eHealth Network

RECOMMENDATION PAPER

on

Policies Regarding eIDAS eID and Health Professional Registries

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

Adopted by consensus by the eHealth Network, Brussels, 15 May 2018

-Keep this page free-

LIST OF ABBREVIATIONS

ACRONYM	DEFINITION
Agreement	AGREEMENT BETWEEN NATIONAL AUTHORITIES OR NATIONAL ORGANISATIONS RESPONSIBLE FOR NATIONAL CONTACT POINTS FOR EHEALTH ON THE CRITERIA REQUIRED FOR THE PARTICIPATION IN CROSS BORDER EHEALTH INFORMATION SERVICES FOR EASIER IDENTIFICATION IN THE TEXT WRITTEN IN ITALICS: "*Agreement*"
CBeHIS	CROSS BORDER EHEALTH INFORMATION SERVICES
CEF	CONNECTING EUROPE FACILITY
DSI	DIGITAL SERVICE INFRASTRUCTURE
EC	EUROPEAN COMMISSION
eHDSI	EHEALTH DIGITAL SERVICES INFRASTRUCTURE
eIDAS	ELECTRONIC IDENTIFICATION AND TRUST SERVICES
eIDAS Regulation	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON ELECTRONIC IDENTIFICATION AND TRUST SERVICES FOR ELECTRONIC TRANSACTIONS IN THE INTERNAL MARKET AND REPEALING DIRECTIVE 1999/93/EC
eHN	EHEALTH NETWORK
EIF	EUROPEAN INTEROPERABILITY FRAMEWORK
eD	ELECTRONIC DISPENSATION
eP	ELECTRONIC PRESCRIPTION
EU	EUROPEAN UNION
ERN	EUROPEAN REFERENCE NETWORK
GDRP	GENERAL DATA PROTECTION REGULATION
HCP	HEALTHCARE PROVIDER
HP	HEALTH PROFESSIONAL
IOP	INTEROPERABILITY
JAseHN	JOINT ACTION FOR SUPPORT THE EHN
LOST	LEGAL, ORGANISATIONAL, SEMANTIC, TECHNICAL
MLA	SEE "AGREEMENT"
MS	MEMBER STATES (OF EU)
NCP	NATIONAL CONTACT POINT FOR CROSS BORDER
NCPeH	NATIONAL CONTACT POINT FOR EHEALTH
NI	NATIONAL INFRASTRUCTURE
OFW	ORGANISATIONAL FRAMEWORK
OFW-NCPeH	ORGANISATIONAL FRAMEWORK FOR EHEALTH NATIONAL CONTACT POINTS
PoC	POINT OF CARE
PS	PATIENT SUMMARY
ReEIF	REFINED EHEALTH EUROPEAN INTEROPERABILITY FRAMEWORK
QSCD	QUALIFIED SIGNATURE CREATION DEVICE

TABLE OF CONTENTS

1. Executive summary

When talking about identification of the roles patient and health professional within eHDSI and CBeHIS the following different use cases for identification of these roles apply:

- (1) Identification of patients using **non-electronic means**;
- (2) Identification of patients and health professionals using **electronic means notified under eIDAS scheme**;
- (3) Identification of patients and health professionals using **electronic means not notified under eIDAS scheme**.

The paper at hand describes the current state of discussion of only one (#2) the abovementioned use cases for identification, namely: **the identification of patients and health professionals based on electronic means notified under eIDAS scheme.**

It refers to both the identification of patients as well as health professionals even though the known legal interpretations of the eIDAS Regulation concerning the existence or non-existence of an legal obligation to implement electronic identification for patients varies significantly within Member States (for more details see section 3). The same applies for the health professional, who identifies the patient at the Point of Care (PoC) and accesses the eHDSI services (currently patient summary and ePrescription).

The paper at hand lays down identified problems, open questions and received comments and tries to outline a way forward by proposing detailed actions to be under taking by different initiatives. The informative annex of this document provides an overview of definitions used and their relation to CBeHIS.

