HEALTHeID

eIDAS – OpenNCP
Connector for eHealth

D1.1. HEALTHeID Vision

Document Information:

Document status:	Final
Document Version:	1.0
Author(s):	Zoi Kolitsi , George Pangalos, Andrew Short (AUTH) Andrea Artzeni, POLITO (Italy)
Member State Contributor(s):	SPMS (Portugal), POLITO (Italy)
Stakeholder Contributor(s):	Petra Wilson, External Expert

TABLE OF CONTENTS

Table of revisions		
Date	Comments	Authors
05-05-2018	Discussion paper on vision and implementation choices	Zoi Kolitsi, George Pangalos
10-05-2018	Implementation of comments following first discussion	Zoi Kolitsi, Andrea Artzeni
17-06-2018	Second draft of discussion paper for discussion in Lisbon f2f	Zoi Kolitsi
24.10.2018	First draft of D1.1. circulated to T1.1 team and expternal expert	Zoi Kolitsi
31.10.2018	Second Draft of D1.1. completed following discussions under T1.2.	Zoi Kolitsi
26.11.2018	Comments by Petra Wilson incoprorated	Zoi Kolitsi
06.12.2018	Editorial review by Alberto Zanni and Patient Consent Annex incorporated	Zoi Kolitsi

Bibliography		
Id	Document title	Authors
	Grant Agreement	

1. Introduction to this document

This document presents the HEALTHeID vision, for citizen identification and authentication in cross border eHealth situations and it is been elaborated under Activity 1 of HEALTHeID.

HEALTHeID aims at developing, testing and delivering to the European Commission (EC) and the Member States (MSs) a reference implementation of an eID Connector, in a Technology Readiness Level (TRL) 7 environment, linking the national OpenNCP-based National Contact Points for eHealth (NCPeH) to the eIDAS node and the relevant attribute providers. What will be pursued is that this implementation will be transferable to other national scenarios. Alignment, both technical and timewise with the deployment of the eIDAS nodes of the core countries will be maximized. Collaboration with DG SANTE, DG DIGIT and DG CONNECT will be sought.

All the resulting eID solution components will be made available as Open Source Software to the eHDSI owner and the National Contact Points for eHealth. These, as well as additional modifications needed to the current Open NCP implementation, will be described in a change proposal and will be submitted to the eHDSI owner.

Activity 1, focuses on the identification of non-functional requirements (nFR), covering policy, organizational and legal aspects, as well as usability guidelines for the eID solution components resulting from the action. This document has been produced under Task 1.1: “Non-functional Requirements” and has explored a number of issues and possible solutions that have been identified as outstanding challenges of eID in eHealth, in order to arrive at the HEALTHeID Vision. The solutions explored are focused on supporting the current deployment of the eHDSI but are not strictly framed by it. In fact , as set out in the Grant Agreement, “*it is expected that the Action will provide a longer-term perspective for mutual trust, by supporting a progressive alignment of the cross-border eHealth infrastructure to the eIDAS Regulation …*”.

The exploration on the topic of electronic identification and authentication is not new. It was first addressed in the epSOS Large Scale Pilot (LSP), with a view to providing a practical solution to running the LSP. The co-operation with STORK at that time through the STEPS initiative did not come to fruition of a realistic approach, mainly because the scenarios explored by STORK did not resonate with the on-site presence of the patient and the cross border transmission of patient identifiers submitted by the health care professional, on behalf of the patient. As a result, epSOS did not address the issue of electronic identification, not least in the spirit of the eIDAS Regulation.

There were however several explorations on the topic of electronic identification and authentication for cross border eHealth, of which the first one is consolidated in the CALLIOPE Roadmap[1] articulating a set of recommendations for action at EU and MS level. While many of these

[1] European eHealth Interoperability Roadmap, December 2010

recommendations, concerning a European framework for eID management are now answered by by the eIDAS Regulation, the CALLIOPE recommendation for joint action remains current: "*In order to support these initiatives, the EU eHealth High Level Group*[2], *together with the European Commission, should consider the requirements of EU level governance in the form of regulatory provisions and a mechanism to sustain the European cooperation for cross-border eID management for healthcare purposes."*

In the absence of an enabling EU legal framework in the period 2010-2013, the follow up eHGI project engaged in an in depth analyisis of the issues that are specific for eHealth and supported policy discussions, including on technical solutions[3]. The eHealth pilot of eSENS was the first real attempt to deliver eIDAS based solutions of eID for eHealth and experimented with solutions that could be minimally invasive with respect to the current implementastion of the core and generic services of the eHealth DSI. At the same time, an exploration undertaken by the Legal Expertise Center of eSENS resulted in the (internal) document titled "eIDAS implications for eHealth". The lessons learned from eSENS experimentation are discussed in more detail in Section 3 of this document. This work in eSENS informed also the drafting of the relevant policy documents on the topic within JAeSHN over the period 2014- 2017.

On this back ground, this documentis structured in the following way:

Section 2 provides an account of the current legal and policy drivers and constraints within which the Vision for HEALTHeID and the part of it that will be technically implemented within this project will be developed.

Section 3 presents the major barriers to presenting an eIDAS compliant solution as part of the eHealth pilot in eSENS.

Section 4 discusses the policy and legal directions and constraints and based on these draws a number of non functional requirements that should drive the HEALTHeID implementation choices and plan.ir

Section 5 proposes the long term vision for HEALTHeID and proposes a number of criteria for assessing implementation choices in HEALTHeID.

