D8.2.4 – Common eID Approach for Health in the European Union

WP8 - Integration in National Policies and Sustainability

24-03-2021

Version 1.0

For adoption

Grant Agreement nº 801558

Co-funded by the European Union's Health Programme (2014-2020)

CONTROL PAGE OF DOCUMENT		
Document name	Common eID Approach for Health in the EU – Information paper for eHN	
Work Package	WP 8 – Integration in National Policies and Sustainability	
Dissemination level	PU	
Status	Final	
Beneficiary(ies)	SPMS	
Author(s)		
Country	**Organisation**	**Name**
Czech Rep	MoH CZ	Hynek Kružík
Germany	Gematik	Maid Erovic
Greece	3rd-RHA	Stella Spyrou, Panagiotis Bogiatzidis, Georgia Tzitzili
Hungary	SU, NHSC	Antal Bódi; Kornél Tóth; István Csizmadia; Márton Kis
Ireland	HSE	Eamon Coyne
Italy	MoH IT	Gabriele Stacchiola
Latvia	NHS	Edgars Goba
Norway	NHN	Simone Vandeberg
Portugal	SPMS	Henrique Martins; Filipe Mealha; João Cunha; Fábio Marques; Sara Russo; Diogo Martins; Anderson Carmo
Romania	CNAS	Anca Somacescu
Serbia	BATUT	Vedran Martinovic
Slovenia	NIJZ	Lucija Tepej Jočić; Hajdi Kosednar
Spain	MoH ES	Alexander Zlotnik
Sweden	ehalsomyndigheten	Manne Andersson

REVISION HISTORY			
Revision	**Date**	**Author**	**Description**
0.1	29/08/2019	João Cunha; Fábio Marques; Filipe Mealha	1st draft document
0.2	29/08/2019	Filipe Mealha	Review and comments.
0.3	30/08/2019	João Cunha; Filipe Mealha	Input of new content.
0.4	01/09/2019	Henrique Martins	Note correction to timeline, add Roadmap details, scope vision, review document, add executive summary and roadmap details
0.5	23/09/2019	Diogo Martins; Anderson Carmo;	Update of the document according the inputs received on the DG's meeting (3rd Sep. 2019 – Brussels)
0.6	22/10/2019	Filipe Mealha	Update of the document to include notes from the Regulation 2019/1157 of the European Parliament and of the Council and from DG DIGIT's report – The use of eID in eHealth – Final report Phase II
0.7	19/06/2020	Filipe Mealha; Sara Russo, Anderson Carmo	Document restructure
0.8	01/07/2020	Filipe Mealha; Sara Russo, Anderson Carmo	Introduction of comments and new content regarding the Survey analysis.
0.9	06/07/2020	Filipe Mealha; Sara Russo, Anderson Carmo	Inclusion of the Proposed Governance Framework for Health eID in the EU
0.10	07/08/2020	Maid Erovic	Comments and additions to the document through the use of non-notified eID systems in eHealth
0.11	08/07/2020	Alexander Zlotnik	Inclusion of clarifications regarding the prevailing interpretation of eIDAS applicability to current eHDSI services in Sections 1.2 (problem statement) and 3.1 (3.1. Electronic identification of Patients Use case). [suggested change]
0.12	15/07/2020	Anca Şomăcescu	Comments on Chapter 1 regarding inclusion of references to funding of research and innovation on the use of eID in the field of eHealth; references on eIDAS, GDPR, NIS interpretation in the document; the emphasis regarding technologies addressed in the document.
0.13	15.7.2020	Lucija Tepej Jočić	Tried to shorten Executive summary
0.14	18.07.2020	Antal Bódi, Kornél Tóth	Review and completion
0.15	24/07/2020	João Cunha	Inclusion of content on previous and current projects. Improvement on policy and legislation.
0.16	13/08/2020	Sara Russo; Anderson Carmo	Inclusion of content in Chapter 1 (Introduction) and Chapter 4 (Policy and Governance Structure Description)
0.17	26/08/2020	Lucija Tepej Jočić	Review and modifications of Executive summary, Chapter 1, Chapter 3
0.18	27/08/2020	Maid Erovic	Review and completion of recommendations

0.19	28/08/2020	Filipe Mealha, Sara Russo, Anderson Carmo	Review and validation of content and recommendations.
0.20	01/09/2020	All authors	Final review of the document
0.20a	08/09/2020	Hugo Agius Muscat (MFH)	QM review of v0.20
0.21	10/09/2020	Anderson Carmo	Validation after QM review
0.22	17/02/2021	Filipe Mealha; Diogo Martins; Anderson Carmo; Fábio Marques; João Cunha; Alberto Zanini (ARIA)	Revision and update of the document accordingly the feedback received from eHMSEG and eHN Technical Subgroup.
0.23	26/02/2021	Filipe Mealha; Diogo Martins; Anderson Carmo; Stella Spyrou; Antoine De Marasse; Eamon Coyne; Kornél Tóth; Lucija Tepej Jočić; Simone Vandeberg; Manne Andersson	Final revision of the document by the working group.
0.24	17/03/2021	Anderson Carmo	Update of the roadmap section according to comments from the Commission.
0.24a	20/03/2021	Hugo Agius Muscat (MFH)	QM review of sections 5 and 6 of v0.24 and some general quality assurance
1.0	24/03/2021	Anderson Carmo Lucija Tepej Jočić	Consolidation of the QM review and inclusion of text update.
1.1	07/06/2021	Anderson Carmo	Update of the document name accordingly the 19th eHN meeting (03 June 2021).

Table of Contents

Index of figures

Index of Tables

Acronyms

Acronym	Description
AAL	Authentication Assurance Level
CALLIOPE	CALL for InterOPErability
CBeHIS	Cross-Border eHealth Information Services
CEF	Connecting Europe Facility
CSS	Common Semantic Strategy
CT	Computed Tomography
DICOM	Digital Imaging and Communications in Medicine
DSI	Digital Service Infrastructure
eD	eDispensation
eHDSI	eHealth Digital Service Infrastructure
eHMSEG	eHealth Member States Expert Group
eHN	eHealth Network
EHR	Electronic Health Record
EHRxF	Electronic Health Record Exchange Format
eID	Electronic identity
EMA	European Medicines Agency
eP	ePrescription
epSOS	European Patients Smart Open Services
EQA	External Quality Assurance
EQALM	European Organisation for External Quality Assurance Providers in Laboratory Medicine
EU	European Union
FAIR	Findable, Accessible, Interoperable, and Reusable
HC	Healthcare
HP	Health Professional
ICD-10	International Classification of Diseases – version 10
ICD-10-CM	International Classification of Diseases – version 10 – Clinical Modification
ICD-O	International Classification of Diseases for Oncology
ICT	Information and Communication Technology
ISCO-08	International Standard Classification of Occupations
LoA	Level of Assurance
LSP	Large Scale Pilot
MRI	Magnetic resonance imaging
NCPeH	National Contact Point for eHealth
NCSP	NOMESCO Classification of Surgical Procedures
NPU	Nomenclature for Properties and Units
OJEU	Official Journal of the EU
PCS	Procedure Coding System
PS	Patient Summary
RMS	Referentials Management Service
SDO	Standards Development Organization
WG	Working Group

Executive summary

Citizenship of the European Union (EU) entitles every citizen to the right of free movement. Freedom of movement entails the right to cross borders with a valid proof of identity[1]. This freedom also extends to healthcare, given that every citizen of the EU may eventually need healthcare. The right of free movement of people shall be exercised in the context of digital technologies, and electronic identity (eID) needs to be verified and authenticated, to prove the identity of patients and professionals in the course of healthcare provision. The eID is a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions[2].

The introduction of minimum security and format standards of electronic identification should allow Member States to rely on its authenticity when EU citizens exercise their right of free movement. The adoption of security standards should provide sufficient guarantees to public authorities and private entities to rely on the authenticity of digital identity means used by EU citizens. Should the Member States be able to exchange identifying information contained on a secure storage medium, the formats used should be interoperable, including in respect of automated border crossing points. Extensive discussions have occurred in the eHealth Network about the relevance and critical aspects of electronic identification (eID) for the secure and reliable identification of patients and professionals that would engage or be the subject of professional engagement with digital services and data in the health sector. Since 2012, this topic has been brought to the eHealth Network on different occasions and was scoped in several European Commission funded projects and initiatives (e.g. STORK, eSENS, eHGI and JAseHN). With the advent of cross-border digital services, the enforcement of eIDAS Regulation[3] and the emergence of multiple novel technologies supporting eID, there is now a time, opportunity and a necessity to align eID implementation throughout the EU. Hence, this paper aims to present the basis, the rationale, and a timely proposal for a common approach in eID for health, not just at cross-border level, but rooted in timely adoption at national level.

The **Common eID Approach for eHealth** shall leverage recent EU regulations and create a holistic approach to eID in eHealth and related ICT services. The approach must be supported by sustainable EU policies of both the eID and eHealth worlds. It should promote convergence of efforts between Member States/countries, considering the sensitivity and vulnerability of health data and available standards and technologies. eID shall be considered as a means to achieve innovative use of health data, supported by a future EU roadmap for eHealth. Increased strength and security of identification of persons is to be implemented, enabling interoperability within and across borders. The governance process for electronic identification shall be interlinked with the governance of projects and services for eHealth in Europe, within the framework of the Joint Coordination Process or other governance entities of eHealth and alignment between different Directorates-General of the European

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0038

[2] http://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf

[3] https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf

Commission and Member States. The scope of this document was agreed by the eHealth Network (eHN) and the Commission in November 2019, and the draft document was approved in June 2020. Following the approval by the eHN, the final approach should be in place from 2021 until 2026.

The common high-level roadmap would support the proposed approach, taking into account the necessary capacity building for full scale eID deployment, and maintaining an open mindset regarding the exact technologies that support eID while ensuring common principles and governance of the different steps in the different national contexts.

The Common eID Approach for eHealth is inspired by the vision of '*full scale deployment of electronic identification in the healthcare sector, raising trust in electronic health data exchange, and taking another step forward towards the Digital Single Market, in a progressive manner, and open to diversity of technological solutions as long as basic principles and security are ensured.'*

1. Introduction

Identification plays a fundamental role in facilitating the interactions among individuals, such as interactions between patients and health professionals. The digital identity for health[4] is a collection of electronically captured and stored identity attributes that uniquely describe a person within the healthcare context and are used for electronic transactions. A digital identity system needs to be supported by processes that aim to manage the lifecycle of individual digital identities.

Healthcare providers and researchers need to identify patients accurately and uniquely in order to record data within healthcare provision as well as to produce health statistics and other data applications for planning, evaluation, emergency response, and improved treatments and disease management. Last but not least, the patient must be enabled to access their own data by digital means[3].

At a cross-border level, managing the identification lifecycle is not an easy quest due to the need to ensure a minimum-level interoperability of eID schemes, high-technological performance and secure schemes. This leads to the need to establish and develop a common approach for the EU to ensure the use of health eID at a cross-border level and support the Member States in achieving a minimum level of trust on eID schemes.

