Co-funded by
the Health Programme
of the European Union

JASEHN
Joint Action to Support the eHealth Network

DISCUSSION PAPER

on

Policies Regarding an eID Specific Framework For eHealth

RELEASE 2

Document status:	For discussion by the members of the eHealth Network at their 12th meeting on 28 November 2017
Approved by JAseHN sPSC	Yes
Document Version:	v6.3
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) Sören Bittins, Fraunhofer FOKUS (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, COCIR

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	2016-05-23	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)
3.1	2016-12-12	STRUCTURE OF DOCUMENT CHANGED	BEATRICE STREIT (GEMATIK)
3.2	2016-12-13	STRUCTURE OF DOCUMENT ENHANCED	BEATRICE STREIT (GEMATIK)
3.3	2016-12-14	SCOPE SPECIFIED	BEATRICE STREIT (GEMATIK)
3.4	2017-01-19	OBJECTIVES SPECIFIED	BEATRICE STREIT (GEMATIK)
3.5	2017-01-20	INITIAL CONSIDERATIONS ADDED	BEATRICE STREIT (GEMATIK)
3.8	2017-01-23	ADDING ON REQUIREMENTS SECTION	BEATRICE STREIT (GEMATIK)
4.0	2017-01-24	ADDING ON REQUIREMENTS SECTION	BEATRICE STREIT (GEMATIK)
4.1	2017-02-02	ADDING COMMENTS FROM FINLAND, AND FROM THE JASEHN EID WS	BEATRICE STREIT (GEMATIK)
4.2	2017-02-03	ADDING FROM ESENS AND AGREEMENT	BEATRICE STREIT (GEMATIK)
4.3	2017-02-06	REVISION OF SCOPE AND OBJECTIVE RELEASE 1-2	BEATRICE STREIT (GEMATIK)
4.4	2017-02-07	REVISION OF SCOPE AND OBJECTIVE	BEATRICE STREIT (GEMATIK)
4.5	2017-02-15	REVISION OF EIDAS AND GDPR	BEATRICE STREIT (GEMATIK)
4.6	2017-02-16	REVISION OF INTRODUCTION	BEATRICE STREIT (GEMATIK)
4.7	2017-02-17	ADDING THE WIDER REMIT OF EID IN EHEALTH	BEATRICE STREIT (GEMATIK)
4.8	2017-02-20	ADDING FROM E-SENS JASEHN JOINT	BEATRICE STREIT

		WORKSHOP AND JASEHN T5.2 WORKSHOP	(GEMATIK)
4.9	2017-02-21	REVISION OF GENERAL CONSIDERATIONS, RESPONSIBILITIES AND DUTIES AS WELL AS LEGAL ENVIRONMENT	BEATRICE STREIT (GEMATIK)
5.0	2017-02-22	FINE TUNING	BEATRICE STREIT (GEMATIK)
5.1	2017-03-27	INCORPORATE OF REVIEWER'S COMMENTS	BEATRICE STREIT (GEMATIK)
5.2	2017-03-29	INCORPORATE OF REVIEWER'S COMMENTS	BEATRICE STREIT (GEMATIK)
5.3	2017-04-20	INCORPORATE SPSC'S COMMENTS	BEATRICE STREIT (GEMATIK)
5.4	2017-09-04	INCORPORATE WS RESULTS	BEATRICE STREIT (GEMATIK)
5.5	2017-09-06	INCORPORATE WS RESULTS	SÖREN BITTINS, (FRAUNHOFER FOKUS)
5.6	2017-09-11	INCORPORATE WS RESULTS	SÖREN BITTINS, (FRAUNHOFER FOKUS)
5.7	2017-09-12	REVIEWING AND UPDATING	BEATRICE STREIT (GEMATIK)
5.8	2017.09-25	DOCUMENT REFINEMENT,	SÖREN BITTINS (FRAUNHOFER FOKUS)
5.9	2017-09-27	FINAL REVISION FOR 1ST SPSC REVIEW	SÖREN BITTINS (FRAUNHOFER FOKUS) JÜRGEN WEHNERT (GEMATIK)
5.9	2017-09-29	WP3 QUALITY CHECK	RADU PIRLOG (BBU), ANDREEA MARCU (BBU)
6.0	2017-10-12	INCORPORATING COMMENTS RECEIVED	BEATRICE STREIT (GEMATIK)
6.1	2017-10-20	FINAL REVISION FOR 2ND SPSC REVIEW	BEATRICE STREIT (GEMATIK), SÖREN BITTINS (FRAUNHOFER FOKUS)
6.2	2017-11-08	INCORPORATING SPSC COMMENTS	BEATRICE STREIT (GEMATIK)
6.3	2017-11-09	WP3 QUALITY CHECK	RADU PIRLOG (BBU), ANDREEA MARCU (BBU)