[2] this group has now evolved into the eHealth Network

[3] eHGI, D8.1: Technical background of eID solutions, March 2012

2. Legal and Policy Context

The main legal foundation of the eID specific framework for eHealth rests upon two Regulations: the eIDAS Regulation[4] and the GDPR, General Data Protection Regulation[5]. Both are general Regulations, i.e. they apply uniformly to all sectors of the digital society and they collectively aim to provide sufficient legal certainty to enable the Digital Single Market. Directive 2011/24/EU provides the legal basis for policy co-ordination by the eHealth Network on eID aspects related to eHealth, while the recent EC Communication on enabling the digital transformation of health and care in the Digital Single Market outlines actions to be taken by the EC and the MS towards implementing the relevant priorities set out in the Digital Market Strategy. More specifically:

1 eIDAS Regulation

The eIDAS Regulation enables the use of electronic identification means and trust services (i.e. electronic signatures, electronic seals, time stamping, registered electronic delivery and website authentication) by citizens, businesses and public administrations to access on-line services or manage electronic transactions. Importantly, it ensures that appropriate eID can have the same legal value as wet signature in cross border transactions and makes mutual recognition of electronic identities (eIDs) mandatory from fall-2018

The Regulation is a self-contained legal framework in its own, in other words it contains all elements that are necessary to create the needed legal certainty for citizens and digital service providers in cross border encounters.

The eIDAS Regulation, consistent with cross cutting policies, promotes a paradigm where the citizens/patients may identify and authenticate themselves using their national eID credentials via a trust network of national eIDAS nodes; once robustly identified and authenticated, the citizen may access cross border on-line services and manage and control access to own personal documents and data, including health data.

It is important to clarify that

- Notification of national eID schemes is done on a voluntary basis. It is entirely up to the Member States to decide if and which national eID system(s) will be notified to the EC; however, the recognition of eID schemes as of September 2018, is mandatory for citizens of a MS for accessing online cross border services.
- The eIDAS Regulation distinguishes between three Authentication Assurance Levels (AAL

[4] Regulation (EU) No 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 and repealing Directive 1999/93/EC

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 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

"low", "substantial" and "high"), which may be applicable to cross border access to services, depending on the nature of the service and the sensitivity of the information being exchanged. Notified national schemes with an AAL "substantial" or "high" must be recognised by other MS.

2 General Data Protection Regulation (GDPR)

The GDPR is applicable to HEALTHeID, to the extent that the chosen HEALTHeID approach may impact the lawful basis for data processing, which is based on the data subject's consent to the processing of personal data for one or more specific purposes. The Consent must be specific and informed and given with a clear affirmative action(Article 7; defined in Article 4).; when consent concerns health data it must also be explicit (Article 9)It should be noted that consent for children may be given by the child's parent or custodian, but that a variation exists across the MS as to the age from which a person under 16 may consent fro themselves (ranging from 13-16).

It should also noted that identification data is itself personal information and is as such subject to the GDPR.

Digital Market Strategy and Digital Transformation of Health and Care (DTHC)

The European Commission "Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society"[6] was published in April 2018 as a specific response to the DTHC priorities, outlining how the European Commission will follow them. In particular, in the eHealth domain, the Communication highlights the importance of advancing the Digital Transformation of Health and Care (DTHC), laying out three priorities to be followed in the coming years:

- Citizens' secure access to electronic health records and the possibility to share their records across borders, and the use of e-prescriptions. (Priority 1)
- Supporting data infrastructure, to advance research, disease prevention and personalised health and care in key areas included rare, infectious and complex diseases (Priority 2)
- Facilitating feedback and interaction between patients and healthcare providers, to support prevention and citizen empowerment as well as quality and patient-centred care, focussing on chronic diseases and on a better understanding of the outcomes of healthcare systems. (Priority 3)

EC initiatives are foreseen also in terms of reviewing the operation of the eHealth Network and in particular Commission Implementing Decision 2011/890, pursuant to Article 14 of Directive 2011/24/EU in order to address these new challenges.

[6] https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering

Directive 2011/24/EU – eHealth Network

Article 14 establishes the mechanisms for cooperation on and the exchange of information among Member States working within a voluntary network, i.e. the eHealth Network, connecting national authorities responsible for eHealth designated by the Member States. Para 2 (c) further provides the mandate of the eHealth Network to support Member States in developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare.

The topic of electronic identification and authentication has been extensively discussed within the eHealth Network. To date, however, no specific policies have yet been adopted in this respect; however the topic is due to be addressed in the eHealth Network's MWP 2018- 2021.

The MWP is also focused on topics relevant to the above DTHC DSM priorities, including on patient access, use of data and digital health literacy of patients, mHealth apps, telehealth and patient-generated data; innovating use of health data; enhancing the continuity of care (e.g. stimulating and supporting the adoption of eHDSI services) and overcoming implementation challenges (e.g. interoperability & standards, skills, trust, security and privacy).

It is noted that the corner stone for full recognition of citizens' rights all around Europe in addressing the first and the third priorities of the DTHC is the existence of electronic identification and authentication solutions for cross border eHealth situations. However, this implies addressing the challenges of person specific rights and duties related to data handling (eg a treating physican will have different rights to an administrator), which in turn demands that the identification of an individual must be also associated to his/her particular role in the healthcare process and hence to the individual's rights to access sensitive personal data or provide permission for access to this data. These challenges have not yet been fully addressed in EU level policy or legislation.

