HEALTHeID

eIDAS – OpenNCP
Connector for eHealth

D1.2 Usability Requirements

Document Information:

Document status:	Final
Document Version:	1.0
Author(s):	Alberto Zanini (LISPA)
Member State Contributor(s):	SPMS (Portugal), AUTH (Greece), LISPA (Italy), POLITO (Italy), Gematik (Germany)
Stakeholder Contributor(s):	

Table of Content

Table of revisions		
Date	Comments	Authors
28/09/2018	First draft	Alberto Zanini (LISPA)
30/09/2018	Comments from AUTH	AUTH
01/10/2018	Further comments from LISPA	Alberto Zanini (LISPA)
03/10/2018	Comments from SPMS and AUTH, included	Pedro M. Miranda (SPSM), Andrew Short (AUTH)
16/10/2018	Alternative solutions described	Alberto Zanini (LISPA)
19/10/2018	Addressed comments from SPMS, AUTH, POLITO, Gematik	Alberto Zanini (LISPA), Pedro M. Miranda (SPSM), Zoi Kolitsi (AUTH), Andrea Atzeni (POLITO), Maid Erovic (Gematik)
23/10/2018	Evaluation criteria applied to all scenarios; former "Solution A" now expanded in several scenarios	Alberto Zanini (LISPA)
24/10/2018	Revision versus CEF eHDSI processes	Marcello Melgara (LISPA)

30/10/2018	Addressed comments from SPMS	Pedro M. Miranda (SPMS), Jürgen Wehnert (SPMS), Alberto Zanini (LISPA)
15/11/2018	Addressed comments from AUTH; general review of the document	Zoi Kolitsi (AUTH), Alberto Zanini (LISPA)
29/11/2018	Further comments from Petra Wilson, SPMS, PoliTo, LISPA addressed	Petra Wilson, Alberto Zanini (LISPA), Jürgen Wehnert (SPMS), João Cunha Gonçalves (SPMS), Marcello Melgara (LISPA), Andrea Atzeni (PoliTo)

Bibliography		
Id	Document title	Authors
[1]	Deliverable 1.1 "HEALTHeID Vision"	Zoi Kolitsi – AUTH (Greece); João Cunha Gonçalves, Pedro Miranda, Jürgen Wehnert - SPMS (Portugal); Andrea Atzeni – POLITO (Italy)

1. Objectives

This document, part of the Activity 1, has the following goal: analyse the suitability of current user interfaces of eIDAS notified eID schemes for patient identification; design tools for enhancing patient experience relating to identification, leaving its implementation to Activity 2; provide recommendations to Member States regarding the usability of their eIDAS eID schemes in order to allow patients to execute their identification process from abroad. The document considers different interfaces and alternative solutions, including the mobile eHealth ID scenario.

2. Current scenario

The current eHDSI specifications define a set of functional requirements for both the Patient Summary (PS)[1] and ePrescription/eDispensation (eP/eD)[2] use cases, where a patient from Country A (country of affiliation) seeks healthcare in Country B (country of treatment). Among such requirements one can find the Functional Requirement 03 – Patient identification:

> "The patient needs to be univocally identified in a reliable way (unique and unequivocal ID) to allow the HP to consult his information (after his explicit consent or authorization). For functional and security purposes in information usage, the univocal identification of the patient is highly relevant. One-to-one and unmistakable identification of the patient must be assured. Patient authentication will be guaranteed at the national level based on the concept of mutual trust. (…)
>
> The process of identification (positive or negative) must be recorded."

In practice, in the Point of Care Portal, specific masks are defined for each Country of Affiliation.

The Health Professional asks the patient for the credentials to be used for his identification, types them in the appropriate mask. Data are sent to the NCPeH-B, which issues a "Cross Community Patient Discovery" (IHE XCPD) to NCPeH-A.

Country of affiliation replies with the patient information, which are displayed to the Health Professional., who should check the Patient identity, get the Patient confirmation of the willingness to be treated by that Health Professional. The confirmation is registered through the check-box in the Point of Care Portal.

The subsequent Treatment Relationship Confirmation is sent from the Country of Treatment to the Country of Affiliation: at this point, PS or eP can be exchanged.

The current procedure has negative usability impacts on the Health Professional who is requested to type long identifiers, with the risk of injecting errors.