LIST OF ABBREVIATIONS

ACRONYM	DEFINITION
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); FOR EASIER IDENTIFICATION IN THE TEXT WRITTEN IN ITALICS: "*Agreement*"
CBeHIS	CROSS BORDER EHEALTH INFORMATION SERVICES
CEF	CONNECTING EUROPE FACILITY
DSI	DIGITAL SERVICE INFRASTRUCTURE
EC	EUROPEAN COMMISSION
eHDSI	EHEALTH DIGITAL SERVICES INFRASTRUCTURE
eIDAS	ELECTRONIC IDENTIFICATION AND TRUST SERVICES
eIDAS Regulation	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
eHN	EHEALTH NETWORK
EIF	EUROPEAN INTEROPERABILITY FRAMEWORK
eD	ELECTRONIC DISPENSATION
eP	ELECTRONIC PRESCRIPTION
EU	EUROPEAN UNION
ERN	EUROPEAN REFERENCE NETWORK
GDRP	GENERAL DATA PROTECTION REGULATION
HCP	HEALTHCARE PROVIDER
HP	HEALTH PROFESSIONAL
IOP	INTEROPERABILITY
JAseHN	JOINT ACTION FOR SUPPORT THE EHN
LOST	LEGAL, ORGANISATIONAL, SEMANTIC, TECHNICAL
MLA	SEE "AGREEMENT"
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 POINTS
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 eHealth Network (eHN) 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 to allow it to grow and persist 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). Cross-Border eHealth Information Services that are processed via NCPeH for the purpose of cross-border healthcare, as they were agreed by the eHN (Patient Summary for unscheduled care; ePrescriptions and eDispensations) and as they will be agreed by the eHN in the future

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 this eID framework was done in two steps, which correspond to two releases. This document addresses the second 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 (OFW-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*) adopted by eHealth Network and to be signed by the competent national authorities.
- Policy Paper on the Interoperability of Registries for Healthcare Professionals to be adopted by the eHealth Network
- e-SENS' T5.2 and eHealth eID Pilot through several Joint Workshops
- e-SENS' WP4 Implication of eIDAS Regulation for eHealth[1]
- Technical Delta Analysis on eID and related topics[2]

[1] 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 e-SENS 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 REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation). In short and only if applicable the eID framework will take into account trust services as a subordinate 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. It shows the boundaries of eID without limiting the scope of technical options.

The eID framework Release 2 not only considers and thus applies to the Patient Summary (PS) and ePrescription/eDispensation (eP/eD) use cases, but remains open for future use cases for CBeHIS, e.g. European Reference Networks (ERNs). However, specific adaptions of the framework may be necessary at a later time.

1.3 Objectives

Based on the eID framework Release 1, which was adopted by the eHealth Network in May 2017, the second release:

- lays down the past and current situation on eID in eHealth to build a common understanding,
- 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.

[2] Input document for the JAseHN T5.2 eID workshops on the 22nd and 23rd August 2017 in Berlin, which was subsequently updated with the results of discussions in the workshops and comments received.
[3] This release is the basis for going live in February 2019 (second wave of CEF eHealth).

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 addresses the Preparation and Deployment Phase as well as the Operation Phase.

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

2. Executive Summary

The eHealth Network Members are asked to discuss the following recommendations:

- The eHealth Network shall adopt that from the second wave of eHDSI on (to go live in February 2019) 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[4].
- The eHealth Network shall adopt common additional attributes[5] for a patient identifier in addition to the eIDAS minimum dataset according to 2015/1501/EU.
  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.
- The eHealth Network shall adopt an agreed level of electronic identification and authentication for CBeHIS. The use of eIDAS eID notwithstanding, this level shall correlate to the equivalent of the eIDAS Authentication Assurance Level "high".
- Each Member State participating in CBeHIS shall document and publish a list of necessary attribute(s), in particular regarding the health professional authentication, required to assure the proper functioning of the access control systems of their national implementation.