Citizen empowerment, enabled through eIDAS, should be therefore viewed within a broader consideration, beyond the current limited scope of cross border exchange for emergency situations and needs to inform the design of the eIDAS Connector in what concerns the ability of the citizens to act upon sharing of their records.

eIDAS and eHDSI Governance

DG DIGIT is the eIDAS DSI owner and also the principle policy domain owner. The Coopertion Network (CN) is a formal cooperation mechanism between MSs established by the implementing decision 2015/296, article 12. The main task of the CN is to exchange information and best practices about electronic identification schemes, technical requirements, assurance levels of eID schemas, as well as peer reviewing eID schemes under the eIDAS Regulation, aiming to "facilitate the technical interoperability of the notified electronic identification schemes with a view to fostering a high level of trust and security appropriate to the degree of risk".

DG SANTE is the eHDSI owner, while the policy owner is the eHealth Network, co-chaired by DG SANTE and a MS representative. As such, DG SANTE is responsible for the evolution, maintenance, updates and add-ons of the core services of the eHealth DSI. The current governance structure incorporates the eHealth Member States Expert Group (eHMSEG) with an advisory role in what concerns the implementation of the eHDSI; the group also provides the liaison with the national implementation teams.

The eIDAS eID mechanisms and their specific regulatory, liability, IT security, trust establishment, and operation environment provisions are likely to impact the operation/fitness of existing and new cross-border electronic services.

In summary,

The eIDAS eID mechanisms and their specific regulatory, liability, IT security, trust establishment, and operation environment provisions are likely to impact the operation/fitness of existing and new cross-border eHealth services.

HEALTHeID implementation proposals, must remain compliant to the eIDAS and GDPR Regulations and associated policies while at the same time balancing MWP and DTHC priorities against what is realistically feasible, given the current constraints of the eHDSI implementation. This demands that the vision and the HEALTHeID implementation is discussed with and validated by the eIDAS and the eHDSI decision makers.

3. Lessons learnt from the eSENS - eID for eHealth pilot

The eSENS eHealth pilot experimented with the approach, where electronic identification of the patient would be added to the workflow currently supported by the eHDSI, which would largely remain unchanged. This workflow foresees that the treating health professional who has been authenticated against his own national authentication service, records and submits the patient identifier, provided in a relevant document. This far, there has not been any electronic identification of the patient, as such, included in the cross-border workflow, because the patient is always assumed to be on site and the identification is performed by the professional on his/her behalf. Likewise, there has not been any implementation of electronically provided specific patient consent. The authentication and authorization of the health professional has not come into scope, given that s/he has been identified, authenticated and authorized at national level and directly with the national infrastructure of the country of treatment.

The e-SENS eID pilot was therefore the first effort to dematerialize the identification process for the patient in adherence to the eIDAS Regulation. This was pursued through injecting the patient identifier into the eIDAS SAML Assertion as an additional optional attribute provided by the respective national attribute provider, which would be connected to the national eIDAS node. This approach was later on also considered in the Deloitte study “The use of eID in eHealth”[7] which concluded that - depending on national choices in the notified scheme - there are broadly 3 national implementation variants of eID schemes suitable for eHealth purposes:

1. Use of eIDAS notified nationally issued eID scheme with unique identifier that is used as the patient ID number for eHealth use cases

2. Use of eIDAS notified nationally issued eID scheme with unique identifier that is not used as the patient ID number for eHealth use cases Use of eIDAS notified nationally issued sector specific eHealth eID scheme with sector specific patient ID number for eHealth use cases

3. The same study proposed 3 respective variants of implementation for the national eIDAS Connector. Figure 1 illustrates the implementation scenario 2, being the most inclusive of all national situations.

eIDAS, assumes an electronic identification workflow, where the citizen requests a service from a Service Provider (SP), then the citizen is authenticated (through his national eIDAS infrastructure) towards the SP before the SP may provide access to its electronic services that the citizen is entitled to. Trust is established through the eIDAS Node in Country-A, in an interoperable transport form, the eIDAS SAML Assertion. Such assertions can be requested through an authentication request by a legitimate service provider (SP) through an eIDAS Connector deployed in Country-B. This assertion is adhering to international technical standards and provides intrinsic and

[7] DG DIGIT/DG SANTE Study for the European Commission: “*The use of eID in eHealth*”

extrinsic security safeguards (such as an electronic signature safeguarding the integrity and authenticity). The SP as a relying party may technically and legally trust the assertions contents as a strong form of citizen authentication.