The eHealth network is asked to discuss and adopt the recommendations laid down in this paper in order to give guidance for the takeover of work ahead after the end of the JAseHN project in June 2018.

2. Introduction

Cross-border sharing of health data imposes the specific challenge that the involved human and organizational actors are usually only recognized within one of the participating countries while being active participants in flows in other countries. This imposes the need for cross-border identity verification processes based on previously established and regulatory backed cross-border trust relationships. This affects both the identification and authentication of health professionals and patients for the uptake of eHDSI and CBeHIS.

The Agreement between national authorities or national organisations responsible for national contact points for eHealth on the criteria required for the participation in cross border eHealth Information Services (*Agreement*)[1] foresees to use notified eID means (#2), non-notified eID means (#3), and non-eID means (#1). All three alternatives

[1] See clauses II.1.1.2 and II.1.1.3 of the *Agreement*

can provide secure mechanism and requirements and it is up to each Member State participating in CBeHIS to decide which of these they will implement and use for their CBeHIS participation.

The paper at hand describes the current state of discussion of only one (#2) the abovementioned use cases for identification, namely: **the identification of patients and health professionals based on electronic means notified under eIDAS scheme.**

For eHealth, the different components of the eIDAS Regulation can provide a holistic framework and a toolbox for establishing trust in CBeHIS. Once fully implemented, the eIDAS Regulation can create enabling conditions for secure transfer of health data across borders in the EU.

3. Background information, state of discussions and received comments

The JAseHN task T5.2 eID of eHealth started its work in May 2015 and organised several workshops partly in a joint manner with the European project e-SENS[2], which was also working on electronic identification of patients and health professionals taking into consideration the eIDAS Regulation. The outcomes of the task work were incorporated into several draft documents for discussion on the policy level.

In May 2017 the eHealth Network adopted the eID specific Framework for eHealth (Release 1)[3], which includes a first approach to describe and align the consequences of the eIDAS Regulation on the uptake of CBeHIS and its eHDSI waves. The eID specific Framework for eHealth (Release 1) explicitly focuses on the identification of patients and health professionals based on electronic means notified under eIDAS scheme and can be seen as an earlier version of the document at hand.

One of the important outcomes of the eID specific Framework for eHealth (Release 1) was, that the first wave of eHDSI, which is planned go live in June 2018, will due to several reasons not be implementable based on electronic means notified under eIDAS scheme. The aforementioned reasons include inter alia the complexity of the topic at such, significant time constraints for implementation and the later entry into force date of the mutual recognition of electronic identification means of the eIDAS Regulation.

Concerning the second wave of eHDSI (February 2019) the current status is that it is not possible to implement technical prerequisites for notified electronic identification means according to eIDAS Regulation within the set time frame and without neglecting other ongoing activities and work. Additionally the political alignment concerning a common Authentication Assurance Level is not reached by now, which is an important aspect for the technical implementation.

This will focus all activities and efforts concerning the identification based on electronic means notified under eIDAS scheme on the third wave of eHDSI (February 2020) and the ones after CEF funding, which may follow.

[2] See https://www.esens.eu/
[3] See https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20170509_co04_en.pdf

An eID framework for eHealth (Release 2), which was prepared by the JAseHN Task T5.2 eID for eHealth, could not be adopted but only discussed at the May 2017 eHealth Network meeting. Due to the fact that the opinion of the Art. 29 working party on the *Agreement* will be ready soonest in April 2018 and a general legal assessment of eIDAS and GDPR are not tasked anywhere at the moment, important counter stones for reaching a common legal interpretation among Member States could not be set sufficiently.

The ongoing work and progress on the second topic of the JAseHN task T5.2 eID for eHealth, the Health Professional Registries, did suffer consequently, as both topics are strongly interlinked with each other and both lacking an general legal assessment. Concerning Health Professional Registries it is expected that a general legal assessment might give more insight and recommendations on what identity information of health professionals needs to be exchanged and processed for a legally reliable patient consent and its enforcement. This would be key information related to Health Professional Registries.