1.1. Current context

Citizenship of the EU entitles every citizen of the EU to the right of free movement, subject to certain limitations and conditions. Directive 2004/38/EC of the European Parliament and of the Council gives effect to that right. Article 45 of the Charter of Fundamental Rights of the EU also provides for freedom of movement and residence. Freedom of movement entails the right to exit and enter Member States with a valid identity card or passport.

Pursuant to Directive 2004/38/EC, Member States are to issue and renew identity cards or passports to their nationals in accordance with national laws.

Considerable differences exist between the security levels of national identity cards issued by Member States and residence permits for EU nationals residing in another Member State and their family members. Those differences increase the risk of falsification and document fraud and also give rise to practical difficulties for citizens when they wish to exercise their right of free movement.

In its Communication of 14th September 2016 entitled '*Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders'*, the Commission stressed that secure travel and identity documents are crucial whenever it is necessary to establish without doubt a person's identity and announced that it would be presenting an action plan to tackle travel document fraud. According to that Communication, an improved approach relies on

[4] http://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf

robust systems to prevent abuse and threats to internal security arising from failings in document security.

The Commission, in the 2016 Action Plan, and in its 2017 EU Citizenship Report, committed itself to analysing policy options to improve the security of identity cards and residence documents.

Regulation 2019/1157 of the European Parliament[5] and of the Council states that the establishment of minimum security standards and the integration of biometric data in identity cards and in residence cards of family members who are not nationals of a Member State are important steps in rendering EU citizens to fully benefit from their rights of free movement.

This regulation also states that Member States should take all necessary steps to ensure that biometric data correctly identify the person to whom an identity card is issued. To this end, Member States could consider collecting biometric identifiers, particularly the facial image, as a method of implementation by the national authorities issuing identity cards.

Member States should exchange with each other such identifying information as is necessary to access, authenticate and verify the information contained on the secure storage medium. The formats used for the secure storage medium should be interoperable, including in respect of automated border crossing points.

Electronic Identification (eID) is the digital identification of citizens through national identification numbers, e.g. citizens card, social security and other identification methods. eID allows the recognition of national eID schemes (including smartcards, mobile and log-in), allowing citizens of one EU country to use their national eIDs to securely access services provided in other EU countries. This electronic identification could be used at both the national level and for cross-border health services.

The eIDAS Regulation provides for legal certainty beyond national borders, a predictable regulatory environment for a seamless cross-border recognition of eID, and trust services (e.g. electronic signatures). This regulation foresees that if a Member State offers an online public service to citizens/businesses for which access is granted based on an eID scheme, then that particular Member State's online public service must also recognise the notified eIDs of other Member States by 29 September 2018. This applies to online services that correspond to an assurance level of 'substantial' or 'high' in relation to accessing that service online. Member States remain free, in accordance with EU law, to recognise eID means that have lower identity assurance levels. The eIDAS Regulation thus ensures that people and businesses can use their own national eIDs to access online public services in other EU countries, where eID services are available.

Current ongoing cooperation projects tackling interoperability challenges at a global scale, such as the Global Digital Health Partnership (GDHP), have also highlighted a confident patient identification process as a key prerequisite for safe and efficient interoperability[6].

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R1157

[6] Connected health: Empowering health through interoperability: https://s3-ap-southeast-2.amazonaws.com/ehq-production-australia/57f9a51462d5e3f07569d55232fcc11290b99cd6/documents/attachments/000/102/278/original/GDHP_Interop_2.05.pdf

1.2. Problem Statement

eHealth Digital Services Infrastructure (eHDSI) services (Patient Summary and ePrescription/eDispensation) and their use cases are in-person (not online) in the country of treatment (country B). Therefore, eIDAS is outside the current scope of eHDSI, although it could be beneficial for future services or use cases (such as patient access to clinical information in a different Member State).

A consensus among Member States regarding operational matters not covered by GDPR, eIDAS Regulation and NIS Directive seem to be still pending at the moment due to many simultaneous legislative reforms. Creating a consensus on this topic seems to be the subsequent step.

The political alignment concerning a common Authentication Assurance Level (AAL) ('substantial' or 'high') for eHealth is not reached as of today. A possible implementation of AAL 'high' is seen as very demanding for Member States; AAL activities may be resumed after the legal review of the eIDAS Regulation and GDPR is complete.

Consequently, additional means, services and mitigation strategies need to be identified to assure minimum-level interoperability of eID schemes that guarantee standardised, high-technological performance and secure schemes; or to encourage Member States to enable purely digital identification and authentication such as mobile eID to compensate for specific interoperability issues with eID based on physical tokens. Both options would introduce some operational challenges to the Member States/countries:

- Deployment/rollout of specific hardware (e.g. contact or contactless smartcard readers) and software (smartcard reader drivers and libraries) at the point-of-care of the country of treatment to handle the heterogeneity of physical-token-based eID means;
- Deployment of country-of-treatment service providers (healthcare portals) enabled for physical-token-based eID or newer eID scenarios, e.g. mobile eID.

Additionally, Member States/countries face some operational challenges necessary to comply with the common approach proposed in this document and achieve the goal of eID-enabled use cases:

- Deployment of the National Contact Point for eHealth (NCPeH) by the competent national authorities participating in the CBeHIS (for cross-border scenarios);
- Deployment of eIDAS connectors by the eID-competent national authorities (if not already deployed);
- Deployment of eID means by the country of affiliation for accessing health services, and notification of its scheme (for cross-border scenarios);
- Deployment of electronic patient registries by the country of affiliation;
- Deployment of electronic health professional registries by the country of treatment and engagement with health professionals' associations.

1.3. Goals

The goals of a Common Approach for using eID in health should be:

1. Structure a common approach on health eID within the EU.
2. Converge development roadmaps for service providers with adoption of eID also to ensure phased adoption of novel requirements regarding electronic identification that are progressively more demanding.

The work conducted in this document is in alignment with other eID initiatives and recommendations from European Commission and the eHealth Network, such as Electronic Health Record Exchange Format[7] (EHRxF) and others.

***Table 1** – Common eID Approach for eHealth Goals, objectives and activities.*

Goal	Description	Objective	Activity
G1	Structure a common approach on health eID within the EU	**O1.1** Define a Common eID Approach for Heath in the EU	**A1.1.1** Define a set of domains related to eID
			A1.1.2 Identify available tools and the shortcomings for each tool
			A1.1.3 Overview about the current and previous EU eID initiatives;
			A1.1.4 Align current and future research projects/policy initiatives between different DGs within the European Commission, as well as Member State/country efforts, in future definitions of solutions, architecture, assurance levels amongst other common and transversal characteristics
		O1.2 Develop common eID assets for Patient Identification	**A1.2.1** Drive the development of common eID assets for Patient Admission
			A1.2.2 Drive the development of common eID assets for Patient Summary
			A1.2.3 Drive the development of common eID assets for ePrescription & eDispensation
			A1.2.4 Drive the development of common eID assets for Telehealth
			A1.2.5 Drive the development of common eID assets for Consent Provision
			A1.2.6 Drive the development of common eID assets for Emergency Call Centre
			A1.2.7 Drive the development of common eID assets for Patient eIDs
			A1.2.8 Drive the development of common eID assets for Laboratory & Medical Imaging Reports access
			A1.2.9 Drive the development of common eID assets for Hospital Discharge Reports access
		O1.3 Develop common eID assets for Health Professional Identification	**A1.3.1** Drive the development of common eID assets for Consent Provision
			A1.3.2 Drive the development of common eID assets for Patient Summary
			A1.3.3 Drive the development of common eID assets for ePrescription & eDispensation / Mobile ePrescription

[7] https://ec.europa.eu/digital-single-market/en/news/recommendation-european-electronic-health-record-exchange-format

			A1.3.4 Drive the development of common eID assets for Death Certificates
			A1.3.5 Drive the development of common eID assets for Telehealth
			A1.3.6 Drive the development of common eID assets for Laboratory & Medical Imaging Reports
			A1.3.7 Drive the development of common eID assets for Hospital Discharge Reports
			A1.3.8 Drive the development of common eID assets for Referral Management
G2	Converge development roadmaps for service providers with adoption of eID and ensure phased adoption of novel requirements regarding electronic identification that are progressively more demanding	**O2.1** Establish a methodology to address alignment to Common eID issues at an EU level.	**A2.1.1** Set up a sustainable plan to ensure alignment between Common eID issues at an EU level.
			A2.1.2 Draft new Common eID for 2020-2025
		O2.2 Establish a relationship between key bodies of the EU and key technological partners in the digital identity process	**A2.2.1** Identify the key identity stakeholders, their roles and responsibilities

2. State of the Art

2.1. Understanding the Identity Lifecycle

This chapter aims at providing some insights on key aspects that need to be addressed in order to realise a common approach to eID in eHealth within the EU.

It is very important to consider the four 'domains' on eID to elaborate the common eID Approach:

Registration / Proof of Identity

The Registration phase begins with the process of uniquely distinguishing an individual, called Resolution. The first step is the **Enrolment**, in which biographical data are presented to the issuing authority for proof of identity to be carried out. The ***Validation*** begins when the authority determines the authenticity and validity of the data provided and relates it to a living citizen.

Subsequently, the ***Verification*** is carried out, in which relationship is established between the claimed identity and the individual who provides the proof of identity. This 'domain' is directly linked with the mechanism of identification used by the patient or the HP at the moment of the health service attendance.

Credential Management[8]

Credential Management consists of the process of creating and distributing virtual credentials as **decentralised digital proof of identity**, such as e-passport, eID card and a unique identifier. The steps are Maintenance (retrieving, updating and deleting credentials) and Revocation (removing the privileges assigned to credentials).

Authentication and authorisation

Authentication ensures the univocal unambiguous identification of the patient/Health Professional through the established identification process. It will generate an electronic authentication of eID and allows the patient/Health Professional to proceed the next steps of the clinical encounter.

After the authentication process the authorisation takes place. The **authorisation** is responsible for guaranteeing the access by the users only to the data or application domains that were previously granted. For that, levels of authorisations must be defined according to the actor's role. For example, a patient, a nurse and a physician must each have a different level of authorisation according to their role.

[8] Technology Landscape for Digital Identification: http://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf

Identity Management[9]

Identity management is the continuous process of retrieving, updating and excluding attributes of each identity.

Figure 1 summarises the life cycle phases considered for the creation of the digital identity described above.