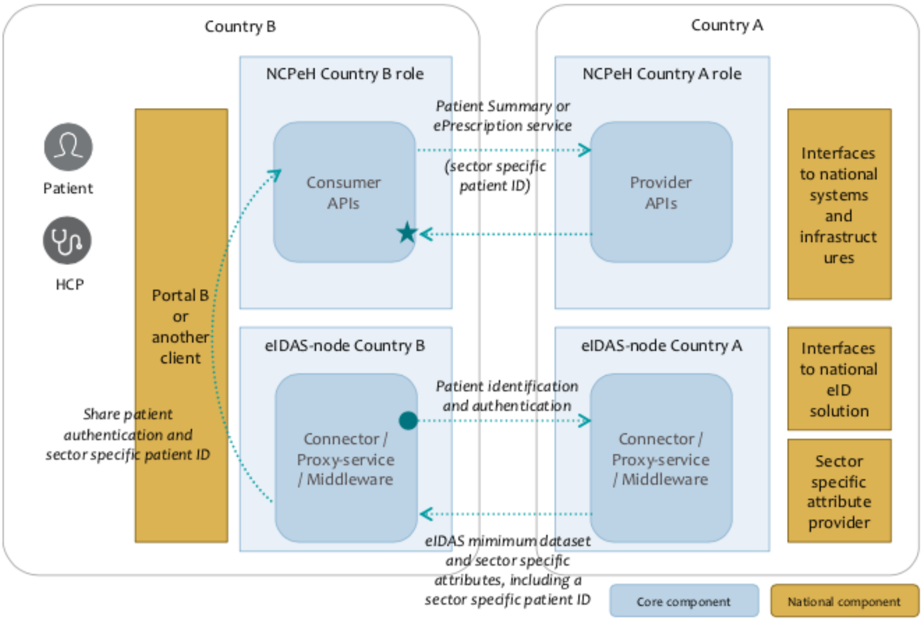

Country B
Country A
NCPeH Country B role
NCPeH Country A role
Patient
HCP
Portal B or another client
Consumer APIs
Provider APIs
Patient Summary or ePrescription service
(sector specific patient ID)
Interfaces to national systems and infrastructures
eIDAS-node Country B
eIDAS-node Country A
Share patient authentication and sector specific patient ID
Connector / Proxy-service / Middleware
Connector / Proxy-service / Middleware
Patient identification and authentication
Interfaces to national eID solution
Sector specific attribute provider
eIDAS mimimum dataset and sector specific attributes, including a sector specific patient ID
Core component
National component

Figure 3: Implementation - Scenario 2

source: Deloitte Study (2016) "The use of eID in eHealth"

There are however several challenges entailed in directly transposing this workflow into an eIDAS compliant electronic identification process:

(i) Including eHealth specific Attributes in the eIDAS SAML Assertion

Implementing the above scenario would mean that, in addition to the mandatory eIDAS Minimum Data Set, the eHealth sector would need to request to have the national equivalent of a patient identifier injected into the eIDAS SAML Assertion as an additional optional attribute.

From an organizational perspective, this scenario would require that MS will ensure that the patient identifier authentic sources meet the requirements of IDPs, agree with their national eIDAS nodes and implement legal/ trust pre-requisites and technical solutions for injecting the patient identifier as an additional attribute in the eIDAS SAML profile, and also establish a process for considering the need for changes and implementing modifications if triggered by changes to the national registries.

Besides the organizational and legal challenges, this approach would entail several technical challenges. By itself, the CEF digital reference implementation of the eIDAS nodes at the moment can only contact one single component acting as ID provider (from the service point of view);

mechanisms to locate/map/obtain additional attribute requires significant modification and sustainability could be challenging. This step would impose several additional requirements:

- the eIDAS Connector needs to obtain and analyse the metadata of the respective eIDAS service to verify the availability of the additional attributes
- the Connector needs to specifically extend the authentication request to include the additional attribute if the metadata of the respective eIDAS service indicates it as being available
- the eIDAS Service in Country-A needs to be able to locate, map, and obtain any additional attributes in addition to the mandatory eIDAS minimum data set and verify the correct linkage of both.

In addition to the above mentioned organizational challenges, this choice would require EU level decisions

- the eHealth Network should adopt "patient identifier" as an additional attribute
- each MS should include the patient identifier in their notified schemes or be able to map citizen identifiers to patient identifiers.

(ii) The "Double Consumption" challenge of an eIDAS Assertion

The eSENS implementation scenario foresees that the patient identifier may then be extracted from eIDAS SAML profile and be further consumed for the purposes of identifying and retrieving clinical documents in the national infrastructure of country A. However, a major obstacle in implementing this approach, is the premature termination of an eIDAS eID use case, after the electronic identification has been consumed by the relying party in the receiving country. From an eIDAS eID perspective, an eID application scenario is entirely concluded as soon as the Service Provider (SP) in Country-B has received the eIDAS SAML Assertion. It is explicitly assumed that the SP is the final and only consumer of this eID.

Currently, the epSOS-based eSENS pilot implementation of the NCPeH foresees decompiling the eIDAS SAML Assertion in Country-B into the individual attributes, populate an IHE XCPD transaction with the extracted attribute values, and relaying this information to Country-A. However, this removes the eIDAS assertion signature and with it the primary anchor for the trustworthiness, integrity, and reliability of the patient authentication.

In addition, from a data protection perspective, the SAML Assertion is meant to transfer personal data between the eIDAS Nodes and for a specific purpose, it being completed once the patient is identified. Further processing of the whole or part of the attributes inside the Circle of Trust, established between the NCPeHs, would require additional informed authorisation by the patient as well as the capacity to later revoke such authorisation.

(iii) Security challenges

Neither the NCPeH primary interaction channel (NCPeH portal) nor the NCPeH itself are currently equipped nor designed to handle the additional functionality of dealing with an eIDAS SAML Assertion for citizen identification/authentication. Furthermore, the NCPeH portal is usually accessed by the Health Professional (HP) and through the HP's computer, which may lack comprehensive IT and security functionality beyond a basic web browser. In the e-SENS pilot, all critical eID tasks were moved into the eHealth eID components that accommodate the additional security and processing needs of advanced eID functionality and provided an eHealth-enabled eIDAS eID Connector as a starting point and for demonstration purposes. However, to enable immediate and widespread exploitation, the eHealth eIDAS Connector must be able to implement advanced electronic services for modern access channels such as lightweight REST-based mobile Apps and a hardened integration that relies on mechanisms that enforce proper security better.

(iv) Usability challenges

Introducing an eIDAS Connector would require additional steps and facilities to provide the patient with a means to personally perform the identification and authentication process and to provide consent for the professional to access his/her health data, at the doctor's office, in order to initiate a health care encounter process. There are obvious UI challenges that need to be addressed. The e-SENS eHealth pilot had explored mobile access scenarios to overcome the usability issues.