In order to successfully implement the eID framework by establishing interoperable eID measures and implementation in CBeHIS the following tasks were identified:

[4] The Agreement applies from the first wave on, yet the eID related aspects apply from the second wave eID on.
[5] For more details refer to section 3.6 Technical Considerations

- An analysis of the impact of the GDPR on the eHDSI and the implementable artefact OpenNCP needs to be performed urgently to assure full compliance with the GDPR assuming full effect in May 2018.
- Requirements of the *eID specific framework for eHealth, Release 2* (the document at hand) need to be implemented into eHDSI 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 eHDSI specifications and OpenNCP reference implementation.
- eHDSI 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 for summer 2018 expected 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 need 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.

3. 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 ReEIF complemented by additional sections where needed.

3.1 The wider remit of eHealth eID

Regulation 910/2014/EU 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 DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Community framework for electronic signatures (e-signature Directive) 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 a transition period until September 2018 applies.

As of today, some Member States have initiated the notification process with one[6] country having passed notification for two national eID Schemes to date. 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.

At that time the epSOS pilot was implemented and operated the eIDAS regulation was not yet in place. Instead the e-signature Directive 1999/93/EC applied and was hence taken into account by the epSOS specifications and OpenNCP reference implementation. Since 910/2014/EU repeals 1999/93/EC, a thorough regulatory alignment is required, and – as a subsequent step - an update reflecting the new requirements and technical solutions of specifications is required. The eHDSI Solution Provider is in charge of the specification update and is currently transposing the old epSOS specifications into a new set of eHDSI Interoperability specifications. Additionally, external projects, such as the e-SENS project - are also motivating further changes to the new set of interoperability specifications in order to maintain, align, and evolve the specifications' applicability and to support further activities, e.g. for piloting purposes such as the e-SENS eHealth eID pilot.

An eHealth eID Study was meant to 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 produced by a Deloitte team in cooperation with DG DIGIT. 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 were identified and described. eID of Health Professionals (HPs) was out of scope. A final draft version of the Deloitte Study on eID in eHealth was shared in November, 2016; it has since been revised and now includes additional MSs' experience: 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.

Above mentioned scenarios draw on the very specific scenarios implemented by the e-SENS eID eHealth Pilot under the vast restrictions on resource and time 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

[6] Opinion No. 1/2017 of the Cooperation Network on the German eID scheme, accessible at https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=48762259

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.

Furthermore, while the applicability of eIDAS eID in reference to the authentication of natural persons is generally agreed upon, a large degree of predominantly legal uncertainty remains on the legal compulsion of eIDAS eID in reference to a natural person in the functional role of a "patient" as well as a health professional acting as a legal person. The legal *Agreement* currently only mitigates specific applicability concerns by constraining the mandatory application of eIDAS eID to only Member States in which eIDAS eID is found to be "*applicable to the health domain*". This approach may bear the danger of solidifying an eHDSI of the two speeds and warranties, in which some Member State operate under the strict legal responsibilities and assurances of eIDAS eID while others rely on purely national means without a commonly agreed and verifiable level of assurance regarding the authentication of participants.

Further complication and a fair degree of confusion also stems from eIDAS eID being an authentication framework for both natural and legal persons. However, since the issuance of an eID SAML Assertion requires a notified national eID Scheme, many Member States only explored how natural persons may be authenticated using their regular eID means, such as an electronic identity card. To date, no notified, pre-notified or planned for notification eID Scheme for *legal* persons is known. Additionally, the Minimum Data Set for legal persons is entirely targeted at presenting a business entity towards authorities and consumers, however, it cannot express the functional[7] or structural roles the eHealth domain requires. The electronic identification of legal persons through eIDAS eID would therefore need a capable national eID Scheme to be notified as well as the same extensions regarding further attributes that the identification of a patient requires. However, in contrast to the optional attribute of the patient identifier within the authentication of a natural person, the additional attributes for legal persons do not only carry an authentication, but in particular the expression of a structural role effectively states an authorisation. While a precedent for mixing the authentication and authorisation exists through the health professional authentication by STORK 2.0, eIDAS eID so far has not formally adopted a similar approach, nor has it prepared any of the legal and technical facilitators to actually enable such a functional authorisation.