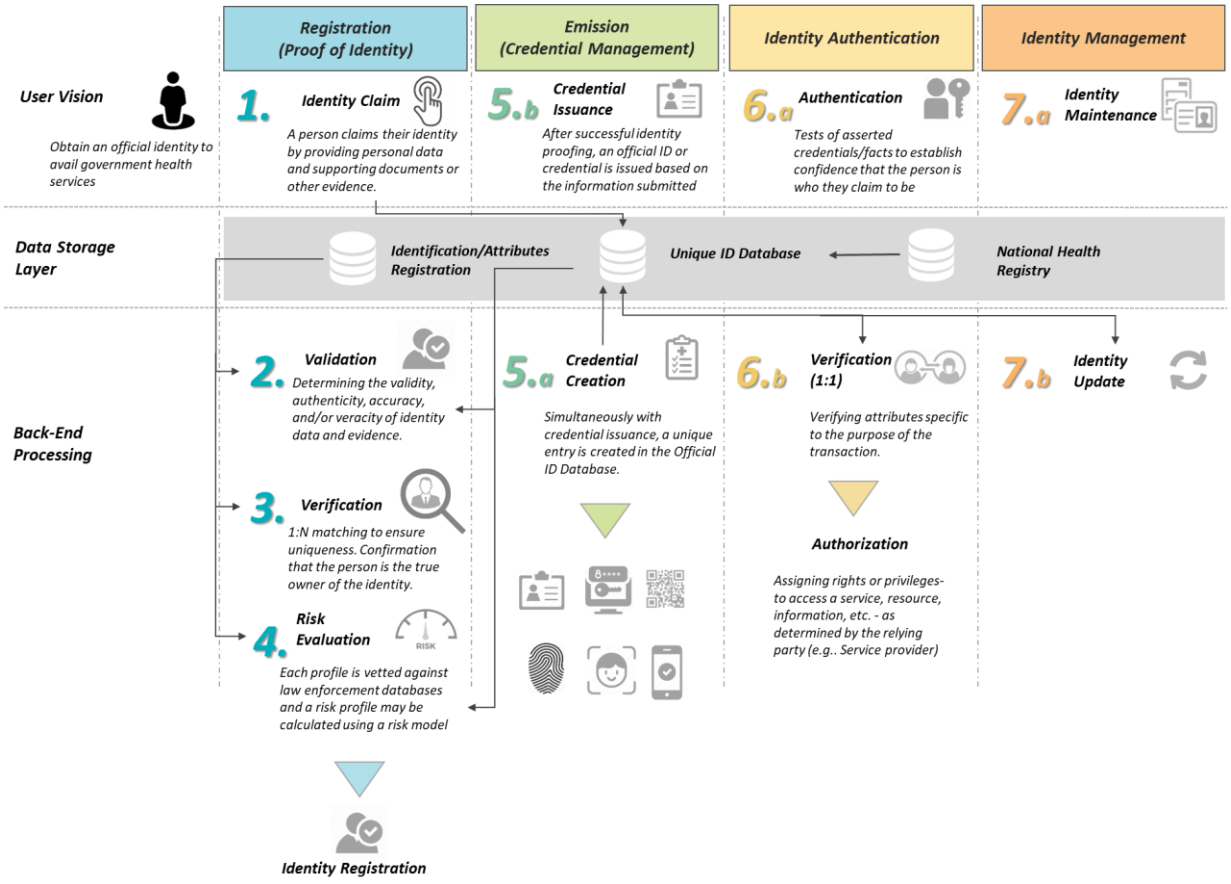

***Figure 1** – The life cycle of digital identity (adapted from Technology Landscape for Digital Identification)*

The expansion of the digital market, associated with a unique national recognition of health professionals by information systems requires the definition of a minimum set of attributes that allows the representation of each health professional, as a unique element. These attributes must guarantee the correct identification of each health professional, in order to avoid the risk of exposure of information to unauthorised health professionals.

[9] Technology Landscape for Digital Identification: http://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf

2.1.1. Levels of Assurance

Authentication is a stage in the digital identity lifecycle. The type of authentication (weak, secure, strong or very strong) depends on the robustness of the technology and the authenticators used. Considering different types of information exchange, it appears that not all transactions require the highest level of assurance (LoA). Single factor authentication, such as an identification number or knowledge of a password, is insufficient to prove the identity of a citizen or professional and does not constitute an accurate authentication.

In the health context, considering the sensitivity of the information accessed by health professionals, the existence of multiple authentication factors is considered relevant in order to provide stronger security (see figure 2).

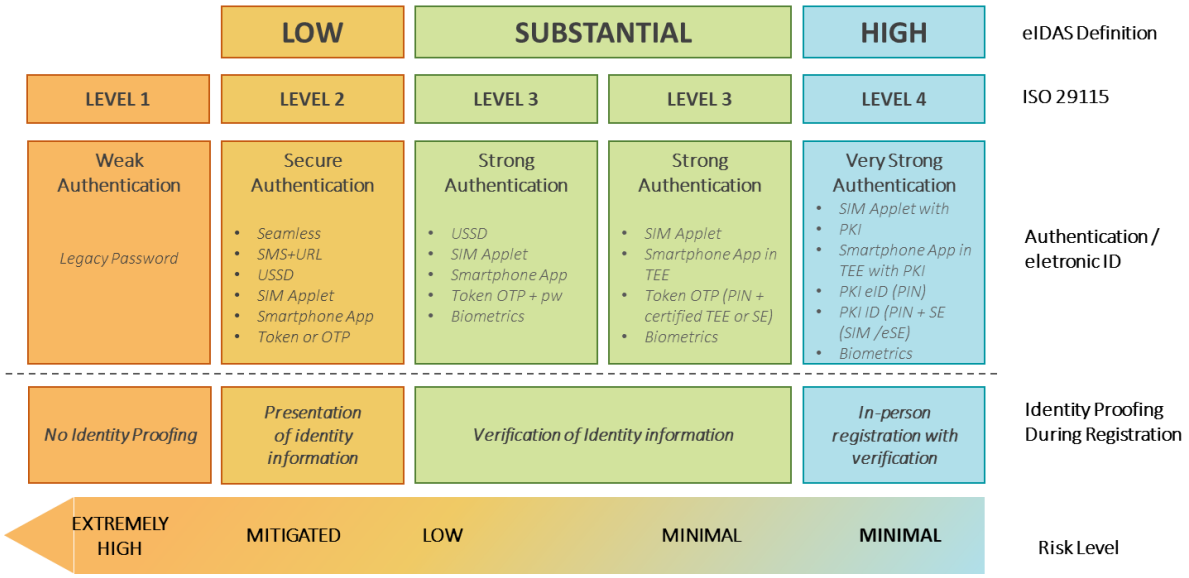

***Figure 2** – Digital identity levels (adapted from Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation)*

2.2. Previous and Current Projects

The electronic identification of individuals has been tackled over the years in different pan-European projects. One such project was the **S**ecure iden**T**ity acr**O**ss bo**R**ders lin**K**ed (STORK)[10], an eGovernment eID 'Large Scale Pilot' (LSP) that ran from 2008 to 2011. STORK aimed at creating a pan-European eID framework and infrastructure to allow EU citizens who are resident in a Member State other than their

[10] STORK | Take your e-identity with you, everywhere in the EU: https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu

own or work in one country and live in another one to access online public services wherever they are located. In that sense, it was the precursor to the current cross-border eID services of the CEF eID Digital Services Infrastructure. At the same time, the European Patient Smart Open Services (epSOS)[11] LSP was also running (epSOS-I, 2008-2011), focusing on piloting the cross-border exchange of Patient Summaries and ePrescriptions, being the precursor to the current CBeHIS of the CEF eHealth DSI[12].

The electronic identification and authentication in eHealth was first addressed in epSOS, by its Identity Management work package, with a view to providing a practical solution to run the LSP. In the scope of the coordination task between STORK and other LSPs, a liaison between STORK and epSOS was materialised in the 'STORK meets epSOS' (STepS) initiative (2009-2011)[13]. The goal was to explore synergies between both LSPs with regards to identity management, ensuring their coordination and enhancing the epSOS identity management processes with the STORK capabilities with regards to identification and authentication of natural persons (patients and health professionals). On the patient side, the selected use case would consist on the substitution of the traditional paper-based identification process in epSOS with the fully-fledged online process developed by STORK. On the health professional side, the focus was on increasing the strength of local authentication mechanisms and enriching the process with authorisation data.

The STepS exercise laid down the foundations for the specific eHealth pilot of the follow-up LSP STORK 2.0 (2012-2015)[14], which focused on:

1. The epSOS-II (2011-2014) Patient Access (PAC) use case: a patient identifying and authenticating, through STORK, against a foreign service provider to access his/her EHR;
2. Representative access to EHR: access on behalf of a patient (delegation / mandate);
3. HP identification: enabling local identification and authentication of health professionals through STORK, with retrieval of additional authorisation information.

All in all, STepS didn't bring a realistic approach to fruition, 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 professional, on behalf of the patient. As a result, epSOS did not address the issue of electronic patient identification. This topic was explored in the e-SENS LSP (2013-2017)[15], as part of its eHealth pilot, and the relevant contributions were invaluable in understanding the implications of eIDAS for cross-border eHealth. Apart from a legal analysis, e-SENS piloted different levels of eID in eHealth, from the baseline epSOS process to a distributed cross-border authentication using STORK 2.0 / eIDAS infrastructures, with a vision towards a fully virtual mobile eID

[11] Cross-border health project epSOS: What has it achieved?: https://ec.europa.eu/digital-single-market/en/news/cross-border-health-project-epsos-what-has-it-achieved
[12] eHDSI Starting Toolkit: https://ec.europa.eu/cefdigital/wiki/x/WKgSB
[13] STORK D7.11 - Implementation Report on eHealth LSP: https://ec.europa.eu/cefdigital/wiki/download/attachments/78558188/D7.11%20Implementation%20Report%20on%20eHealth%20LSP%20FINAL.pdf?version=1&modificationDate=1552376489209&api=v2
[14] STORK 2.0 - Secure idenTity acrOss boRders linKed 2.0 (STORK 2.0): https://joinup.ec.europa.eu/collection/secure-identity-across-borders-linked-stork/document/stork-20-secure-identity-across-borders-linked-20-stork-20
[15] e-SENS Pilots - 5.2.1 ePrescription / Patient Summary: http://wiki.ds.unipi.gr/display/ESENSPILOTS/D5.6-2+-+5.2.1+-+ePrescription_Patient+Summary

scenario. The work from e-SENS helped the Joint Action to support the eHealth Network (JAseHN)[16] to elaborate policy and recommendation papers on eID, which were adopted by the eHealth Network[17].

The latest of this series of projects is HEALTHeID (2018-2019)[18]. Benefiting from the lessons learned from e-SENS, this project introduced the paradigm shift in the current CEF eHDSI use cases needed to properly address the eIDAS Regulation, by offering a set of patient-directed online services as suitable candidates for a strong authentication of patients via the eIDAS infrastructure, empowering them through their personal smartphone.

CEF eHDSI builds on specifications initially designed in epSOS, thus inheriting much of its identity management processes. The importance of this topic is further reinforced in the Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth based on the criteria required for the participation in Cross-Border eHealth Information Services (Agreement), adopted by the eHealth Network in May 2017 and signed by the competent national authorities participating in the CBeHIS, with references, in its Clause II.1.1.2 and II.1.1.3, to the identification of patients, health professionals and healthcare providers as well as to the authorisation of a health professional. Although the work on eID in eHealth is far from recent, it hasn't yet made its debut in the currently operational CEF eHDSI services. A new project, X-eHealth (2020-2022), has a task that aims to leverage the experience of HEALTHeID and national projects of eID in eHealth to define a way towards a seamless cross-border eIDAS solution that can be finally integrated in CEF eHDSI, in line with the Commission Recommendation on a European Electronic Health Record exchange format. The eID is not the main focus of this project, however the inclusion of this kind of initiative in projects reflects the need for establishment of a strong eID Approach for health in EU.