Due to the soon end of the JAseHN project the task T5.2 eID for eHealth requested the Member States and the level of national Competence Centers for eHealth and on the political level of the eHealth Network to investigate each their specific national situation concerning a possible compliance of their national systems to the proposed eIDAS Authentication Assurance Level “high” and estimate consequences related to possible national legal implications, economic investments as well as the technical implications for their national infrastructure. Comments, questions, points and information received on diverse channels in written or verbal form were collected, organized by the responsible JAseHN task and laid down condensed in this document adding a suggested way forward by proposing detailed actions to be under taking by different initiatives.

3.1 Interpretation of eIDAS Regulation and GDPR

As of today, there is no common and assured interpretation of the legal implications of both the GDPR and eIDAS Regulation concerning the sustainable provision of CBeHIS, which is shared by the Member States.

There is no common legal interpretation of eIDAS Regulation concerning the existence or non-existence of a legal obligation to implement electronic identification based on electronic means notified under eIDAS scheme for the role of a patient for the current eHDSI services (patient summary and eprescription). Different interpretations arouse from the fact, that the health professional identifies the patient at the Point of Care and access the online service directly in the non-acting presence of the patient. On the other hand, a patient can be seen as directly involved as the online service of eHDSI deals with his or her own sensitive medical data.

The introduced concept of so called *closed systems* in the eIDAS Regulation[4] is also viewed differently when talking about eHDSI online services. It is not clear by now whether CBeHIS as a combination of several national infrastructures can or cannot be seen as a *closed system* between a defined set of participants, which have no effect on third parties. Even if CBeHIS as a whole can be seen as a *closed system* of Health Professionals there would be an effect on a third party, namely on patients.

National legal interpretation of GDPR, eIDAS Regulation and probably NIS Directive seem to be still pending in Member States at the moment due to many simultaneous legislative reforms. Creating a common legal interpretation of Member States seems to be the subsequent step after forming the national legal interpretation.

3.2 Agreement between national authorities or national organisations responsible for national contact points for eHealth on the criteria required for the participation in cross border eHealth Information Services (Agreement)

The Agreement between national authorities or national organisations responsible for national contact points for eHealth on the criteria required for the participation in cross border eHealth Information Services (*Agreement*)[5] foresees to use notified eID means (#2), non-notified eID means (#3), and non-eID means (#1).

All three alternatives can provide secure mechanism and requirements and it is up to each Member State participating in CBeHIS to decide which of these they will implement and use for their CBeHIS participation.

The *Agreement* undergoes currently a legal assessment by the Art. 29 working party. A final opinion is expected for April 2018 and will be discussed by the Member States. There is no obligation to implement the opinion of the Art. 29 working party; however, changes of the *Agreement* itself or on other relevant and prominent aspects of the eHDSI services may occur and affect also the identification based on electronic means notified under eIDAS scheme.

3.3 Changes of national eID implementations in Member States

Member States were asked previously to investigate their national situation concerning a possible compliance of their national systems to the proposed eIDAS Authentication Assurance Level “high” and estimate consequences related to possible national legal implications, economic investments as well as the technical implications for their national infrastructure.

[4] See eIDAS Regulation EU/910/2014 (21)
[5] See clauses II.1.1.2 and II.1.1.3 of the *Agreement*

Some Member States will have to change their national legislation in order to implement the identification based on electronic means notified under eIDAS scheme. Some Member States already introduced eID means which are not per se compatible with the requirements of eIDAS Regulation e.g. because of missing required data or not fully fulfilling the requirements concerning issuance of the eID means. Some Member States push the topic as data protection and security is one of the national key priorities. Some Member States seem to have no clear position or priority towards identification and authentication of patients and health professionals. Several Member States pointed out that the possible implementation of identification based on electronic means notified under eIDAS scheme would take long-term preparatory work and cannot be done within the timeframe of CEF funding for eHDSI.