[1] PS Functional requirements: https://ec.europa.eu/cefdigital/wiki/x/4w9AAg

[2] eP Functional requirements: https://ec.europa.eu/cefdigital/wiki/x/5w9AAg

The authentication of the patient, when the Country of Affiliation returns the Patient's information, by comparing them with the Patient's ID document, is left to the Health Professional: the control actually performed is weak, and errors could occur.

The verification of the fact the patient was adequately informed about the treatment of his data (i.e. presentation of the Patient Information Notice and its acceptance by the patient) is not assured by a traced procedure.

3. Re-framing patient identification in the light of eIDAS

eIDAS introduces a new landscape for patient identification for cross-border eHealth.

Firstly, eIDAS assumes an electronic identification workflow, where the citizen requests a service from a Service Provider (SP), then the citizen is authenticated (through his national eIDAS infrastructure) towards the SP before the SP may provide access to its electronic services that the citizen is entitled to. Trust is established through the eIDAS Node in Country-A, in an interoperable transport form, the eIDAS SAML Assertion. This assertion is adhering to international technical standards and provides intrinsic and extrinsic security safeguards. The SP as a relying party may technically and legally trust the assertions contents as a form of citizen authentication.

Secondly, it is important to reconsider the concepts described in the previous sections in the light of this re-framing. As a first step, the HEALTHeID Connector implementation process must adopt definitions and concepts as described in the eIDAS Regulation and translate them appropriately to the cross-border eHealth context. This identification process will then lead to identification and authentication of an individual, without however necessarily providing for locating the individual, as a patient registered with his/her national health care system and national eHealth infrastructure.

It is therefore important to recognize that, in addition to the eIDAS workflow, the HEALTHeID Connector must provide for completing the patient identification through capturing or mapping the identification data to the patient identifier.

3.1 Usability requirements: users' perspective

While defining the new functionalities, basic users' requirements should be taken into consideration, for example:

Health Professional (HP) Requirements:

a) Efficiency:
   i. Single Sign-On: avoid to perform a login for each new patient ;
   ii. Avoid (re-) typing long Patient identifiers ;
   iii. Avoid too may nested pages ;
   iv. Complete the Patient Authentication should be performed in about 30 seconds, maximum 1 minute, having the Patient in front of the HP ;

v. In general, most properly when Patient Authentication is time-consuming, the possibility to complete all the administrative procedures before the encounter starts ;

b) Effectiveness:

i. Avoid being obliged to use different terminals, or copying and pasting from one window to another one ;

ii. Avoid handing the keyboard over to the Patient ;

iii. Provide an easy way of finding/displaying/printing information for the Patient (e.g. Patient Information Notice,….) ;

c) Trust:

i. Trust the patient authentication, avoiding the need to doublecheck ;

Patient Requirements:

a) Efficiency:

i. Avoid the need of re-authenticating several times during one encounter ;

ii. Avoid (re-) typing long Patient identifiers ;

iii. Complete the Patient Authentication in about 30 seconds, maximum 1 minute, having the possibility to perform authentication before being in front of the HP ;

b) Effectiveness:

i. Possibility to use his own device ;

ii. If a common device/kiosk is used, assure the needed privacy while typing sensitive data ;

iii. Allow a simple, user-oriented user interface. Accessible to all, including elderly people ;

iv. Consider the possibility to use at least the English language, and not only the SP language, or - in an enhanced scenario - even the Patient language

d) Trust:

i. Trust the patient authentication released by the Identity Providerdome, avoiding the need to doublecheck.

4. Proposals to enhance patient identification

6.1 Assumptions

- Health Professional (HP) in Country B is required to use a domestic Identity Provider (typically not joining the eIDAS network) to login into a Service Provider (SP) ;

- Patient and Health Professional (HP) are co-located, i.e. in the doctor's office, in a Pharmacy, or at any other point of care, in Country-B ;

- The SP used by the HP and by the Patient must be identical ;

- The use cases addressed in HEALTHeID assume the operation of one single SP (the national NCPeH), however, authe usability analysis should be applicable for future scenarios which may require multiple, trusted SPs. Those scenarios could be evaluated e.g. in the Handing Over, after the Transferathon.

6.2 Evaluation criteria

Each of the solutions described below, are evaluated against their capacity to serve the HEALTHeID vision.