Alternatively, eIDAS eID provides a technical mechanism and legal framework to establish a temporary "*Binding between the electronic identification means of natural and legal persons*[8]". This enables a natural person to act as a legal person, being capable of delegating that structural responsibility to other legal persons; yet it does not address the challenges regarding the eID Scheme to be used nor how the actual structural role is to be expressed within the eIDAS eID SAML Assertion[9].

[7] The terms functional and structural roles are used in adherence to the HL7 Role Engineering Process in order to properly capture and reflect the requirements of the eHealth domain.
[8] according to Annex 2.1.4 of the Commission Implementing Regulation (EU) 2015/1502
[9] For more details refer to section 3.6 Technical Considerations

Consequently, and despite the technical capability to do so, eIDAS eID currently does not appear to be a suitable candidate for electronic identification outside the realm of natural persons for the eHealth domain. Mitigating factors such as the inclusion of domain-specific optional attributes or bindings between natural and legal persons' eID exist but may impose entirely new critical legal challenges.

With the inception of eIDAS and its trust services, the provisions of the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCILof 27 April 2016 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 - commonly and hereinafter referred to as General Data Protection Regulation (GDRP) - will also take full force upon the eHDSI in general. Although the topic at hand, specifically and narrowly scoped to eID, is only partially affected by the GDPR, many of the legal implications are applied by proxy. Instead of being entirely legitimated by an informed consent of a typical voluntary application, eIDAS eID brings and relies upon its very own regulatory framework and technical specifications. Consequently, many of the regulations within the GDPR do not immediately apply to eIDAS eID itself but to the subsequent systems that integrate eIDAS eID as a solution component.

For instance, in adherence to Article 35 of the GDRP, a data protection impact assessment is not to be done for eIDAS eID itself but for the application that relies on eIDAS eID to authenticate their system participants. Therefore, the duty of providing such an assessment for any "*type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*" may fall on the eHDSI or the participating Member States. However, for the eHDSI to rely on eIDAS eID is not only a challenge or even a threat but may also massively simplify the data protection assessment and certification made mandatory through Article 35 of the GDPR if a "*processing on a large scale of special categories of data referred to in Article 9(1)*" actually takes place. eIDAS eID as a legally imposed service with its own legal framework may assist not only towards any potentially required assessment as a "*due diligence*" safeguard according to Article 25 and 32 but also as a risk mitigation, aversion, and minimisation strategy by providing a self-accreditation as an "*approved certification mechanism*" according to Article 42 of the GDPR.

Regardless of the aforementioned considerations and outside the scope of eID an impact analysis of the GDPR onto the eHDSI and the implementable artefact OpenNCP needs to be performed urgently to assure full compliance with the GDPR assuming full effect in May 2018.

3.2 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 evaluate 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 for online services 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; due to the necessary rechecking and implementing processes in MS this would 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.**
- Some critical future considerations have been omitted from this framework due to currently unclear enforcement obligation. Namely, the implications of Article 25, 32, and 83 of the GDPR can only be referenced at the appropriate places within this framework but cannot be assessed towards their complete impact on the eHDSI. Another noteworthy omission is the implication of the Directive on security of network and information systems (NIS Directive).
- 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 June or July 2018) will operate without electronic identification. Patients and HPs will be identified and authenticated as described in the epSOS use cases of PS and eP/eD[10]. For the second wave (go live in February 2019) and

[10] Further details are laid out in the original epSOS Common Components Specifications (see http://www.epsos.eu/uploads/tx_epsosfileshare/D3.4.2_epSOS_Common_Components_Specification_01.pdf) but are superseded by 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).

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 for CBeHIS. 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 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 health providers (HP) 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).

- eIDAS eID and its ancillary trust services are predominantly designed towards the authentication of natural persons. The eHDSI may greatly benefit from the legal stability as well as technical interoperability of eIDAS eID. However, one should not rely on the technical interoperability of eIDAS eID as being a complete and self-contained solution for all eHDSI requirements. In particular the authentication of health professionals and the providence of additional identity attributes (namely any attributes that exceed the mandatory Minimum Data Set[11] of eIDAS but which are required for the proper functioning of the eHDSI use cases) requires further work by the eHealth domain[12].