Three Member States provided some details about their national situation:

- The use of electronic means of identification of the patient is not mandatory in **Spain** when the patient is not the one accessing his or her data. It is recommended to use card-reader software to identify patients by the health professional, but other alternatives are possible to identify patients at the Point of Care. Spain points out that the eHDSI online services (patient summary and eprescription) will not be provided directly to patients, and therefore, there is no need to identify electronically patients since patients can be identified in situ at the Point of Care by the health professional.
- In **Estonia** the patient has non-electronic and the health professional has electronic identification and authentication. It would be an Estonian requirement to go for AAL “high”, even though Estonia is not ready yet to implement identification based on electronic means notified under eIDAS scheme. The additional attribute to identify the patient would not be needed for Estonia; however, Estonia does not intend to implement identification and authentication based on electronic means notified under eIDAS scheme for patients. Implementing identification and authentication based on electronic means notified under eIDAS scheme for health professionals would be feasible at a later point in time.
- **Finland** does have the legal interpretation that the eHDSI online services (patient summary and eprescription) are not applicable concerning eIDAS Regulation, as these online services are not accessed by the patient itself but directly accessed by the health professional. Notwithstanding the legal interpretation aforementioned, Finland views the timetables presented so far as not realistic, as most of the MS do not even have technical solutions to handle eID in their points of care in the national context.

Additional insight may provide the recently published study on secure cross-border identification from mobile devices[6] performed by GSMA, which includes a pilot in some Member States and lessons learned.

Naturally the situation in Member States might be even much more complex as laid down above and the aforementioned comments are not exhaustive at all.

3.4 Financial implications of the implementation of notified eID means in Member State

It is an undisputed fact, that the implementation of notified eID means for CBeHIS will create probably significant costs for Member States. This will include both one-time and recurring costs depending on the specific national prerequisites and situation. The request for a socio-economic analysis is comprehensible but clarification for each Member State in its dedicated situation for a potential usage of notified eID means in a cross-border context can only be provided appropriately at national level.

3.5 Changes to fundamental paradigm of eIDAS eID in the context of eHealth

After the first national eID scheme – the German new identity card – was notified[7] and with the Italian eID scheme SPID[8] currently being in pre-notification, the actual impact of the eIDAS eID paradigm of enabling a European citizen to identify and authenticate from his/her country of affiliation against a digital service offered in or by another country could be established.

The eHealth domain operates under a distinctively different paradigm in which the bearer of the eID scheme, the citizen in its role as a patient, is physically present in the foreign country and is authenticating against a digital service that is native to this particular country. Consequently, additional means, services, and mitigation strategies need to be identified to assure low-level interoperability of eID Schemes (such as card readers) or to encourage Member States to enable purely virtual identification and authentication such as mobile eID to compensate for specific interoperability issues with physical token based eID.

[6] See https://ec.europa.eu/digital-single-market/en/news/new-study-secure-cross-border-identification-mobile-devices;
https://www.gsma.com/identity/wp-content/uploads/2018/02/MC-for-cross-border-digital-services_eIDAS_Feb2018-FINAL-web.pdf

[7] See
https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+notified+eID+schemes+under+eIDAS

[8] See https://ec.europa.eu/digital-single-market/en/news/first-private-sector-eid-scheme-pre-notified-italy-under-eidas

3.6 Authentication Assurance Level “High”

The eIDAS Regulation distinguishes between three Authentication Assurance Level (“low”, “substantial” and “high”), which gives guidance to the degree of confidence in an authentication process. The three AALs are built on one another by adding more requirements to be met by the particular electronic mean. For the AALs “substantial” and “high” these electronic means have to be notified by the Member State following the procedure of the eIDAS Regulation.