(v) Integrating the Patient Consent workflow

The current patient consent process, as primary legal basis for access to patient's data, is decoupled from a strong patient identification process and is reduced to the health care professional confirming orally received consent confirmation.

eIDAS eID is fully adaptable to provide a much more integrated electronic identification and patient consent process during any eHealth encounter and it could allow us to combine the legal requirement for patient consent specific to the health care encounter, from the eHealth domain, with the attribute disclosure authorization of eIDAS eID to generate an integrated streamlined, patient-centric electronic patient identification and interaction with SP workflow. This integrates better with technology under the patient's control, such as an eHealth App on a smart phone.

4. Legal and Policy Requirements for HEALTHeID

There are several implications emerging from above legal and policy framework and affecting the HEALTHeID vision. These are:

Alignment of Concepts and Definitions

The definitions provided in the eIDAS Regulation should from now on apply to HEALTHeID:

- '**electronic identification'** means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
- '**person identification data'** means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;
- '**authentication**' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;
- **'relying party'** means a natural or legal person that relies upon an electronic identification or a trust service;

The first observation is that while they differ in their articulation[8] from those of the eHDSI Identity Management Specification[9] they are not in effect misaligned. It must be, however, clarified that identifying and authenticing the person is not enough for carrying out the eHDSI use cases. It is further necessary to identify a person as a patient in his national eHealth system[10].

nFR 01: The HEALTHeID Connector implementation process must adopt definitions and concepts as described in the eIDAS Regulation and translate them appropriately to the cross border eHealth context.

nFR 02: In addition to the eIDAS workflow, the HEALTHeID Connector must provide for completing the patient identification through capturing or mapping the identification data to the patient identifier.

nFR 03: Any additional step in the eIDAS workflow should be carefully designed and verified as to its ability to preserve the LoA enabled by the eID scheme.

[8] *Identification* provides an answer, whether the provided identity information is sufficient to determine the entity or not, but it does not deal with the validity of identity; *Authentication* is the process of establishing an acceptable level of assurance that a claimed identity of an entity is genuine.

[9] Identity Management Specification: https://ec.europa.eu/cefdigital/wiki/x/9w9AAg

[10] see FR03 "Patient Identification: The patient needs to be univocally identified in a reliable way (unique and unequivocal ID) to allow the HP to consult his information (after his explicit consent or authorisation)… One-to-one and unmistakable identification of the patient must be assured. Patient authentication will be guaranteed at national level based on the concept of mutual trust….".

Patient identification

The three situations identified in the relevant Delloite study (see section 3) will impact HEALTHeID in different ways:

- Where a notified, nationally issued eID scheme with unique identifier that is used as the patient ID number for eHealth use cases will be employed by country A, citizen and patient identification may collapse into one single step.
- The same applies in situations where a notified, nationally issued sector specific eHealth eID scheme with sector specific patient ID number for eHealth use cases will be employed.
- In all other cases, patient identification and authentication in cross border eHealth may be generally described as a two step process: in the first step, the citizen involved in a cross border eHealth encounter must be authenticated under eIDAS; subsequently, the citizen must be further identified *as a patient*, by means of his/her patient identifier which links the person univocally to his electronic health documents and entitlements in the national health care system.

HEALTHeID should adopt and provide solutions for the third general scenario. In this scenario however, two major challenges need to be addressed:

(i) Patient identifiers as an additional attribute present unsurpassed organizational and legal constraints,

(ii) Even if patient identifiers could be carried across borders inside the eIDAS SAML profile, the extraction process itself would bare them off the trust they are enshrined while as part of the eIDAS Attribute profile.

HEALTHeID should therefore seek alternatives of equal legal strength to collecting and sharing this important identification attribute. For example,

- Where a MS is in the position to technically and legally map the person identifiers to the patient identifiers, this mapping will become a national level action,
- Where such mapping is not possible or the preferred approach, the authenticated citizen will be invited to submit his/her own patient identifier, electronically on-line, replacing the respective action performed by the health professional.

In both cases above, trust is established by the trust framework within the network of NCPeHs. In the case of patient provided information, all checks and controls applied today for HP enabled entries are relevant. In addition this on-line service is provided by the SP to the patient, following eIDAS authentication of the individual it can therefore enjoy the legal effects of the eIDAS.

nFR 04: the HEALTHeID Connector should be designed and implemented in a way to cover all possible national situations; the default settings should therefore allow for a MS with a non health specific notified eID scheme and no possibility to map person to patient identifiers to employ the HEALTHeID eIDAS Connector.

Establishment of an on-line service context

In the present eHDSI use cases, there are no direct on-line services provided to the patient e.g. in the form of accessing data, providing consent, submitting information or a request etc. eIDAS, on the other hand, assumes interaction between three parties: a **Citizen** wishing to access a cross border service and therefore interacting with a ***Service Provider*** operating in a country other than his/her country of affiliation, the latter being a relying party for identifying and authenticating this citizen to his respective **national eIDAS node**.

Recital 12 describes the aim of the eIDAS Regulation as being "to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible".   Recital 14 further explains that "the principle of mutual recognition should only relate to authentication for an online service. The access to those online services and their final delivery to the applicant should be closely linked to the right to receive such services under the conditions set out in national legislation."