3.3 Legal Environment

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

The main foundation of the eID specific framework for eHealth is the eIDAS Regulation and the GDRP, which applies to several domains, not specifically to eHealth. Additionally, 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*) needs to be taken into account. The eIDAS Regulation and the GDRP is directly applicable to all Member States regardless of whether they participate in CBeHIS or not. The *Agreement* shall be signed by MS which participate in CBeHIS or intend to do so.

The following 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

[11] According to Annex I of the Commission Implementing Regulation (EU) 2015/1501 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[12] For more details refer to section 3.4 Organisational and Policy Requirements

regulation). However, the recognition of notified eID schemes is mandatory from September 2018 on for online services.

- 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 GDRP shall 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 only 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.
- eIDAS eID is the most prominent function of the eIDAS regulation, however, it only deals with the authentication of natural and legal persons. Further functionality and means for electronic identification, such as end-entity authentication for systems and digital services, are not governed by eIDAS eID, but by the eIDAS trust 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 Regulation explicitly state that the domain eHealth has been taken into consideration. The eIDAS regulation applies to cross-border patient data exchange with online-services such as PS and/or eP 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.

The GDRP makes 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*) lays down legal boundaries for the CBeHIS provision on the grounds of the eIDAS regulation and several other applicable laws. The *Agreement* was adopted by the eHealth Network in May 2017 and is to be signed by the competent national authorities intending to join the CBeHIS after receiving the opinion of the Art. 29 Working Party.

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 for CBeHIS. 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 when acting as country A or B.

The legal foundation of the eID specific framework for eHealth consists of the eIDAS regulation, the GDPR and the *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 for online services 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 PS and eP/eD use cases of CEF eHealth. The new eIDAS regulation differs substantially from 1999/93/EC and has already forced a preliminary update of the specifications governing the processing of digital certificates and electronic signatures. This update is, however, only capable of providing a temporary foundation for Wave1 and 2 of the eHDSI. Therefore, the new regulation and its impact is to be analysed more thoroughly and further actions for implementations need to be initiated.
- The *Agreement* prepared by the T6.2 of JAseHN refers to provisions of the eIDAS Regulation and GDPR (*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.
- Further relevant legislative acts may also apply and impose additional requirements on the electronic identification facilities, such as the Directive 2011/24/EU in Article 11 (2) through the potential need of encoding, transporting, and processing enforceable authentication and authorisation statements across borders.

3.4 Organisational and Policy Requirements

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

The *Agreement* lays down the eHealth specific rules for cross-border patient data exchange with online-services such as PS and/or eP. For CBeHIS implementation the following two

requirements concerning the *Agreement* shall be fulfilled, which were already laid down in the *eID specific framework for eHealth Release 1*:

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*).**

Building on that, the following recommendation especially addresses the second wave of eHDSI in relation to identification and authentication of patients and HPs.

3) **The eHealth Network shall adopt that from the second wave of eHDSI on (go live in February 2019) 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[13].**

For cross-border purposes, a unique patient identifier at national level is a necessary requirement for each individual patient to be linked to their 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 authentication assurance levels (eIDAS AAL) 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."

Special notice shall be placed on the proper identification and authentication of health professional, especially in the cross-border context. The current *Agreement* mandates every Member State participating as a country-B in CBeHIS to properly authenticate its health professionals and to perform an a-priori validation of their credentials and the explicit authorisation to perform specific tasks in healthcare. The *Agreement*, however, does not impose any requirements on country-B to communicate the result of those assurances to country-A in any specific form, for instance the identifier being unique across borders or that the authorisation can be verified independently across borders.