The AAL “substantial” might be the standard choice when providing services with personal data, e.g. name, address, and bank account details of a dedicated person for internet shopping. The AAL “high” might be reserved for services with high-level data sensitivity. Taking into account the definition of health data in the GDPR one may come to the conclusion, that sensitive medical data of a patient shared across borders might need the highest degree of confidence in an authentication process which would be available.

However, the political alignment concerning a common Authentication Assurance Level (“substantial” or “high”) is not reached as of today. A possible implementation of AAL “high” is seen as very demanding for Member States, so that it is recommend resuming related activities under this thesis until the to be performed legal review of eIDAS Regulation and GDPR (see section 4 recommendations) is finished. The AAL may be revisited following completion of the legal review.

4. Recommendations

The eHealth Network Members are asked to discuss and adopt the following recommendations laid down in this paper in order to give guidance for the takeover of work ahead after the end of the JAseHN project in June 2018:

1. The eHealth Network shall agree that a legal review of eIDAS Regulation and GDPR in relation to a sustainable uptake of CBeHIS will be carried out under the responsibility of the eHealth Member States Expert Group (eHMSEG) especially but not limited to the following key points:

a. Applicability of eIDAS Regulation concerning electronic identification and authentication of patients and health professionals for the CBeHIS online services (patient summary and eprescription)
b. Applicability of eIDAS Regulation concerning the usage of trust services in order to create legal certainty for the CBeHIS online services (patient summary and eprescription)
c. The aforementioned key points a) and b) will be accomplished by a cross-check with
    i. the GDPR concerning patient consent, required identity information of health professionals for the exchange and procession of patient consent and its enforcement as well as requirements concerning cross-border sharing a sensitive medical data and
    ii. an interoperability assessment concerning the use case *Identification of patient and health professionals using electronic means NOT notified under eIDAS scheme*.
d. The work will be done by taking into account the *Agreement* and report of the art. 29 working party.

2. "The eHealth Network shall agree that the outcomes of the legal review of eIDAS Regulation and GDPR after discussion and validation on the policy level (see recommendation#1) will be integrated into the CBeHIS roadmap for future services and features, which will be elaborated within the JAseHN consecutive Joint Action, the eHealthAction, under the responsible Task T6.1 Support of the eHDSI uptake.

3. The eHealth Network shall agree that the whole outcome of JAseHN T5.2 *eID for eHealth* will be made available for the European Research and Development project called *HEALTHeID,* which is going to implement a reference implementation of an eHealth eIDAS Connector Country-B.

5. Annex with related definitions and their mapping on CBeHIS[9]

The standard ISO/IEC 24760-1 specifies core concepts of identity and identity management and their relationships. It will be used as a baseline for defining the most prominent actors in a cross-border healthcare scenario and for mapping these onto roles related to identification and authentication.

Entities and Identities

Any item that has recognizably distinct existence is called an ENTITY. Examples for entities in CEF eHealth are health professionals, patients, data managing services, medical documents, etc. Each entity can be characterized by ATTRIBUTES that describe the state, appearance, etc. of that entity. Sets of attributes make up the IDENTITY of an entity. The attribute values of an identity for an entity are IDENTITY INFORMATION of that entity.

It shall be noted that there is a n:m relationship between entities and identities. E.g. the same entity may be linked with the identity information “female, blonde, 35 years old” and “nurse midwife working at Berlin City Hospital”. As well the identity information “female, blonde, 35 years old” may be linked with multiple entities.

Identification

Identity information that unambiguously distinguishes one entity from another is called an IDENTIFIER. Identifiers are always only defined within the scope of a DOMAIN OF APPLICABILITY, where the entity’s attributes can e.g. be used for distinguishing the entity from other entities. The process of recognizing an entity in a particular domain of applicability as distinct from other entities is called IDENTIFICATION.

