the eID framework for eHealth Release 2. This is the task of JAseHN T5.2 to be done until November 2017. To meet this deadline the tasks is currently preparing a proposal for subcontracting as discussed in the JAseHN workshop.
- Requirements of eID framework for eHealth Release 2 need to be implemented into epSOS specifications and OpenNCP reference implementation. This task should be carried out by eHDSI Solution Provider and become a part of the March 2018 Release of the epSOS specifications and OpenNCP reference implementation.
- epSOS specifications and OpenNCP reference implementation have to be aligned with eID eIDAS profile and sample implementation called eIDAS-Node especially for but not limited to eID. This task should be carried out by eHDSI Solution Provider in collaboration with DG DIGIT in order to cater for needs of the eHealth domain on eID and consider those in the summer release of the eID eIDAS profile and its sample implementation. This has to be done in alignment with the eIDAS Cooperation Network.
- Requirements concerning Trust Services needs to be addressed for CBeHIS provision. This task should be carried out by eHDSI owner and eHDSI Solution Provider in collaboration with eHMSEG in order to reach an aligned understanding on Trust Services in CBeHIS and agree on the next steps towards the definition of requirements.

4. References

4.1 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)

4.2 Content-related references

- eHealth Network documents
  - Organisational Framework for eHealth National Contact Points (OWA-NCPeH)
  - General Guidelines on electronic exchange of health data under cross-border Directive 2011/24/EU (Release 2)
  - Guideline on Patient Summary for unscheduled care (Release 2)
  - Guideline on ePrescription and eDispensation (Release 2)
  - Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross Border eHealth Information Services (Agreement)
  - eID for eHealth: towards EU governance
  - 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 (final draft available)
- epSOS documents
  - WP3.4 epSOS Common Components Specifications
- NCPeH Release
  - Wave 1 – Release Candidate [W1-RC]
  - Wave 1 – Operation Ready (to be published by 1st June 2017)
- Deloitte eHealth eID Study 'The use of CEF eID in the CEF eHealth DSI' Draft Report V2.0

5. Appendices

5.1 Definitions

CONCEPT	DEFINITION
CBeHIS	The generic services are the necessary implementation of data exchange at country level, the core services at EU level. These together enable the provision of Cross Border eHealth Information Services (CBeHIS).
CEF eHealth DSI	is the initial deployment and operation of services for cross-border health data exchange under the Connecting Europe Facility (CEF). eHDSI sets up and starts deploying the core and generic services, as defined in the CEF, for Patient Summary and ePrescription.
Communication Gateway	MS system that manages CBeHIS transactions with other MS and which connects to the NI. It is an entry/exit point from the MS, acting on behalf of a HP and citizen (at a Point of Care) that assures the exchange of patient's medical data in a controlled environment.
Compliance Establishment Process	A well-defined set of activities and evidences used to ensure that NCPeH compliance can be established, maintained and reinforced
Country A	The country of affiliation. This is the country that holds information about a

	patient, where the patient can be univocally identified and his data may be accessed.
Country B	The country of treatment i.e. where cross-border health care is provided when the patient is seeking care abroad.
eIDAS Cooperation Network	The eIDAS Cooperation Network, which was created by the Commission Decision EU 2015/296 implementing the eIDAS Regulation, is one of the main tools of cooperation between the Member States in the area of electronic identification (eID) in order to achieve interoperability and security of their eID schemes. It provides a forum with regular meetings, where Member States can exchange relevant information, experience and good practice.
eHDSI Owner	eHDSI Owner (DG SANTE Unit B3) is responsible for overall policy planning and coordination for eHDSI (prepare the meetings of the eHealth Network and support its work, and ensure the liaison between the eHealth Network, eHDSI IT governance and various Commission services.
eHDSI Solution Provider	eHDSI Solution Provider (DG SANTE Unit A4) is responsible for the provision of core services (to build the eHDSI specific software and services; advise and assist Member States on setting up the generic services, and ensure that they are linked to the core services (technical and semantic interoperability)). The DSI Solution Provider for Building Block services (eID, eDelivery ...) to the eHealth domain is DG DIGIT (A3, B4).
Framework	Is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful.
Guideline	A suggested way of compliance when doing something. It is visible to those using or supporting the use of a particular service but there are no sanctions if not followed.
Guideline for Adoption	Intended to present to the eHealth Network's members a clear guideline with the intention for it to be adopted and optionally implemented by the EU MS at national level in the next step.
National Infrastructure	The healthcare IT infrastructure, which manages patient and HP/HCP[13] identification and health care records in MS
NCP	National Contact Point as referred in Article 6 of the 2011/24/EU Directive
NCPeH	National Contact Point for eHealth, that may act as an organization and technical gateway for the provision of eHealth Cross-Border Information Services
NCPeH Deployment	Set of activities aiming to evidence the NCPeH compliance with the full range of requirements (LOST) established towards CBeHIS provision
NCPeH Implementation	Process of Prepare, Deploy and Operate a NCPeH
NCPeH Operation	Set of activities performed by the MS while providing the service to the citizens and health professionals
NCPeH	Set of activities aiming to set up an NCPeH

[13] see Article 3 (f) and (g) of Directive 2011/24/EU

Preparation	
Organisational Framework	Define core characteristics, duties and responsibilities of a NCPeH
PoC	A Point of Contact is a location where an EU citizen may seek healthcare services. It can be a hospital, a pharmacy or any other point of the healthcare system of Country B.
Requirement	Definition of relevant needs (business, functional, non-functional, technical and technological) for system specification and implementation