Last but not least, a reference should be made to the CEF European Blockchain Services Infrastructure (EBSI), where the bleeding-edge use case of a European Self-Sovereign Identity Framework (ESSIF) is being explored, envisioning an individual in full control of their identity (e.g. via a digital identity wallet)[19]. The eHealth sector should keep an eye on this project, not only due to its innovative use of digital identity data, but also to its draft amendments of the eIDAS Regulation[20], the consequences of which for the eHealth sector are still unknown. The current revision of the eIDAS Regulation should also be scrutinised.

[16] JAseHN: https://webgate.ec.europa.eu/chafea_pdb/health/projects/677102/summary

[17] Policy paper on eID specific framework for eHealth - Release 1: https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20170509_co04_en.pdf

Policies Regarding eIDAS eID and Health Professional Registries: https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20180515_co11b_en.pdf

[18] HEALTHeID: https://www.spms.min-saude.pt/healtheid/

[19] About SSI eIDAS Bridge: https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about

[20] Introducing the SSI eIDAS Legal Report: https://ssimeetup.org/introducing-ssi-eidas-legal-report-ignacio-alamillo-webinar-55/

2.3. Policy and Legislation

In the context of regulation and standardisation at the EU level, the following stand out:

- 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: this so-called 'eIDAS Regulation' aims to guarantee the use of national eID systems to access public services in other EU countries where eID systems are available.
- 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 (General Data Protection Regulation) (Text with EEA relevance)
- Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare: EU directive on the right to exercise access to cross-border healthcare.
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union: the so-called 'NIS Directive' on security of network and information systems provides legal measures to boost the overall level of cybersecurity in the EU.
- The Commission will come in 2Q 2021 with a proposal for an EU-wide framework for secure public electronic identification. Offering a framework for the use of digital identity attributes (eHealth attributes among others) linked to identity to all European citizens is being considered in this context.

In the international context, highlighting the contribution from the International Organisation for Standardization (ISO) relating to management of authentication: the ISO/IEC29115:3013 standard identifies four levels of assurance of authentication and proposes measures to reach each of the four levels and guidelines for mitigating threats.

3. Brief Definition of Use Cases

This chapter aims at contextualising the need for the establishment of a common eID Approach for health within the EU by presenting the two most common identification use cases (value propositions) of the healthcare sector: identification of patients and health professionals.

3.1. Electronic identification of Patients – use case

Patient identification is the process by which the set of attributes describing the identity of the natural person interacting with health services (either the patient seeking healthcare or managing his/her own health data) are unambiguously recognised. The result of patient identification and authentication is a proof that the patient is who they claim to be. Electronic identification of patients is the process by which the patient identification and authentication is established using any electronic means or, using eIDAS terms, is the process of using person identification data in electronic form uniquely representing a natural person (the patient). While recent health data access models were born with electronic patient identification in mind (e.g. patient access to their own data through a portal or app), more traditional business processes where the patient is identified by a health professional (e.g. by presenting an identification card to the admission clerk) still rely on purely non-electronic and passive participation of the patient. Patient eID has the power to turn the patient into an active participant in this process, elevating the strength, assurance and trustworthiness of the claimed identity by exploring new generation technologies and digital infrastructures (some emerging from recent regulations, e.g. eIDAS or GDPR).

Specifically, in the case of CBeHIS, in the current eHDSI deployment, the patient identification process is performed by the HP, and the patient is identified and authenticated using demographic data, without any kind of eID, based on the national policies for patient identification in the country of affiliation. After successful identification of the patient by the country of affiliation, the HP still has to verify, by themselves, the demographic data returned against the one present in the identification document provided by the patient. As the eHDSI has already shown, there is a wide variety of identification means available across Europe. Even within a single country, more than one may be available. This creates a huge burden for the HPs of the country of treatment, forcing them to be aware of this diversity and to perform the manual identity confirmation in order to adequately identify a foreign patient (an administrative duty which is alien to the HP's regular organisation of work). Electronic identification removes such barriers and opens the possibility for patient self-identification and authentication. On the other hand, electronic identification by the HP could also create certain challenges such as the need to support a large number of eID schemes (even if these are only software-based) used in other Member States in every single point of care. A possible solution could be a common software-based eID standard which all Member States agree to support. Finally, the usage of eID for patients should take into account scenarios such as break-the-glass, wherein the urgency of healthcare is of the utmost importance and certain safeguards are allowed to be bypassed.

Research on Master Patient Indexes have shown that patient identification based on human handling of demographic data (subject to the risk of misspellings and other mistakes) results in a relevant rate of patient mismatching and duplication of records. 'Reasons that duplicate records continue to plague healthcare systems include varying methods of matching patient records; departmental system silos; lack of data standardisation; lack of policies, procedures, and data ownership; frequently changing

demographic data; multiple required data points needed for record matching; and default and null values in key identifying fields.' Study authors conclude that 'To improve patient matching, increasing the use of more sophisticated technologies is critical. For example, using biometrics, smart card readers, and advanced algorithms (...)'. Electronic identification of patients comes in a way to guarantee uniqueness in patient identity, helping to solve these issues and, in the end, increasing data quality.[21]

Based on the two previously mentioned patient-centred approaches to health services – seeking healthcare and managing their own data – the following non-exhaustive list of use cases demonstrate the potential for benefitting from electronic identification of patients:

- Patient admission at the admission desk/counter: patient could be identified through, e.g. mobile means, in the best case avoiding even the waiting line/time and the contact with the admission clerk;
- Person acting on behalf of: this would allow proper and secure identification in cases where the data subject (the targeted patient) is not the person directly requesting the healthcare service. This use case is currently being developed in CEF eHDSI. Examples of its application include:
    - ePrescription/eDispensation in a pharmacy: electronic identification of the person acting on behalf and, additionally, triggering the electronic identification of the patient he/she is acting on behalf of (e.g. sick patient at home being requested to identify through mobile means upon a relative's request for dispensation of his/her medication at a pharmacy), allowing a fully informed dispensation by the pharmacist;
    - Patient Summary: the patient is a minor and one of the parents must be electronically identified to give the HP access to the minor's Patient Summary document. Another case is when the patient is an incapacitated or disabled adult and another person is authorised/entitled to act on their behalf;
- Consent (or other legal document) provision: patient eID would increase the authenticity, correctness and non-repudiation of electronic consents and other legal documents stemming from GDPR, strengthening the certainty of this legal act. The cross-border version of this use case was, to some extent, explored by the HEALTHeID project, where patient eID enables the proper acknowledgement of the Patient Information Notice of the country of treatment (as deemed necessary according to the GDPR);
- Patient access to their own laboratory results, e.g. exploring patient eID as a secure means of accessing this kind of information in its cross-border fashion (following one of the new information domains identified in the Commission Recommendation about Electronic Health Record Exchange Format[22]);

[21] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4832129/

[22] https://ec.europa.eu/digital-single-market/en/news/recommendation-european-electronic-health-record-exchange-format

- An emergency call centre health professional being able to automatically and securely identify a patient, leveraging the latter's mobile phone as an eID means;
- A patient sharing his/her own health data collected from personal devices (e.g. wearable devices): patient eID would allow immediate sharing of such data with health professionals and its aggregation in the patient's EHR;
- Patient eID as a means for closely-linked cross-sectoral cooperation, e.g. identifying the patient as an insured person under the Electronic Exchange of Social Security Information (EESSI) domain (Annex 4).

Other emerging use cases should also be considered to be included on the eID use cases with focus on the patient-centred approaches to health services, at national and cross-border levels. During the COVID-19 pandemic there is a pressing need to support new use cases (e.g. vaccination/test proofs or vaccination appointments). The common eID Approach should be aware of the emerging use cases and be able to identify and define a specific implementation plan and adopt it in a short-term Approach, ensuring the further high-quality provision of healthcare assistance regarding these new use cases.

Cross-border use cases can find in the reuse of the CEF eID Building Block a good ally for proper eID implementation. The benefits of patient eID reflect on the patient identification process, the first step of the current eHDSI use cases, as already described. On the other hand, a cost-benefit analysis of the usage of the eID Building Block on a case-by-case basis would be warranted.

This means that overall, accurate and secure patient identification introduces several benefits in healthcare in the areas of patient management and treatment (e.g. improved quality of care; transition and continuity of care; reduction in duplicate diagnostic testing; longitudinal healthcare record), health insurance and benefits programs (e.g. streamlined billing and claims processing; reduction of fraud) and data collection for planning and research (e.g. public health; big health data).[23]

3.1.1. Known used standards and means

Since electronic-based identification of citizens began to be a matter of concern for society, both public and private sectors of the political-economic spectrum started to address the technological challenge mainly from the same perspectives:

- **Technology:** Realising how the most recent electronic devices and systems, over the years, could provide ways to identify a person;
- **Social engineering:** Taking advantage of the technological possibilities and finding how to use them for identification purposes, causing the least possible impact in the society habits and routines.

[23] http://documents.worldbank.org/curated/en/595741519657604541/The-Role-of-Digital-Identification-for-Healthcare-The-Emerging-Use-Cases.pdf

In this sense, the citizen identification systems moved from credential-based authentication applications to mobile-based authentication systems, going through several stages of evolution, such as the usage of smartcards for the purpose.

Although the eID trends followed by countries all over the world share the principles described above, the same cannot be realised when analysing the system implementations, that were designed and built to serve eID purposes of each country/geopolitical area; in other words, each implementation standard of eID relies on the administrative environment variables (e.g. politics, demography, administrative division, economy, etc.) of the region where it was implemented.

Taking into consideration only the technological aspects, nowadays there are several identification standards, or proof of concept projects, with capabilities to provide support for the wanted purpose for citizen identification. In the following paragraphs, the results are presented of an analysis made about available techniques that are, or could be, used to identify a patient against a healthcare related system.

- **Credential based authentication** – An authentication based on a secret shared between the user and the system (e.g. a password). Regarding the password lifecycle, a password can be persistent over time, or can be used only once (an **OTP**, one-time-password), usually requested/acquired through mobile devices (e.g. using an IVR system, SMS or other dedicated systems like **QR code generators**).
- **Smartcard Authentication** – A standard that uses the information contained in the smartcard to identify the user, although to grant the access to that information it is always necessary for the user to introduce a PIN to assure the authenticity. These systems are widely used by governments to provide identification documents in this format (e.g. citizen cards, Foreign Cards, Diplomatic Identity, etc.).
- **Mobile Authentication** – A system that identifies the user by the identification of their smartphone, making use of some technological frameworks, such as special SIM cards or the identification of the device itself containing private keys of the user in systems based in asymmetric-encryption for authentication.
- **Biometric Authentication** – A standard that makes use of biometric characteristics (e.g. iris, fingerprints, etc.) of a user to identify them against the system. Nowadays, with the growth of the use of smartphone computing capabilities and their proliferation among the general population, these identification systems now have a renewed importance since it is possible to perform biometric recognition through a mobile device anywhere.

As it was stated previously, although these technologies are used widely all over the world, there is no mainstream standard used, not even agreed, inside the EU context, causing every identification authority to define its own implementation/usage protocol. In Annex 1, the overall state of play about this matter across the EU is depicted, presenting the technologies/protocols adopted or under development for eID purposes within each country. Moreover, specific constraints may apply in the context of healthcare provision, as some means of identification cannot be applied in specific situations, e.g. due to patient's acute health condition, deteriorated health, or lack adequate of e-skills.