Example: A doctor can be identified within the healthcare domain of applicability through the doctor ID assigned to him by the national doctors’ association. This ID will not be usable for identification in the eGovernment domain of applicability, e.g. when filling in a tax form. On the other hand, a health insurance will not be able to identify a doctor by his tax ID. Even worse, the health insurance will even not be able to discover if the tax ID is an identifier at all (it is not; e.g. me and my wife have both the same tax ID).

This last aspect – not knowing if provided identity information is an identifier within another domain of applicability – is particularly important for CEF eHealth: A doctor in country B can never be able to identify a patient from country A unless country A provides him with the knowledge about which identity information about a patient from country A is required to univocally distinguish this patient from other patients from the same country A.

By this,

- a patient from country-A can only be identified within the “country-A” domain of applicability as this is the only context where provided identity information of

[9] This is a helpful illustrating section from the document *Technical Delta Analysis*, which was written by the JAseHN task T5.2 eID for eHealth.

the patient can be used for univocally distinguishing the patient from other patients.

- a care provider or care provider organization can only be identified within the "country-B" domain of applicability as this is the only context where provided identity information of the provider (organization) can be used for univocally distinguishing the provider (organization) from another provider (organizations).

This definition is notable because in the CEF eHealth scenario a patient's identity information is processed in the "country-B" domain of applicability while the identification of the patient can only occur in the "country-A" domain of applicability. As well identity information of a provider needs to be processed in the "country-A" domain of applicability while the identification of this provider can only be performed in the "country-B" domain of applicability.

Identity Assurance

Processing identity information of an identity that was identified in another domain of applicability raises the question of IDENTITY ASSURANCE (defined as "the level of confidence in provenance, integrity and applicability of identity information including confidence in identity information maintenance" in ISO/IEC 24760-1).

Identity assurance is a critical issue within the eHealth domain due to the presetting that each domain shall consider every other domain as a "black box". Unless there is a reliable assurance (for instance through harmonizing regulatory frameworks such as the eIDAS regulation or to a lesser degree through bilateral contracts) about how Identity Information Providers and Identity Information Authorities are operated in the other domain, the stability and applicability of the provided identity information cannot be assured sufficiently:

- An IDENTITY INFORMATION PROVIDER makes available identity information. It creates and maintains identity information for entities known in a particular domain. Weaknesses in this respect (e.g. insufficient attribute value lifecycle management) may lead to altered, outdated and/or incomplete identity information.
- IDENTITY INFORMATION AUTHORITIES are the on entities within a domain of applicability that can make provable statements on the validity and/or correctness of one or more attribute values in an identity defined within that domain.
- One major problem with this is that an NCPeH usually only may take the role of an Identity Information Provider while Identity Information Authorities are operated within a national infrastructure with often rather restrictive and country-specific interfaces to external services. This affects all entities in a domain of applicability that rely on the verification of identity information for a particular entity that is managed within another domain. Both the provider in country-A and the patient data managing services in country-A are such RELYING PARTIES:

- Data managing services in the “country-A” domain of applicability release protected health information based primarily on the patient’s consent and subsequent national security and/or application policies. An audit trail is written for non-repudiation that documents which operations have been performed and what information had been released to whom for what reason. For policy decision and audit trail writing the data managing services relies on the validity and correctness of identity information about a care provider that was identified in the “country-B” domain.
- Health Professionals in the “country-B” domain of applicability must be sure to only process data of the patient who authorized them for doing so. For this they rely on proper patient identification in the “country-A” domain.
- In some instances, such as the electronic prescription, the legitimacy of the issuance of the eP as well as the qualification and sufficient authorization of the prescribing health professional needs to be transported into country-B to enable the latter to act on this behalf.
- Based on the original epSOS solution the CEF eHealth project shall assess alternative solutions for patient and provider identification which provide a higher level of identity assurance than the original epSOS solution.

Interoperability

For identities to be processed across domains, the attributes that make up the identity shall be technically and semantically interoperable. For this each attribute shall implicitly or explicitly be linked with a defined DOMAIN OF ORIGIN which specifies the meaning and format of the attribute value.