Article 6 "When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body in one Member State, the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online…"

In the eIDAS realm, it is therefore essential to recognize and map three roles: the citizen/consumer in country A seeking to receive a service from a Service Provider in country B, who is "the relying party" i.e. relies upon the its national eIDAS node of country B for identifying and authenticating the individual requesting the service. In the current cross border eHealth services of unplanned care, we can map these roles as follows:

- **the patient from country A**, is seeking to receive
- **an (on-line) service** i.e., provide access to own PS or ePrescription to a HP in country B
- from **NCPeH in country B**, who is then "**the relying party**" i.e. relies upon the
- **national eIDAS node** of country B for identifying and authenticating the individual.

It should be however noted that in the current use cases, the patient does not receive an on-line service not even at the level of providing electronic consent. While it is recognized that the design and implementation of such services is out of scope of HEALTHeID, the HEALTHeID Connector would be void without an on-line service directed by the Service Provider to the patient.

nFR 05: the HEALTHeID Connector should be designed and implemented with the aim to enable patient access to an on line service. Such a service should be identified and linked to the HEALTHeID use case.

Privacy and Data Protection by design

HEALTHeID must observe requirements for data protection by design and by default (Article 25, of GDPR) ensuring that data protection will be designed into the business processes of the eIDAS

Connector. Processing of personal data in HEA:LTHeID is lawful under Article 6, para 1, lit (a) of the GDPR, i.e, the data subject has given consent to the processing of his or her personal data for one or more specific purposes, where 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (Article 4 Definitions, (11)).

In compliance with these requirements, the standard eIDAS workflow makes provisions for specific consent to be provided by the citizen for the disclose of identification data to the SP for the purpose of identification.

Considering that the identification process for eHealth is concluded with the acquisition of the patient identifier for the purpose of locating, retrieving and disclosing personal (health data) to the HP via the SP, it is necessary that the patient consent to this specific disclosure is executed, as described in section 3(v), through a strong integrated electronic identification and patient consent process during any eHealth encounter to generate an integrated streamlined, patient-centric electronic identification and patient consent workflow.

Providing specific consent to access of health data by a specified HP in the context of a specified health care encounter could be considered as a kernel electronic service provided by the SP. It is noted that neither the consent to treatment nor recording of data arising from the treatment are legal if the patient has not been given information about the test/treatments proposed. Similarly the patient should be informed that the treatment episode will be documented and such data stored in a record which may then be integrated into his or her health record at home. The fact that information has been provided (ideally including a copy of written information) should be recorded alongside the consent.

HEALTHeID implementation should also address the response to situations where processing is necessary to protect the vital interests of the data subject and for of another natural person or for the purposes of the legitimate interests pursued by a third party which require protection of personal data, in particular if the data subject is a child. The provisions of Article 8 of GDPR (Conditions applicable to child's consent in relation to information society services) apply. Although not all MS can handle child's consent or consente provided electronically on behalf of another person based on power of atterney, such provisions should be also considered in HEALTHeID.

Annex I contains the HEALTHeID Patient Information Notice and Patient Consent Forms.

nFR 06: A specific health care encounter context must be established; the patient must provide informed consent in relation to this specific context. This context should be also articulated into text information made available to the patient in advance to providing consent.

nFR 07: The strong patient identification process, which includes specific patient consent for disclosure of identification data to the SP, should be extended to also include specific patient consent for disclosure to the health care encounter and for a specified period of time nFR 08: The HEATHeID Connector should provide also for linked eIDs as in the case of children linked to a guardian, or adults over whom a power of atterney exists.

nFR 09: Technology under the patient's control (such as an eHealth App on a smart phone) must be considered for the implementation of the above workflows.

Patient empowerment through eIDAS HEALTHeID

The cross border eHealth ecosystem typically assumes an interaction pattern in which the health professional acts on behalf of the patient. A traditional workflow, as implemented through the CBeHIS of the eHDSI, would consider the patient being mobile while the health professional is stationary. The system initiates an electronic health care episode through an action of the health professional. As a consequence, the HP and the supporting systems are then required to locate the patient electronic records dynamically.

In supporting, in particular, the Digital Market Strategy and Digital Transformation of Health and Care alternative approaches must be considered. A potentially more efficient approach would be to place the patient in the driver seat, who will then provide access for a specific HP (or, in the general DTHC context, another party), within a given healthcare encounter, through proper authorization by the patient. It is also important to note that although the current eHealth DSI considers that the exchange of patient data takes place between the country of affiliation (A) and the country of treatment (B), this approach would be extendable to a patient in ANY country, addressing an HP in ANY country and providing access to own health data stored in ANY country.

The scope and mandate of HEALTHeID is to implement, test and validate an appropriate solution for electronic patient identification, suitable for immediate deployment in the eHDSI, by the parties involved, which are the national NCPeH, without an obligation to address situations beyond this scope. Nevertheless, in selecting the proper implementation choice, scalabiltiy to use cases that will be supported as part of the eHealth Network MWP should be also considered.

nFR 10: HEALTHeID should address citizen empowerment enabled through eIDAS, within a broader consideration, beyond the current limited scope of cross border exchange for emergency situations.

nFR 11: The design of the HEALTHeID Connector should address, as a minimum, the requirements of the first priority of the DTHC for enabling the citizens to act upon sharing of their records and be extendable to all three priorities in the future.

5. HEALTHeID Vision

Cross border eHealth can benefit greatly from the adoption of eIDAS based electronic identification and authentication of patients, leveraging on the high level of legal certainty and robust liability framework introduced by eIDAS and also the GDPR. The operation of the ERNs is also paving the way for networked, patient centered cross border healthcare, while enabling technologies will further contribute to the vision of Euroepan citizens that are enabled to decide upon and manage access to their own data.