3.1.2. Electronic identification constraints and challenges

An **electronic patient register** is required for both national and cross-border data exchanges, as a means to identify the natural person engaging with the healthcare service and properly connect

him/her to his/her clinical data through one (or a combination of) identifier(s). Thus, setting up of such digital infrastructure is seen as a mandatory step to achieve proper electronic identification of patients. This encompasses not just the technical activities of creating the registry and enabling connection with specific eID means of the end-user but also the organisational activities, related to the updating of patient data collected during his/her encounters with the healthcare services and the definition of business processes needed to qualify the patient register with an authoritative and trustworthy status. Furthermore, in the legal field, challenges arise with regards to GDPR-compliant processing of personal data, but also national legislation for setting up and operating existing or future national patient registries may vary significantly between Member States, for example in their content, scope, use case and level of detail.

Constraints exist in current business processes where a health professional performs patient identification on the patient's behalf. Moving to a patient-centric electronic identification demands a significant shift in the current paradigm of these business processes, impacting the people, as well as the organisations. New business processes, potentially changing in a significant way the actors and their interactions, need to be defined and integrated into daily organisations' routines in the smoothest way possible. The eID aproach and policies shall support an intensive programme on digital literacy for eID at different levels (patients, HPs, organisations and decision-makers).

Other constraints exist with regards to the eID means. The usage of physical-token eID means (e.g. smartcards) demand additional hardware and software solutions at the point-of-care, which increase the operational burden of such eID solutions, from technical, organisational and financial points of view (e.g. rollout of smartcard readers in the healthcare institutions of a country that should be compliant with ISO 7816[24], leading, if needed, to be installed properly in order to read up to 20 different smartcards and in some cases, change hardware e.g. contact vs contactless). Such constraints also apply in the case of a patient-triggered eID (e.g. the burden of a patient having to have a smartcard reader to authenticate against his/her patient portal). Therefore, virtual authentication schemes can be the preferred approach to overcome this challenge.

On an organisational level, governance and operation of healthcare services and national eID schemes may fall under the responsibilities of different organisations and ministries. Policies for these two different worlds may be provided by different cooperation groups. Most notably, in the cross-border world, we have the eHealth Network and the eIDAS Cooperation Network as the policy bodies ruling the procedures to be followed by organisations and ministries of each realm. Connecting eID to eHealth will demand a close alignment between these kinds of entities, both at national and EU levels. Healthcare may already have a legacy means of electronic identification, and implementation of new eIDAS compliant means may thus require substantial investments in ICT infrastructure and applications, such as investment in new eID reading devices and implementing software services for provision of healthcare - specific identifiers.

[24] https://www.iso.org/obp/ui/#iso:std:iso-iec:7816:-8:ed-4:v1:en

3.2. Electronic identification of Health Professionals – use case

HP identification is the process by which the set of attributes describing the identity of the natural person interacting with health services (the HP providing healthcare) are unambiguously recognised. The result of HP identification and authentication is a proof that the HP is who he/she claims to be and that he/she is entitled to access health data. Electronic identification of HPs is the process by which the HP identification and authentication is established using any electronic means (eID) or, using eIDAS terms for online services, is the process of using person identification data in electronic form uniquely representing a natural person (the HP). Authorisation to access particular types/sets of data is defined based on the role and profile of the HP.

With the emergence of EHRs, electronic identification of HPs became a reality and is now common practice. But there is a huge diversity in eID means: they vary within an organisation and between software vendors, groups of health professionals, country regions and between countries. Additionally, some of these means may not provide the necessary level of assurance needed for the processing of health data by the professionals, in accordance with the recent data protection legislation.

There is a need to introduce, maintain and interconnect heath professional registries for authentication of health professionals. Apart from eIDs, the registries shall provide information about professional qualifications as an essential criterion to evaluate rights for access to health data. As the source of authoritative information, health professional registries should fulfil minimum requirements for accurate and secure identification, authentication and authorisation of health professionals. The heterogeneity of registries may raise some concerns on their regulation, data quality, control and trustworthiness, once they are integrated through eID means. Having a common vision and approach for HP eID in Europe would assure a least common denominator on electronic identification processes and means, guaranteeing appropriate security levels, legal certainty and completeness of information.

The European Commission identified the need for the creation of a common European Health Data Space, which would foster the sharing of different kinds of health data within the EU, thus supporting the delivery of healthcare, as well as the development of new treatments, medicines, medical devices and services[25]. Regarding the current situation related to the COVID-19 pandemic, information exchange to support research and statistics has become more urgent.

The following non-exhaustive list of use cases demonstrate the potential for benefitting from electronic identification of health professionals:

- Consent (or other legal document) provision: to trace to whom the patient provided his/her consent or other legal document stemming from GDPR;
- Secondary use of data: promote cross-border health-data exchange to support research and statistics in the field of health;
- Telehealth: accurate identification of the HPs participating, e.g. in a video-call;

[25] https://ec.europa.eu/digital-single-market/en/news/member-states-meet-european-commission-discuss-protection-personal-data-health-sector

- Referral management: to have a full trace of referrals between HPs, their specialties and the healthcare organisations in which they are working;
- Mobile ePrescription or Death Certificates: ensuring access of HPs to mobile versions of these use cases and secure linkage for the HP authoring of these clinical documents;
- Digital Signatures by health professionals: eID can be applied for digital signatures of discharge reports, medical certificates and other types of medical documents that need to be duly signed by a health professional;
- All the use cases included in the Commission Recommendation about EHRxF: Patient Summary, ePrescription/eDispensation, Laboratory results, Medical imaging and reports, Hospital discharge reports
    - Enriching the cross-border exchanged documents with trustworthy information on the identity of the HP (or HPs) who authored the clinical document;
    - Allowing fine-grained traceability of the requester of clinical data on both countries;
    - Elevating the trust, by the country of affiliation, in an identification and authentication process carried out by the country of treatment.

Similarly, relating to the patient ID use case, cross-border use cases may explore the reuse of the CEF eID Building Block for proper eID implementation. The benefits of HP eID reflect on the HP identification process, a prerequisite of the current eHDSI use cases.

Consequently, all use cases starting with the identification of the HP have increased benefits, although implementation costs should also be taken into account.

3.2.1. Known used standards and means

Regarding the identification of a professional against an IT system, in broad terms, is in fact based on the premise that a professional is, first and foremost, a citizen. In this sense, and in general, currently the methods used to enable professional authentication does not depend on an interface used to perform identification, it is mostly based on the capability of the corporate dedicated systems to establish the connections between citizen metadata and its certified professional.

Following this principle, both private and public corporate entities implemented their own identification systems based on the technological trends enunciated in section 4.1.1, taking advantage of the intrinsic features that a dedicated system has to offer in this context:

- **Data Ownership** – Once a system is designed and implemented to serve the requirements of a determined organisation only, it can be adapted to use every kind of person identification, because the correlation between an identified citizen and its professional data is made by the system itself, and does not depend on the identification interface (e.g. citizen smartcard, credentials, etc). At this level, as the professional metadata of the users is managed by the same system that uses it to grant professional identification, the information distribution among systems opened a set of advantageous opportunities of interoperability and integration between different platforms.
- **Interoperability and Integration with third-party systems** – Due to the distribution of the data operated by each organisation to perform professional identification, third-party platforms

(e.g. Active Directories; Microsoft Office 365) began to be used as a data source to perform identification of users, taking advantage of some organisational processes already consolidated, such as the mandatory usage of Office 365 accounts to enable user authentication inside a corporate IT applications domain.

Regardless of the consolidated identification paradigms, nowadays, as consequence of some initiatives about personal and professional data aggregation in the context of eID purposes, it is already possible to commute the mainstream paradigm of professional information distribution, gathering that data in the same format as the adopted standards for personal identification. In this sense, there are already some projects, at different levels of reliability and execution, to unify both personal and professional identification in the same process and using the same technological interfaces (e.g. Professional Attributes Certification System in Portugal); more details are presented in Annex 1.

3.2.2. Electronic identification constraints and challenges

An electronic register of health professionals (one or more, according to national needs) is required for both national and cross-border data exchanges, as a means to identify if a person or an entity is entitled to access particular sets of data. Thus, setting up such digital infrastructure is seen as a mandatory step to achieve proper electronic identification of health professionals. This encompasses not just technical activities of creating the registry and enabling connection with specific eID means of the end-user but also organisational activities related to the engagement of national health professionals' associations and the definition of business processes needed to qualify the health professional register with an authoritative and trustworthy status. Furthermore, in the legal field, challenges arise with regards to GDPR-compliant processing of personal data, but also national legislation for setting up and operating existing or future national professional registries may vary significantly between Member States, for example in their content, scope, use case and level of detail.

The guideline of the Joint Action to support the eHealth Network on 'Interoperability of Electronic Professional Registries'[26] explores the idea of defining a minimum common denominator for data elements representing relevant health professional information, considered sufficient for interoperability purposes. In addition, such a document could not extract in detail the semantic requirements of such an interoperability scenario, e.g. the need for an associated controlled vocabulary to enable transformation, translation and encoding of the national health provider information into a pan-European format. Thus, a close link to the eHN's Semantic Subgroup is anticipated, to properly address the semantic aspects of the controlled vocabulary and any other related semantic requirements; not as a replication, but to ensure similar logics are used, and also since many semantic knowledge bases have been used to characterise professionals (e.g. what is meant by midwife, or nurse, may seem obvious but, without a clear commonly-agreed meaning, what some countries call one or the other may differ). A link to 'common professionals' recognition' across the EU and the Commission units working on that is likely to be needed at some stage.

Other constraints exist with regards to the eID means. The usage of physical-token eID means (e.g. smartcards) demand additional hardware and software solutions at the point-of-care, which increase

[26] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20170509_co05_en.pdf

the operational burden of such eID solutions from the technical, organisational and financial points of view (e.g. rollout of smartcard readers over the healthcare institutions of a country). Therefore, virtual authentication schemes can be the preferred approach to overcome these challenges.

Just like the patient eID use case, other constraints can be found in the adaptation of business processes to eID, potentially changing some actors and/or interaction patterns, impacting on people and organisations. To assure smooth adoption of eID, approach and policies shall support an intensive programme on digital literacy for eID at different levels (HPs, professional associations, organisations and decision-makers).

As in the patient eID use case, on an organisational level, governance and operation of healthcare services and national eID schemes may fall under the responsibilities of different organisations and ministries. Policies for these two different worlds may be provided by different cooperation groups. Most notably, in the cross-border world, we have the eHealth Network and the eIDAS Cooperation Network as the policy bodies ruling the procedures to be followed by both the organisations and ministries of each realm. Connecting eID to eHealth will demand a close alignment between these kinds of entities, both at national and EU levels.

4. Policy and Governance Structure description

4.1. Guiding Principles

The principles defined in this chapter enable a structured cooperation between the different stakeholders belonging both to the public and private sector.