In practice, and in absence of further regulation or imposition of responsibilities, the technical implementation of the eHDSI merely assumes that the respective country-B has fulfilled its obligations completely. There is only an Audit Trail documenting the provided attributes of the

[13] The Agreement applies from the first wave on, yet the eID related aspects apply from the second wave eID on.

foreign HP. This information is extracted from the values encoded within the Identity Assertion (IdA) and its correctness and stability is signified by the NCPeH-B applying its electronic signature to the assertion:

- an identifier of the referenced health professional
- the role of the health professional in reference to, expressed as "medical doctor"
- the entitlements of that role in country-B's jurisdiction, expressed by using the HL7 role engineering catalogue vocabulary (permissions)

Through the definition of the role, country-A may indirectly derive the qualification as a health professional as country-B would violate their obligation to regulate admission to the CBeHIS if this role is assigned improperly. The providence of the entitlements in country-B's jurisdiction states the currently activated permissions of this health professional, while the identifier in combination with the issuing country enables some degree of traceability. However, in the light of providing routine health service across borders, those assurances from country-B to country-A may be too coarse. Taking Recital 52 of 2011/24/EU as an example, the requirement "The Member State of affiliation may need to receive confirmation that the cross-border healthcare will be, or has been, delivered by a legally practising health professional." imposes a need for a multi-dimensional entitlement of a health professional while the implementation of the eHDSI may currently only provide an unsubstantiated statement of the requestor being a qualified health professional.

Consequently, country-B needs to encode and transport at least the following information to country-A in order for the latter to fulfil its obligations towards patient consent and access control prior to the disclosure of senstive of personal information, specifically that a HP in country-B is indeed:

1. qualified as a health professional,
2. authorised to exercise "*activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment*", and
3. entitled to perform a very specific activity, such as "*prescription was issued in another Member State by a member of a regulated health profession who is legally entitled to do so*" or to request information about a foreign patient across borders

In conjunction with the *Agreement* and the Audit Trail, country-A may be capable of documenting a good-faith decision regarding the exchange of clinical information. However, especially in the light of the GDPR Article 5, 25, 32, and 7 and with the indisputable availability of technology that can make those statements explicit, the health professional authentication needs to be updated to adhere to at least the current state-of-the art.

Consequently, and the operation of registries for health professionals notwithstanding, an explicit, traceable, and cross-border authentication of health professionals must be performed and enforced for all cross-border eHDSI applications.

4) **The eHealth Network shall adopt common additional attributes[14] for a patient identifier in addition to the eIDAS minimum dataset according to 2015/1501/EU.**

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.

Injecting the authoritative, cross-border patient identifier into an eIDAS SAML Assertion alongside with the eIDAS Minimum Data Set and the assertions signature greatly increases the recognition, legal stability, and interoperability of the eHDSI patient authentication. Furthermore, the to-be applied protection demands of the Treatment Relationship Confirmation Assertion – currently the only technical artefact carrying the patient identification from country-B to country-A – are significantly lowered and the information contained in the eIDAS SAML Assertion becomes entirely enforceable. The decoupling of the eHDSI security infrastructure and eIDAS eID as a separate service reassigns the obligation for subject confirmation (patient authentication) from the eHDSI to the respective national competent authority while being able of preserving the specific domain need for securely transporting additional information (patient identifier) with positive implications to Article 5, 9, 25, and 32 of the GDPR. Using injected patient identifiers also removes the need for the IHE Cross-Community Patient Discovery Profile and its transactions from the eHDSI.

Member States participating in CBeHIS, however, may only be mandated to operate eIDAS-compliant services to the extent of the eIDAS regulation itself. Consequently, the injection of an additional attribute is a voluntary extension of the eIDAS service and may be discarded or discontinued at any point in time in favour of disclosing only the eIDAS Minimum Data Set within the eIDAS SAML Assertion. Both approaches can be operated simultaneously within the eHDSI with no immediate functional restrictions, however, relying on the eIDAS Minimun Data Set only requires additional national backend services, additional facilities to maintain the security context over separate services, as well as additional transactions in the eHDSI.

The decision towards the adoption of common patient identifiers in conjunction with the eIDAS Minimum Data Set shall be taken without implying or mandating the use of explicit technology in order to preserve the freedom and flexibility of the Member States regarding the implementation and operation of their national health infrastructure. Consequently, the relevant bodies need to be tasked with designing a specification that enables the full activation of eIDAS

[14] For more details refer to section 3.6 Technical Considerations

eID and trust services for one MS while accommodating MS that select equivalent means towards eID. For instance, while one Member State may choose to inject the cross-border patient identifier attribute alongside with the Minimum Data Set into an eIDAS eID SAML Assertion, another Member State may prefer to only communicate the Minimum Data Set in the eIDAS SAML Assertion. Both approaches adhere to the eIDAS regulation, its technical specifications, and provide an equivalent level of authentication assurance. However, the second example requires an additional patient matching service in country-A and the continued operation of the eHDSI Patient Identification Service in country-B.