In CEF eHealth the domain of origin for each attribute is defined as part of the epSOS specification on provider and patient identities. For all epSOS defined identity attributes, the domain of origin is either an international standardization organization or a European regulative body.

Authentication

AUTHENTICATION is defined as a formalized process to determine that presented identity information associated with a particular entity is applicable for the entity to be recognized in a particular domain at some point in time. By this authentication provides a proof that an entity is linked with a claimed identity. The result of a successful authentication process is an AUTHENTICATED IDENTITY. Identity information that is suitable to prove the univocal linkage of an identity to an entity is called a credential. Credentials are something that the identity subject knows, possesses or has access to, such as a username/password, a smartcard, and biometric measures. During the authentication process, the subject is presented with a challenge, in which a combination of credentials needs to be presented in order to conclude the process and yield an authenticated identity. This challenge can be an internal mechanism, such as a PIN to unlock a smartcard or an suitably robust piece of external information, such as an already succeeded Single Sign-On from another Identity Provider.

Authentication typically involves the use of a policy to specify a required level of assurance for an authenticated identity. The level of assurance of an authenticated identity usually depends on the kind of credential used for authentication, the number of independent factors involved in the verification of the credential and the policies defined for protecting all of these entities and processes.

The process of identification is often implemented as an authentication in order to obtain and assert a specific level of assurance in the resulting linkage between a person and an electronic identity. However, it is important to distinguish between the two in the eHealth domain, as identification is the primary safeguard of the patient safety dimension (this clinical data does belong to that person), while authentication is a tool supporting the enforcement of information security, privacy, and data protection concerns.

The epSOS technical specification defines means to transport identity information within containers, the so-called identity assertions, where an identity assertion is a certified statement by an identity information authority used by a relying party for authentication with a specified level of assurance. In scenarios where the identity information authority and the relying party are located in different domains, an identity assertion may hold the cryptographic proof of a successful authentication, created with algorithms and keys agreed between parties. Consequently, the relying party may verify and validate the claimed identity by examining the cryptographic proof and by this accepting the authentication performed in another domain or by a third party. Accepting identified and authenticated identities from other domains based on an established trust relationship between the affected domains is called IDENTITY FEDERATION across these domains.

epSOS identity federation suffers from a rather low level of assurance of the federated identities. There is no authentication performed on patient identities in a formalized manner which leaves it to the relying parties to assess if the provided identity information is really linked with a certain patient. Provider identities are provided to foreign domains through the NCPeH of country-B which is not an Identity Information Authority. Even worse, the relying party in country-A has to accept identities from country-B which it cannot verify on its own because identity federation is only implemented between NCPeHs.

If identity federation is to be used for CEF eHealth it shall be end-to-end in a manner that either a relying party can validate identity information directly or that identity information is shared cross-border only between federated identity information authorities.

Identity Management

From the previous sections is becomes obvious that the epSOS notion for considering identity attribute sources and management within the national infrastructures as black boxes is not sufficient. Especially the epSOS solution of considering NCPs as Identity

Information Authorities does not reflect the respective responsibilities and regulations within country-B and therefore is a source for weakening the level of identity assurance.

In particular each country-B needs to operate a dedicated IDENTITY MANAGEMENT for provider identity attributes. This includes the definition and proper implementation of processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in provider identities within the country-B domain. Country-A also has to define and implement an identity management for patients who gave consent to the cross-border sharing of their health data.

Part of the management of identities is the definition of REFERENCE IDENTIFIERS which are intended to remain the same for the duration an entity is known in the domain and is not associated with another entity for a period specified in a policy after the entity ceases to be known in that domain. Such identifiers are indispensable for efficiently referencing to entities which shall be identifiable across the participating countries. Once such an entity has been identified, a reference identifier allows for referencing to that entity without having to identify it again in advance to any interaction where this entity is involved.