Universal Coverage – Inclusion – Simplicity

- Ensure access by health professionals who work in the public and private sectors;
- An individual's use of their digital identity should be simple and intuitive.

Integrity – Security – Confidentiality

- Ensure data consistency;
- An individual has the right to keep their digital identity information private;
- The use of digital identity to access the patient's clinical information must guarantee data security and privacy. The professional who accesses the data must have permission to access it.

Open Data – Openness – Reusability[27]

- Adoption of standards and norms to facilitate interoperability;
- The level of openness of a specification/standard is decisive for the reuse of software components implementing that specification;
- All stakeholders have the opportunity to contribute to the development of the specification and a public review is part of the decision-making process;
- The specification is available for everyone to study;
- Reuse and share solutions and cooperate in the development of joint solutions when implementing EU public services.

Once-Only Principle[28,29]

- Ensure that citizens and businesses are requested to supply the same information only once to a public administration;
- Citizens and businesses should not have to supply the same information to public authorities more than once for the cross-border exchange of evidence.

Building and Sustaining Trust – Transparency – Data Privacy – Fair Use

- Ensure privacy and data protection;

[27] https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf
[28] Proposal for a Regulation of the European Parliament and of the Council on establishing a single digital gateway to provide information, procedures, assistance and problem solving services and amending Regulation (EU) No 1024/2012, COM(2017) 256 final, 2017/0086 (COD) https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017AE2781
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017XX1011(01)&from=PT

- Right to know who had access to the data – transparency regarding who accessed it.

User Centricity – Ownership – Consent

- An individual's digital identity should not be used or shared without their explicit consent, or as permitted by law;
- Individuals own their identity and personal data.

Zero trust principle

- Treat everything connecting to eHealth infrastructure as untrusted until an access request (by patient/HP) is unambiguously identified.

4.2. Proposed Governance Framework and Involvement with Stakeholders

In order to ensure the fulfilment of a Common eID Approach for Health, the eHN is asked to indicate (e.g. eHN Technical Sub-group) or create a group as an intervening of a robust and stable governance model. This group will be responsible to manage the eID approach, and to coordinate and support its development. Within the digital identity ecosystem there is a set of primary stakeholders that play complementary/supporting roles in the eID processes in the context of each country. The governance model is the key to achieve overall coherence in the eID approach.

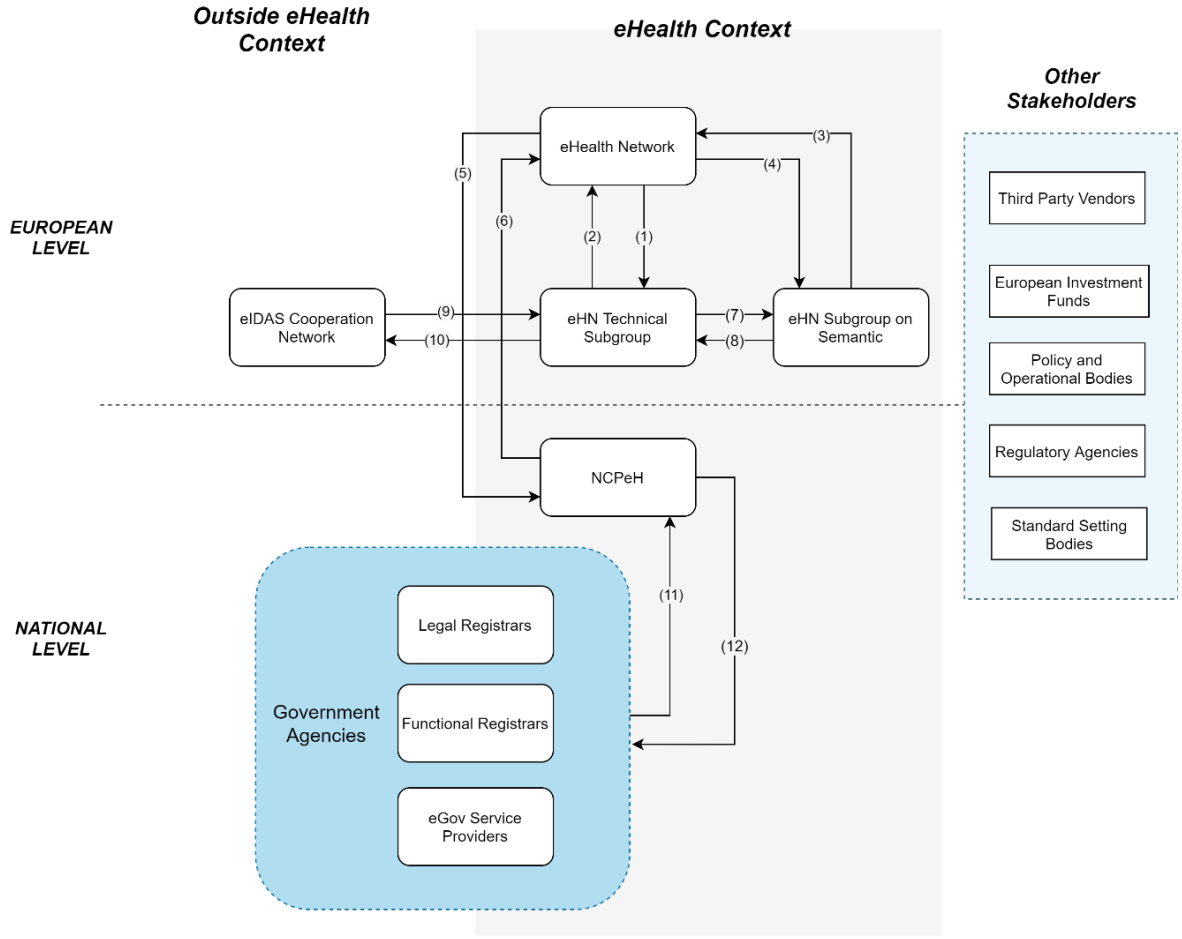

***Figure 3** – Proposed governance framework for Health eID in the EU*

Relations between the bodies:

***Relationship 1 and 2:** the eHN technical Subgroup supports the eHN on technical issues. This group is focused on the use cases.*

***Relationship 3 and 4**: the eHN Semantic Subgroup exerts its functions under the eHN scope. The eHN Semantic Subgroup shall propose semantic guidance to the eHN for endorsement, in this way acting as a consulting body to the eHN, which in return shall take the eHN Semantic Subgroup's proposals and structure them as EU level guidelines.*

***Relationship 5 and 6**: the NCPeH uses the guidelines and recommendations produced by the eHN in order to take forward the deployment/operation of the cross-border services. The NCPeH is the national body responsible to exchange the national data in the cross-border context.*

***Relationship 7 and 8**: these Subgroups are under the influence of eHN and have strict communication between them in order to achieve mutual support.*

***Relationship 9 and 10**: the eIDAS Cooperation Network will exchange information regarding good practices on electronic identification schemes with the eHN Technical Subgroup to ensure an alignment about the use of eID on national and cross-border contexts.*

***Relationship 11 and 12**: the relationship between NCPeH and the Government Agencies can be managed directly with Legal Registrars, Functional Registrars and eGov service providers or could be performed by an intermediate agency.*

***Other Stakeholders** represent additional different parties that have an interest in the development of eID and can either affect or be affected by the course of the eID initiative. The eID approach must have a close relationship with the other stakeholders to ensure the development of this approach. These stakeholders can be important in some phases of the approach.*

A brief description of the main stakeholders and their roles in the digital identity ecosystem is provided in Table 2. Each stakeholder is intended to define a relevant organisation that may be set up at a national, EU or global level in order to support or carry out follow-up actions related to digital identification. The stakeholders were organised within the following two fundamental categories[30]:

- ***Government Agencies*** – comprising national bodies that play one or more principal role(s) in the digital identification lifecycle.
    - ***Legal registrars*** are the agencies in charge of providing legal identification to citizens. These may include national identification authorities in charge of creating and maintaining national ID cards and other documents.
    - ***Functional registrars*** are agencies that create and maintain identity registries for a specific purpose or service, e.g. Medical Council, Pharmaceutical Society and other Health and Social Care Councils and identity provider agencies responsible for registries of health professionals.
    - ***eGov service providers*** are government agencies or platforms that provide online services to citizens or residents which require some proof of identity and entitlement.

- ***Enablers*** – agencies which enable and support the identity systems. These enablers can operate at an EU and global Level.
    - ***Regulatory agencies and organisations*** regulate, control and audit digital identity systems. The goal of these actors is to ensure that digital identity and authentication providers follow legal standards and best practices for the collection, storage, and use of personal data.
    - ***Standard setting bodies*** are organisations that provide protocols for digital identification and authentication. The goal of these agencies is to increase interoperability and build open and scalable identity solutions.
    - ***Policy and operational bodies*** are agencies which enable and support identity systems at a strategic, technical and operational level.

It is important to highlight that Table 2 presents a general view about the stakeholders' role in the eID ecosystem, however they can be different among the Member States due to different types of organisation.

[30] Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation

	STAKEHOLDERS	PROVIDERS	ROLE
GOVERNMENT AGENCIES	***Legal Registrars***	**NATIONAL LEVEL** • National ID Agency; • Birth Register; • Passport Agency; • Ministry of Interior	• Digital ID providers • Attribute providers • Authentication providers • Service providers
	Functional Registrars	**NATIONAL LEVEL** • Health and Social Care Councils or Professional Associations, such as Medical Council or Pharmaceutical Society • Agencies for Registers of Health Professionals • Hospitals • Primary Care	• Digital ID providers • Attribute providers • Authentication providers • Service providers
	eGov Service Providers	**NATIONAL LEVEL** **(examples of eGov Service Providers)** • e-Identita, I.CA (Czech Republic) • SI-TRUST (Slovenia) • EESTI (Estonia) • Autenticação.Gov (Portugal) • State Treasury (Hungary)	• Authentication providers • Service providers • Service entitlement authorisation providers
ENABLERS	***Regulatory Agencies***	**NATIONAL LEVEL** • National Data Protection Authority **EUROPEAN UNION LEVEL** • European Data Protection Board	• Regulation & oversight
	Standard Setting Bodies	**GLOBAL LEVEL** • Global Digital Health Partnership • International Organization for Standardization • International Electrotechnical Commission	• Standard setting • Provide technical and data standards • Build trust • Support information security and cybersecurity
	Policy and Operational Bodies	**EUROPEAN UNION LEVEL** • DG DIGIT • DG CONNECT • eHealth Network • eIDAS Network • CIO Network • eGov Steering Board **NATIONAL LEVEL** • Ministry of Defence – Committee of Digital Security • National Health Insurance • State Audit Office • Ministry of Health • Ministry of Finance	• Entitled to EU healthcare services with European Health Insurance Card (EHIC)

Table 2 *– Key identity stakeholders and their main roles*

5. Recommendations

Following the need for common electronic identification, recommendations on how to address this issue are provided.

Recommendation 1: Preferable use of eIDAS infrastructure, for the cross-border eHealth context

The use of cross-border authentication through the eIDAS Infrastructure (Opinion No. 5/2019 of the Cooperation Network on version 1.2 of the eIDAS Technical specifications[31]) provides a clear legal framework, both for interoperability and level of security/assurance. The eIDAS Regulation provides a reliable, and convenient manner for online services to identify their users. Is important to note that these services are applicable only for online services.