The level of authentication assurance appropriate for eHealth shall be strict enough to fully protect medical data exchange (article 12 §3 and §7 of eIDAS Regulation). Only the highest authentication assurance level of eIDAS matches the requirements to securely exchange sensitive medical data across-borders.

5) **The eHealth Network shall adopt an agreed level of electronic identification and authentication for CBeHIS. The use of eIDAS eID notwithstanding, this level shall correlate to the equivalent of the eIDAS Authentication Assurance Level "high".**

3.5 Semantic Requirements

Depending on the decision towards the professional registries, some technical artefacts on electronic identification would benefit from inclusion in the semantic facilities of the eHDSI. Especially the authentication of the health professional, in particular but not limited to their explicit functional role, HP specialty, and health professional organisation facility type, are very useful candidates for further processing in country-A. However, those attributes are exclusively derived and issued within the realm of the national infrastructure in country-B and no further requirements are imposed to assure their cross-border interoperability. Consequently, country-A may not necessarily rely on a sufficiently high degree of expressiveness and robustness for its own processing, for instance to process those attributes in a security context to make an informed access control decision. That would significantly exceed the obligations of country-B towards the collection and encoding of those attributes beyond warranting the internal HP authentication and authorisation as stated in the *Agreement*.

Therefore, it is recommended to also explicitly assign semantic responsibility for the structural eID attributes to either:

- a future initiative within the scope of the Registries as part of their mutually agreed and commonly applicable controlled vocabulary for the eHealth domain; **or**
- to mitigate the registries absence for wave 2 the latest by extending the MVC and potentially MTC by the required values.

6) **Each Member State participating in CBeHIS shall document and publish a list of necessary attribute(s), in particular regarding the health professional authentication, required to assure the proper functioning of the access control systems of their national implementation.**

3.6 Technical Considerations

The current evolution of the OpenNCP as implementation artefact of the eHDSI specifications as well as the specifications itself are considered to be not well prepared to support the new requirements on electronic identification imposed by eIDAS. It is also not capable of documenting and asserting some of the certification requirements from the GDPR. However, constant maintenance of the OpenNCP by the eHDSI Solution Provider as well as work performed by external contributors, such as the e-SENS project, are addressing specific technology gaps in a punctual fashion.

Other externally imposed requirements, such as the implementation and operation of TESTA-ng as a substitute for the NCP-to-NCP IPSec Virtual Private Network (VPN) have been found to have no immediate impact on eID.

Regardless of the strategy and attempt to re-use some of the existing functionality, the current eHDSI specifications need to be evaluated and updated urgently to assure correct coping with the newly imposed requirements and a sufficient degree of flexibility towards supporting even more new functionality. Consequently, and as also 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*[15]*, though not exhaustive, is indicative of the breadth of issues that need to be examined.*"

This analysis and evaluation needs to generate tangible results for the technical implementation of eID requirements with a particular emphasis on Regulation 910/2014/EU (including ancillary trust services), Regulation 2016/679/EU (in particular Art. 9, 20, 25, 32, 33, 35, and 83), and Directive 2011/24/EU.

On eIDAS, the technical consequences on CBeHIS have to be analysed in detail and taken into account for the eID framework Release 3. Consequently, the eHDSI 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 entirely within the scope of JAseHN's T5.2 eID for eHealth. If needed for CBeHIS, Trust Services shall be addressed through new activities as laid out in section 4. Closing remarks.

Some preliminary work, including the provision of new specifications, digital services, and demonstrators, has already been performed and is available to JAseHN as well as the eHDSI Solution Provider. For instance, various eID aspects of the services PS and eP/eD were

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

specifically addressed in the EU-project e-SENS[16] through the eHealth pilot[17]. 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.

However, any combined approach with eIDAS eID requires the capability to encode and transport an additional attribute[18] patient identifier. This attribute will be added to the eIDAS SAML Assertion in addition to the eIDAS minimum data set[19], while the minimum dataset remains unchanged.