At the same time MS and the European Commission have been investing in the sustainable deployment of cross border eHealth services, starting from the successfully piloted CBeHIS involving the cross border access of Patient Summaries and ePrescription.

The HEALTHeID vision carefully balances the need to safeguard and avoid disruption of the current CEF eHDSI infrastructure and services, against the need to migrate towards better integrated cross border eHealth in the DSM realm. The HEALTHeID Vision builds on the following universal principles underlining both the present and the projected future of cross border eHealth.

I. Citizens - Patients

Our electronic identities, mutually recognized under the eIDAS Regulation, are our passport to enjoying access to digital services in all sectors, offered anywhere to citizens living and working anywhere in the EU. The potential impact for health care is immense, as this enables a multitude of services, not least those involving sharing of health data across borders and, as envisioned in the EC Communication, can further shape the future of health and care provision.

Strong electronic identification and authentication for the citizen is necessary for enjoying the potential benefits, it may however not be enough. The citizens must be also identifiable in their national eHealth infrastructures, via their patient identifiers, which may differ from their citizen identifiers. While the situation regarding general vs specific patient identifiers varies amongst MS, it is important to consider that, for health care purposes, electronic identification envolves the identification and authentication of a citizen as well as identification of the patient, irrespective of whether these need be two seperate steps or a single step, i.e., where general purpose identifiers are used for health care purposes or where health specific eID schemes have been notified.

> HEALTHeID is about patient identification, in compliance with but going beyond the strict eIDAS scope.

II. Patient empowerment

We may identify three main process components, leading to lawful data sharing:

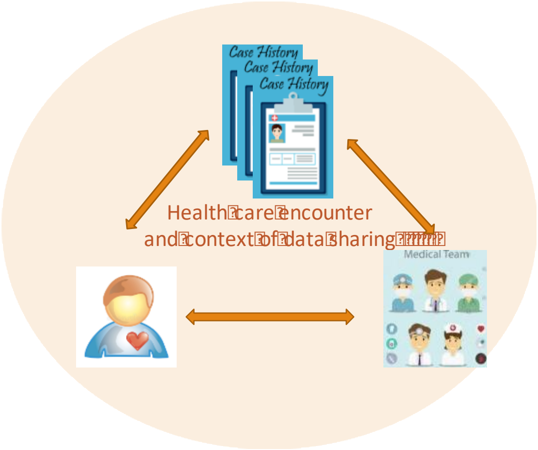
(i) Identification and Authentication of the *patient* towards the SP

(ii) Establishment, by the SP, of the context of the data sharing, i.e., correlation of the patient, involved HP(s) and health data to be shared in a uniquely identified health care encounter

(iii) Enabling HP access to the document through context specific and informed patient consent and subsequently informing the patient about this access

The first component involves a generic eIDAS information flow, supplemented as needed by health specific patient identification.

The second component is not eIDAS driven, but is necessary to establish the specific situation and context of data sharing to which consent of the identified patient will be provided to. For establishing such a context, it is necessary to link the patient (eID), the patient identifier (if different) in the country where the health data is, the health professional and the data to be shared and associate it to the specific health care encounter.



The third component closely couples the eIDAS identification of the individual to patient consent. This step then establishes the legal pre-requisites for lawful data sharing through obtaining the specific consent of the identified data subject to disclose the identified health data within the specific context, as previously established.

This interaction described above is not a scenario in itself but a universal, flexible foundation to integrate and operate strong eID within and aside from the eIDAS eID framework and its associated trust services.

HEALTHeID solutions will leverage on the potential to match the strong AAL, made transparent and secured by the eIDAS workflow to conclude a fully regulated-by-design process leading to lawful access to health data.

III. Interaction Patterns

In our current approach employed by CBeHIS, the two collaborating NCPeHs in country B and country A, assume roles of Data Consumer (DC) and Data Provider (DP), respectively. In future generalized scenarios, the DP can be any entity that stores and manages health data in any country, whereas the role of DC can be with one or more entities that consume health data in one or more other countries. This case, is already today the real life situation within the members of the ERNs, where DPs from one or more countries share data with DCs in one or more countries, on the basis of patient consent, specific to the context of the ERN function and processes.

The authorization for access to medical information of a particular patient by a specified health professional or in a more general case a specified care team, enables a variety of future exchange patterns with the SPs as trusted anchor points, for example,

- Patient pushing medical information to a particular HP or care team, based on an HP/team locator (i.e. patient needs to “locate” the HP/care team-SP enables the process of locating the DC);
- Enabling a specific HP to pull medical information for a particular patient based on an information locator (i.e. the HP need to “locate” the electronic clinical document they need

to access-SP enables the process of locating the DP who will then locate the requested clinical document)

- Enabling the integration of further, potentially patient-controlled, data sharing scenarios (e.g. a rare disease patient enabling access to his records by a multinational care team defined within an ERN, or rare disease patient enabling access to parts or the whole of his data for research purposes by the members of the scientific ERN community).

A HEALTHeID patient driven approach could augment the current eHDSI services, but could also be deployable in other scenarios, beyond the scope of the current CBeHIS.

The HEALTHeID vision is not constrained by the limitations of our current uses cases. Although the implementation will focus on serving the current CBeHS use cases, the design and technical implementation choices will lay the foundations for patient enabled future scenarios of lawful sharing of health data, between DPs and DCs in the EU.

5.1 Criteria for assessing Implementation Choices against the HEALTHeID Vision

Within the scope of the technical implementation activities of HEALTHeID, alternative implementation strategies are explored. These alternatives should be assessed against certain criteria in order to ensure a proper balance between ambition and what is feasible within the timeframe and the scope of the project.