Recommendation 2: Development of software based eID Strategy for eHealth services

Considering the trend towards mobile services, eID schemes should be provided in mobile compatible forms. Each Member State should ensure that authentication schemes are suitable for mobile and ensure the development of a mobile-friendly service when choosing the appropriate eID scheme. This consideration is aligned with the recent Commission Recommendation '*Embracing mobile identity for eGovernment*'[32] in relation to mobile eID. The strategy must ensure a fallback mechanism to the traditional identification means for the particular cases where the patient is unable, for some reason, to use these innovative solutions. Some notified eID schemes under eIDAS which are mobile oriented have LoA 'high', i.e. comparable with the LoA of smartcards.

Recommendation 3: Ensure that the use of the traditional identification means for offline services (e.g. citizen card, passport) is still a possibility

Even with the development of electronic means of identification, the Member States should ensure that traditional means of identification for the use cases in offline services be possible. For offline (in person) services provided at the point of care, the use of an eID scheme should be possible but optional.

Recommendation 4: Use of a sector-specific eID scheme, with a sector-specific patient identification number for eHealth use cases

The use of a sector-specific eID scheme, with a sector-specific patient identification number, should be preferred. In those cases where the use of a specific health eID scheme is not possible, the use of a national eID scheme is recommended, whether notified under eIDAS or not, with a unique identifier

[31] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=148898549

[32] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2020/05/06/Embracing+mobile+identity+for+eGovernment?pk_campaign=XSELL-Bulletin49-202005&pk_source=email&pk_medium=CEFbulletin&pk_content=success_story

that is used as the patient identification number for eHealth use cases. This could be possible through reconciliation between eIDs from the multiple national sectors. Nevertheless, appropriate personal data protection measures must be considered. For both offline and online digital health services, further work is needed for citizen eID schemes. The work should focus on the interoperability of already-existing healthcare-specific citizen eID schemes in the Member States.

Recommendation 5: Use of a sector-specific eID scheme, with a sector-specific health professional identification number for eHealth use cases

The use of a sector-specific eID scheme, with a sector-specific health professional identification number, should be preferred. In those cases where the use of a specific health eID scheme is not possible, the use of a national eID scheme is recommended, with a unique identifier that is used as the health professional identification number for eHealth use cases. Nevertheless, appropriate personal data protection measures must be considered.

Recommendation 6: Implementation of a 'High' Level of Assurance for health professionals

The security and integrity of health data is key for patients, doctors and other health professionals in research and innovation uses and for society, as a whole, to preserve potential information assets. Access to health data must be independent of where the data is located and must comply with GDPR and other data protection legislation. What must be guaranteed is that unauthorised access will never occur; the system must be set up to prevent this. It is advisable to set this aim along the lines of 'zero trust'[33], which is becoming commoner nowadays. This principle excludes the possibility of human faults or malicious activity in the operation of the systems. In order to ensure that these statements be achieved, the Level of Assurance of the eID schemes should be 'High' (at least to the equivalent of two-factor authentication), preferably targeting the eIDAS concept of 'High', to allow trust in the related services, as portrayed in Figure 2, Chapter 2. However, the use of the eIDAS-compliant schemes should be optional.

Recommendation 7: Use of sector-specific non-notified eID schemes for cross-border eHealth use cases (eID schemes outside the eIDAS Regulation)

In cases where it is not possible to use eIDAS-notified eID schemes, the use of national health sector-specific eID schemes (e.g. with unique patient or health professional identifiers and further demographic data) is recommended. These eID schemes are provided by the national identity issuers where the identity data are managed (e.g. health insurance companies or medical associations).

In a cross-border context, patient or health professional identification can always be ensured without eIDAS eID schemes in accordance with data protection laws. The fact that proof by means of notified eID means can be suitable in terms of data protection law does not oblige exclusive use of these notified eID schemes.

[33] Zero Trust – Treat everything connecting to eHealth infrastructure as untrusted until the patient or healthcare professional requesting access is unambiguously identified

The eHN highlighted, in its 16th meeting[34], that '*some Member States remarked that there are new technologies and possible identifiers not notified under eIDAS framework. It is important to ensure that the proposals on the table are open but new possibilities also fit the purpose of healthcare and are not just pushed by other sectors'.*

Recommendation 8: Member States should create the conditions necessary for their national bodies to set up and govern eID schemes

Member States should use their national government structures to provide eID schemes and/or improve the existent schemes in order to achieve a high level of assurance and their use in the health context.

Recommendation 9: The need for specific value sets to support eID use cases should be referred to the eHN Subgroup on Semantics.

For countries who have a national value set for professional categories, performing mapping between international standards and national code systems is recommended. The adoption of standards to ensure interoperability principles is recommended. Consequently, the analysis of ISCO-08[35] (International Standard Classification of Occupations) is required for the eHN Subgroup on Semantics. This classification organises jobs into a defined set of groups according to the tasks and duties undertaken in the job.

Recommendation 10: The eHealth Network should promote the necessary work to fulfil the eID use cases

The eHN should support the development of the eID use cases on the national and cross-border levels for the Member States, taking into account the different eID schemes among the Member States.

Recommendation 11: Extend the health eID to reach also the private sector, for cross-border sharing of information[36]

The eHN could promote the use of the national eID schemes for Health in the private health sector. It is important to support an effort to converge towards the approach to achieve a common eID for Health in the EU.

[34] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20191128_sr_en.pdf

[35] https://www.ilo.org/public/english/bureau/stat/isco/isco08/

[36] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-

Recommendation 12: The possibility of developing and adopting a common eID for all Member States should be considered[30]

The eHN should promote the adoption of eID schemes for digital identification among the EU Member States. The EU is developing and improving the interoperability framework of the eHealth sector and it is fundamental that the all Member States consider adopting the common strategies to strengthen the sector and ensure the correct identification of citizens (patients and health professionals) wherever they are in the EU.

Recommendation 13: Coordinating the development of the eHealth eID with the future European Digital Identity

The new Commission proposal for a trusted and secure European Digital Identity covering all EU citizens expected in Q2 2021 may bring important benefits to identification in the health sector. The development of eHealth eID cross-border should be closely coordinated with this project to avoid overlap.

6. Roadmap

The following section shows a roadmap for the different aspects of the common approach at high level (6.1) as well as at the goal/objectives level (6.2).

6.1. Roadmap for approach approval and implementation

6.1.1. Preparatory phase (September 2019 – March 2021)

The approach building process required alignment between different Directorates-General of the European Commission and the Member State co-chair of the eHN between September 2019 and March 2021, and the acceptance by the eHAction Steering Council of its inclusion as a possible extra activity between April 2021 and the official start of its implementation.

It is key to interlink between DG DIGIT (and CIO Network) and DG CONNECT (and eGov Network and eIDAS Trust Services Workgroup) activities on this matter, and as such this document shall be presented and further discussed with all parties, given their roles in the subject being discussed. The Commission is currently evaluating the eIDAS regulatory framework[37] and ran an open consultation from 24 July to 2 October 2020. It is important to consider the revision of the eIDAS and the emergence of new technologies, in the elaboration of this document, in order to support the continuous development/improvement of eID schemes among EU Member States.

There was full agreement on the scope of this document by participants in the eHAction Steering Council in March 2020, as well as support by eHealth Network representatives and the Commission for the draft in November 2019, and then approval of the draft document in June 2020; the final approach should be approved in June 2021 by the eHN and should be in place when EU bodies are aligned to drive this common approach at cross-border level.

6.1.2. Implementation phase

The necessary collaboration mechanisms would be set up in the first six months. Upon the start of the implementation period, the following high-level roadmap would support the approach proposed in this document, maintaining an open mindset regarding the exact technologies that support eID at any given moment, but ensuring common principles and common governance of the different steps in the different national contexts.

Before to start the implementation of the eID approach, is needed an agreement between the Member States, and European working groups (such as eHN subgroups and others) about the minimal authentication level. This level of authentication can be different for patients (at least 1-factor of authentication) and healthcare professionals (at least 2-factor of authentication).

[37] https://digital-strategy.ec.europa.eu/en/policies/trust-services-and-eid

6.2. Roadmap for the first three years

Below, in Figure 4, a roadmap is presented for the first three years. It has options to cover additional items that can be raised for discussion if the need arises.

In **Year 1** the approach is focused on Goal 1: 'Structure a common approach on health eID in the EU'. The work on this goal during the first year of the approach will ensure the achievement, by Member States, of a minimum structure needed to establish a common approach: approval of the action plan of the eID Health approach, technical analysis of previous and ongoing projects related with eID, and identification eID initiatives that could be related with eID.

In **Years 1 to 3** the work initiated on Goal 1 will continue and Goal 2, 'Converge development roadmaps for Service providers with Adoption of eID', will be initiated. At this stage, the Member States will converge efforts to adopt the eID approach for Health and start the implementation of the eID assets and ensure a phased adoption of novel requirements progressively.

In **Year 3** the recommendations for the following three years will have been prepared. An evaluation of the work done on this approach will have been carried out and the elaboration of a new approach for the following years could be initiated. The work done in this year will support decisions about the continuation of the approach and how it can be achieved.

The common eID approach for health is already in alignment with some projects, however this common approach must be open to alignment with new initiatives regarding eID.

- **Common Semantic Strategy (CSS)** – the CSS is being developed by the eHN Subgroup on Semantics. This group is working towards adoption of standards facilitating large-scale exchange of health information in the EU, by facilitating convergence on interoperability standards for all Member States.
- **X-eHealth** – this is a project to implement the EHRxF Commission Recommendation. The information domains referred on the EHRXF Recommendation that have not yet been discussed in other projects are the focus of this project (i.e. laboratory results; medical imaging and reports and hospital discharge reports). This project has a task (T4.1: Electronic Identification implementation) that is directly related with digital identification for eHealth services.