Furthermore, the potential solution of injecting additional attributes into the eIDAS SAML Assertion does indeed raise the need to reconfigure the national implementation of the eIDAS Node in country-A as well as extending the functionality of the eIDAS Connector in country-B. However, since all attributes exceeding the contents of the eIDAS Minimum Data Set are considered optional, Member States are entirely free in their decision to choose or discard this possible solution, which may raise the operational costs of the eHDSI in practice. Both options are fully compliant with the eIDAS regulation and offer an identical extrinsic Authentication Assurance Level. While the specific requirements on the identification, authentication, as well as authorisation of health professionals are fairly stable by now (also refer to *Policy Paper on the Interoperability of Registries for Healthcare Professionals* for details), the technology at the current point in time is not. For instance, eIDAS eID is technically capable of supporting the needs of CBeHIS regarding health professionals, however, most participating Member States are not and direct their available resources at providing strong electronic identification and authentication means of citizens as natural persons. This yields in the critical issue of not being able to notify the required national eID Schemes as fundamental authentication means for health professionals – or in summary – we would only be able to authenticate a health professional as a citizen

[16] The aim of the e-SENS project was 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, aimed 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).

[17] e-SENS has carried out an eHealth eID Pilot with Austria, Greece, Italy, Portugal and Spain participating in it, which brought up more detailed results and experiences on technical level.

[18] 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.

[19] Sector specific attributes can be added under 2.7 Sector Specific Attributes of eIDAS SAML Attribute Profile v1.1 and future versions.

through the notified citizen eID of the MS but not specifically as a HP through the existing national means. Also considering that many national eID Schemes for Health Professionals are – despite of being considered as very secure in their operation – either not suited for immediate notification or fail to justify the burden of notification towards the expected benefit of providing cross-border HP authentication.

Other candidate technology for HP authentication outside of eIDAS eID is available but may require an additional thorough regulatory evaluation. One possible candidate can be EU Login, formerly known as the European Union Authentication Service (ECAS). EU Login is a federated authentication framework, which is capable of generating an interoperable, secure, and traceable cross-border HP authentication by federating the established national eID system for HP authentication. No further requirements, such as a need for notification of the underlying eID Scheme, are imposed. However, this (and other regulatory issues) may limit the highest achievable Authentication Assurance Level (AAL) to the equivalent of eIDAS' "substantial". Backed by a suitable contractual framework, for instance the *Agreement*, in conjunction with an existing national certification of the existing eID Scheme (to adhere to Article 25 GDPR), and in conjunction with EU Login/ECAS already being used within the eHDSI, this might be an acceptable migration path until eIDAS eID with its robust legal framework is available for all participants.

Any technical solution towards HP eID needs suitable attribute providers to preserve technical and semantic interoperability as well as to generate warranties that the subject of the authentication is indeed a qualified, authorized, and entitled health professional as outlined in *Policy Paper on the Interoperability of Registries for Healthcare Professionals*.

4. Closing remarks

The present document outlines the second 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,
- adds concrete measures and requirements to be included in the eHDSI specifications for March 2018 Release[20] and
- sets up sustainable principles and requirements for an interoperable eHealth-specific eID solution for CBeHIS.

The 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.

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

In order to successfully implement the eID framework by establishing interoperable eID measures and implementation in CBeHIS the following tasks were identified:

- An impact analysis of the GDPR onto the eHDSI and the implementable artefact OpenNCP needs to be performed urgently to assure full compliance with the GDPR assuming full effect in May 2018.
- Requirements of *eID specific framework for eHealth, Release 2* (the document at hand) need to be implemented into eHDSI 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 eHDSI specifications and OpenNCP reference implementation.
- eHDSI 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.

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

- 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 specific framework for eHealth Release 1
  - Policy Paper on the Interoperability of Registries for Healthcare Professionals
  - 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
- Technical Delta Analysis on eID and related topics V0.6

6. Appendices

6.1 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[21] 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 Preparing, Deploying and Operating a NCPeH
NCPeH Operation	Set of activities performed by the MS while providing the service to the citizens and health professionals
NCPeH Preparation	Set of activities aiming to set up an NCPeH
Organisational Framework	Define core characteristics, duties and responsibilities of an NCPeH

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

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