The following criteria are proposed:

Criterion 1: Compliance with eIDAS Regulation. The proposed approach should respect fully the eIDAS requirements and exploit maximally its enabling properties, i.e., it should exhaust the possibilities for a viable and sustainable solution within the provisions of the eIDAS Regulation without the need for additional agreements (nFR 01 , nFR02, nFR05)

Criterion 2: Privacy by design The proposed approach should respect the relevant GDPR requirements and exploit maximally its enabling legal basis for access to health data and its safeguards as to the protection of the individual’s rights (nFR 06 , nFR07, nFR08).

Criterion 3: Security The proposed solution should protect against security breaches (e.g when using a shared devices) and to preserve the Level of Assurance (LoA) of the patient authentication through out the whole process (nFR03).

Criterion 4: Patient Empowerment: The proposed approach should enhance citizen experience when taking chanrge of own choices in relation to access to own health data, reflecting good alignment to the DSM Strategy and the relevant policies as expressed in the eHealth Network MWP and the “EC Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society".(nFR04, nFR09, nFR11)

Criterion 5: Scalability The preferred solution should have the minimum possible impact and disruption on the current deployment of the eHDSI; however, the solutions proposed should take a longer term perspective, not least of the eHealth Network immediate priorities reflected in the MWP 2018-2021 (nFR10, nFR11).

Criterion 6: Availability The proposed approach should be appropriately balance digital patient empowerment against accessibility by minority segments of the population i.e. it should exploit widely used technologies by the European citizens (such as smart phones, personal connected devices etc) and also consider alternatives for minority situations (nFR04, nFR9, nFR11).

ANNEX I. Patient Information Notice and Consent Forms

2. BACKGROUND - WHAT IS EUROPEAN eHEALTH

- As a European citizen you are entitled to seek the help of a healthcare professional in another EU country for planned or unplanned (emergency) care.
- In most cases you will be able to claim reimbursement for such care (further advice from your National Contact Point)
- The healthcare professionals in the country you are visiting will be able to treat you much better if they can see the main parts of your healthcare records – **known as your Patient Summary** and your prescription history and active prescriptions - **known as your ePrescriptions**.
- The European Union has established a safe and secure system for allowing a healthcare professional in the country you are visiting to access and view your Patient Summary or to dispense your ePrecriptions.
- In order to be able to use that system the health care professional must have:
  - ○ Your consent to identifying you electronically
  - ○ Your consent to accessing and viewing your Patient Summary and ePrecriptions
  - ○ Your consent to creating a record of the care you receive or the medication you have been dispensed in the country you are visiting.
- This form concerns only the three consents above.
- Even if you provide these consents, you may still refuse any treatment or care offered to you in the country you are visiting.

1. IDENTIFYING YOURSELF

- The healthcare professional or a member of their staff in the country you are visiting will ask you to identify yourself using the electronic identification system.
- They will explain how to use the local identification application.
- You will not be asked to share any PIN code or other confidential identification tool.
- Your identification information will be kept in the healthcare system as long as is necessary for the care and treatment you will receive.
- A record of the fact that you have been identified as well as your name and contact details will be kept by the

ACCESSING YOUR PATIENT SUMMARY and ePRESCRIPTIONS and CREATINGA NEW RECORD

- Once you have been securely identified the healthcare professional will use the European eHealth secure infrastructure to contact your home country and request to retrieve your Patient Summary.
- The healthcare professional will be able to see major illness you have had, medication you are taking and other key information.
- Anything you have asked your home doctor not to include in your Patient Summary will not be visible to the healthcare professional in the country you are visiting.
- If you are provided with a medication, a dispensation report will be returned to your home country.
- A record of the care and treatment you receive in the country you are visiting will be stored there for as long as is required by local law.

3. Your Rights

- You have the right to give or withhold your consent to providing electronic identification or to access to your Patient Summary or e-Prescriptions by a healthcare professional in a country you are visiting.
- This does not mean you will be refused care, but your care may be impacted if the healthcare professional cannot access your Patient Summary.
- You are entitled to receive further information about the purposes for which your data will be used and who will have access to it.
- You have a right to a portable copy of the record the healthcare professional in the country you are visiting has created, but this duty may be fulfilled some weeks after your visit.
- If you find any errors in the record created in the country you visited, you have right to have such errors corrected.
- Further information on your rights may be found at WWWW.xxx.yy

PATEINT IDENTIFICATION DETAILS (automatically filled in)

First Name: .... **Surname:** ....

Date of Birth: □□ □□ □□□□ **ID number:** □□□□□□□□□

If Required

PARENT/GUARDIAN IDENTIFICATION DETAILS (automatically filled in)

First Name: .... **Surname:** ....

Date of Birth: □□ □□ □□□□ **ID number:** □□□□□□□□□

☑ **I CONSENT to providing my* electronic Identification**

I understand that my electronic ID will be used only to gain access to the Patient Summary held in my home country and/or to my ePrescriptions for the purposes of this health care encounter

Signature **Date**

☑ **I CONSENT to my Patient Summary* being accessed and viewed by the healthcare professional in [name of country]**

I understand that my Patient Summary/e-Prescriptions will be used only for my care /dispensation of medication and for administrative purposes linked to my care, for the purposes of this healthcare encounter

Signature **Date**

☑ **I CONSENT to a record of the care* I have received in [name of country] being created and stored in that country**

I understand that this record will be used only for my care and for administrative purposes linked to my care.

Signature **Date**

....

*To be modified accordingly to each situation i.e. individual or proxy, Patient Summary or ePrescription.