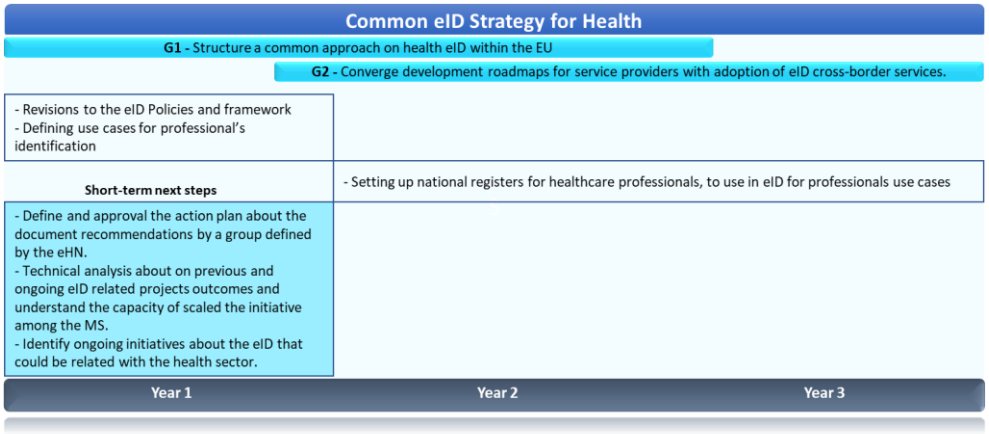

Figure 4 *– Roadmap for the development of eID for eHealth and objectives during the first three years of the Common eID Approach for eHealth.*

7. Annexes

7.1. Annex 1 – List of notified eID schemes under eIDAS

Table 3 – Information about the pre-notified and notified eID schemes under eIDAS:

Member State	Title of the scheme	eID means under the scheme	Level of assurance	Status
Portugal	Chave Móvel Digital	Digital Mobile Key	High	NOTIFIED
Belgium	Belgian eID Scheme FAS / Itsme®	itsme® mobile App	High	NOTIFIED
Portugal	Cartão de Cidadão	Portuguese national identity card (eID card)	High	NOTIFIED
Czech Republic	National identification scheme of the Czech Republic	CZ eID card	High	NOTIFIED
German	German eID based on Extended Access Control	National Identity Card Electronic Residence Permit	High	NOTIFIED
Estonia	Estonian eID scheme: ID card Estonian eID scheme: RP card Estonian eID scheme: Digi-ID Estonian eID scheme: e-Residency Digi-ID Estonian eID scheme: Mobiil-ID Estonian eID scheme: diplomatic identity card	— ID card — RP card — Digi-ID — e-Residency Digi-ID — Mobiil-ID — Diplomatic identity card	High	NOTIFIED
Netherlands	Trust Framework for Electronic Identification (Afsprakenstelsel Elektronische Toegangsdiensten)	Means issued under eHerkenning (for businesses)	Substantial, High	NOTIFIED
Italy	Italian eID based on National ID card (CIE)	Italian eID card (Carta di Identità elettronica)	High	NOTIFIED
Latvia	Latvian eID scheme (eID)	eID karte eParaksts karte eParaksts karte+ eParaksts	Substantial, High	NOTIFIED
Denmark	NemID	Key card (OTP) Mobile app Key token (OTP) NemID hardware Interactive Voice/Response (OTP)	Substantial	NOTIFIED

Member State	Title of the scheme	eID means under the scheme	Level of assurance	Status
		Magna key card (OTP)		
Netherlands	DigiD	DigiD Substantieel DigiD Hoog		PEER REVIEWED
Portugal	Sistema de Certificação de Atributos Profissionais	Professional Attributes Certification System		PRE-NOTIFIED
Lithuania	Lithuanian National Identity card (eID / ATK)	Lithuanian National Identity card (eID / ATK)		PEER REVIEWED
Spain	Documento Nacional de Identidad electrónico (DNIe)	Spanish ID card (DNIe)	High	NOTIFIED
Slovakia	National identity scheme of the Slovak Republic	Slovak Citizen eCard Foreigner eCard	High	NOTIFIED
Croatia	National Identification and Authentication System (NIAS)	Personal Identity Card (eOI)	High	NOTIFIED
Belgium	Belgian eID Scheme FAS / eCards	Belgian Citizen eCard Foreigner eCard	High	NOTIFIED
Luxembourg	Luxembourg national identity card (eID card)	Luxembourg eID card	High	NOTIFIED
Italy	SPID – Public System of Digital Identity	SPID eID means provided by: Aruba PEC SpA Namirial SpA InfoCert SpA In.Te.S.A. SpA Poste Italiane SpA Register.it SpA Sielte SpA Telecom Italia Trust Technologies S.r.l. Lepida SpA	Low, Substantial, High	NOTIFIED
Hungary	Hungarian personal identification cards (eID)	• Permanent personal identification card • Temporary personal	High	NOTIFIED

Member State	Title of the scheme	eID means under the scheme	Level of assurance	Status
		identification card		

Legend:

NOT NOTIFIED: The Member State has not officially communicated its intention to notify its eID scheme to the European Commission.
PRE-NOTIFIED: The Member State has officially communicated its intention to notify its eID scheme to the European Commission.
PEER REVIEWED: The eID scheme has been peer reviewed by representatives of other Member States.
NOTIFIED: The country has notified its eID scheme to the European Commission and the information has been published to the Official Journal of the European Union.

NB: Recognition of the notified eID schemes shall take place no later than 12 months after the publication to the OJEU.

7.2. Annex 2 – Survey Results: List of notified eID schemes

***Table 4** – Information about the pre-notified and notified eID schemes under eIDAS and eID schemes outside of eIDAS (based on survey 1)*

Member State	Title of the scheme	eID means	Level of assurance	Hardware or Software based	Status
Czech Republic	National identification scheme of the Czech Republic	CZ eID card	High and Medium	Hardware and Software	NOTIFIED
	Datové chránky	Datové chránky			
	National Health Insurance number	National Health Insurance number			
	National Healthcare Client ID	National Healthcare Client ID			
	National Healthcare professional ID	National Healthcare professional ID			
Germany	German eID schemes	German eID based on Extended Access Control (not for patient identification)	High	Hardware and Software	NOTIFIED
		Certificate based Identity Provider of National Telematics Health Infrastructure (Smart Card)	Medium	Software	NOT NOTIFIED
		Federated eID scheme by the state health insurances	Medium (for mobile use cases); Low (for web scenarios)	Software	NOT NOTIFIED
Greece	Taxis		Low	Software	NOT NOTIFIED

	HERMIS		Low	Software	NOT NOTIFIED
	THEX				NOT NOTIFIED
Latvia	Latvian eID scheme (eID)	eID karte	High	Hardware	NOTIFIED
		eParaksts karte	High	Hardware	NOTIFIED
		eParaksts karte+	High	Hardware	NOTIFIED
		eParaksts	High	Software	NOTIFIED
Spain	Documento Nacional de Identidad electrónico (DNIe)	Spanish ID card (DNIe)	High	Hardware	NOTIFIED
	Cl@ve	Spanish citizens & legal immigrants	High, Medium, Low	Hardware and Software	
Ireland	MyGovID (DEASP)			Software	
	MyAccount (Revenue)			Software	
	Revenue Online Service (Revenue)			Software	
	IHI (Individual Health Identifier)			Software	
Estonia	Estonian eID scheme	ID card	High	Hardware	NOTIFIED
		RP card	High	Hardware	NOTIFIED
		Digi-ID	High	Hardware	NOTIFIED
		e-Residency Digi-ID	High	Hardware	NOTIFIED
		Mobiil-ID	High	Hardware	NOTIFIED
		diplomatic identity card	High	Hardware	NOTIFIED
Slovenia		Qualified digital certificates on doctor's cards		Hardware and Software	
		Digital personal ID card		Hardware	
		Mobile/cloud eID		Software/Cloud	
Hungary	National Identity Card	e-ID cards contain: Fingerprint	High	Hardware and Software	NOTIFIED

		The data required for creating an electronic signature and signature certificate Social security identification number Tax identification number Unique electronic identifier Up to two telephone numbers to be called in the case of emergency			
	Electronic Residence Permit (non-resident eID card)	Residence permit	High	Hardware	NOTIFIED
	Health Insurance Cards	Social security identification number	High	Hardware	NOT NOTIFIED
Romania	National Health Card				
	European Health Card				
	Electronic Health Record				
	Electronic Prescription				

Legend:

NOT NOTIFIED: The Member State has not officially communicated its intention to notify its eID scheme to the European Commission.

PRE-NOTIFIED: The Member State has officially communicated its intention to notify its eID scheme to the European Commission.

PEER REVIEWED: The eID scheme has been peer reviewed by representatives of other Member States.

NOTIFIED: The country has notified its eID scheme to the European Commission and the information has been published to the Official Journal of the European Union.

NB: Recognition of the notified eID schemes shall take place no later than 12 months after the publication to the OJEU.

7.3. Annex 3 – Survey Questions

1. Considering the health context, please fill in the table considering your national digital identification schemes.

1.1. Considering all actors, fill in the following table:

eID schemes that your country uses. (please refer any eID schemes)	Are they eIDAS compliant ?	Are they notified under eIDAS? If yes, when were they notified?	When are they planned to be notified?	Are they deployed at a national level?	Which actors can be identified by which schemes?	Which schemes are hardware base, and which are software base?	Which level of assurance does the scheme provide? (high, medium, low)

Please, use one line per eID Scheme.

1.2. Considering the patient and the schemes identified in the previous table, fill in the following table:

What eID schemes does your country use? (please refer any eID schemes specific to patient identification)

What eID schemes does your country use? (please refer any eID schemes specific to patient identification)	Are they used exclusively for patient identification?	Are they used or planned to be used for patients to access their data?	Do they relate to patient consent? (please specify)

2. The categories of health professional, currently in use under ISCO-08 in the HDSI services are as follows:

1. Medical Doctor
2. Nursing professionals
3. Midwifery professionals
4. Pharmacists
5. Pharmaceutical technicians and assistants
6. Dentists
7. Physiotherapist
8. Dieticians and nutritionists
9. Audiologists and speech therapists' nutritionists
10. Optometrists and ophthalmic opticians
11. Medical imaging and therapeutic equipment technicians
12. Health professionals not elsewhere classified (e.g. Others)

a. Considering these categories and 'others', please fill in the following table:

Does your country use this reference set at a national level, or does it use another value set?	**Does your country use other international reference sets? Please specify.**	**Is there a professional association for managing and maintaining professional categories? Please specify.**	**Does your country possess national identity providers? Please specify which.**	**Is there a national agency for managing and maintaining these identity providers? Please specify.**

Considering the European Health Dataspace concept, please provide answers to the following questions:

b) Does your country consider the European Health Dataspace for other categories of users of eHealth data? E.g. social care and research. (please specify)

c) Does your country include and categorise other actors referring to secondary use of data? (please specify)

3. Regarding the adoption of eIDAS in the health context, please provide answers to the following questions:

a) Do you find that there is added benefits for your country and, specifically for the eHealth context, in the usage of the available eIDAS infrastructure?

b) What do you find to be the drawbacks of the adoption of eIDAS to support eHealth services? (please specify in regard to challenges and potential losses, including costs of opportunity)

c) Does your country have in place a Mobile Strategy for eHealth services? If so, does it regard the use of mobile to address patient identification?

7.4. Annex 4 – eID and EESSI

More than looking at eID solutions for EESSI, there is an ongoing initiative called 'European Social Security Number', which is basically about digitising what we call 'portable documents', such as the European Health Insurance Card (EHIC), and the verification of social security coverage.

There are two steps in the process, just like in eHealth:

1. the identification and authentication of the citizen;
2. the actual use case, which could be, for example, the verification of health insurance coverage, for unplanned care, in a hospital, as a substitute to EHIC.

The EHIC could indeed be out of date while still having an expiry date which is still valid, so the verification it provides is not fraud-proof: people could present a EHIC which is still valid on paper while at the same time the citizen is not covered anymore, because he moved to another country, or dropped from social security coverage for any other reason.

One of the ideas regarding identification of citizens was to create a new European Social Security Number as a unique means of identification, or at least a unique identifier to which all Social Security identifiers could be mapped, but we now think that we could also potentially simply use the eIDAS framework, the eID building

block, and the eIDAS nodes which have been put in operations recently, and for which a group of countries have sent notification to the Commission.