These have been defined in D1.1. and are briefly described here:

- ✓ **Criterion 1: Compliance with eIDAS Regulation**. The proposed approach should fully respect the eIDAS requirements and exploit maximally its enabling properties, i.e., it should exhaust the possibilities for a viable and sustainable solution within the provisions of the eIDAS Regulation without the need for additional agreements (nFR 01, nFR02, nFR05) ;
- ✓ **Criterion 2: Privacy by design** The proposed approach should respect the relevant GDPR requirements and exploit maximally its enabling legal basis for access to health data and its safeguards as to the protection of the individual's rights (nFR 06, nFR07, nFR08) ;
- ✓ **Criterion 3: Security** The proposed solution should protect against security breaches (e.g when using shared devices) and preserve the Level of Assurance (LoA) of the patient authentication throughout the whole process (nFR03) ;
- ✓ **Criterion 4: Patient Empowerment:** The proposed approach should enhance citizen experience when taking charge of own choices in relation to access to own health data, reflecting good alignment to the DSM Strategy and the relevant policies as expressed in the eHealth Network MWP and the "EC Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society" (nFR04, nFR09, nFR11) ;
- ✓ **Criterion 5: Scalability** The preferred solution should have the minimum possible impact and disruption on the current deployment of the eHDSI; however, the solutions proposed should take a longer-term perspective, not least of the eHealth Network immediate priorities reflected in the MWP 2018-2021 (nFR10, nFR11) ;
- ✓ **Criterion 6: Availability** The proposed approach should appropriately balance digital patient empowerment against accessibility by minority segments of the population i.e. it should exploit widely used technologies by the European citizens (such as smartphones, personal connected devices etc) and also consider alternatives for minority situations (nFR04, nFR9, nFR11).

This approach will help us to identify the best solution, taking into account – one by one - all the key factors mentioned above.

6.3 Overview of possible approaches

We will present several possible solutions taking into account the knowledge gained from previous EU-funded projects and the challenge of HEALTHeID, which aims to integrate a comprehensive eIDAS authentication experience for the Patient. Being the Patient a central stakeholder in all possible approaches, we first try to identify how he/she can interact with the chosen eIDAS national Identity Provider, or in other words which tools and instruments he/she could use. After having studied several opportunities, we finally discovered three possible macro-categories of devices that the Patient could use:

- A *personal device*, owned by the Patient, in his/her availability at the Point of Care (e.g. a smartphone) ;
- A *device owned by the HP*, and available for all his/her Patients in the Point of Care (e.g. a desktop PC) ;
- A *device* available for all *Patients* ("*shared*") at the Point of Care and not owned or used by the HP (e.g. a desktop PC or a "kiosk").

Every solution is described with appropriate details in the sections below.

6.4 Solution A ("personal device")

1. HP opens the SP from a personal device (i.e. a notebook) and authenticates herself/himself using a specific, domestic Identity Provider (typically not joining the eIDAS network); this step can also be performed later in the flow, being independent of the Patient's authentication ;

2. The establishment of a specific relationship between the specific HP and the patient is achieved through the creation of a uniquely identified encounter by some means i.e. a unique session number identifier. Appropriate security measures could be applied, e.g. the session could expire once the relationship is created or unused for a certain period. It consists of 5 digits and could be communicated orally ;

3. The Patient is made aware of the issued HP-session-Id by the HP ;

4. In this proposal, the Patient is allowed to use a mobile device to login into the local SP using the eIDAS Identity Provider infrastructure, in order to gain authentication from an IdP in her/his country of affiliation (Country A); to do so, step 5 is performed ;

5. The Patient opens a web application (or an App) from her/his mobile device. At that moment, Patient is still not authenticated against the eIDAS network. The web application (or App) asks the Patient which is the Country of Treatment where she/he is located at that moment, in order to locate the right SP (the one from the Country of Treatment) ;

6. The SP requires the individual/patient is required to perform an eIDAS authentication using his/her device. Firstly, if not set as an App pre-defined parameter, the user is

asked to choose her/his Country of affiliation ("Where are you from?"), then the SP contact the eIDAS national connector, that exploiting the eIDAS eID infrastructure allow the authentication to proceed with the specific flow implemented by the National IdP (which are typically usable also from mobile devices, i.e. Italian IdPs are designed to do so); during the authentication flow, user is informed about who will access his/her data and why, and is required to explicitly authorize the SP to access his/her identity data (data to be disclosed are typically displayed to the user while asking for his/her *authorization*) ;

6.a. Depending on the national situation, the patient identifier may or may not be amongst the disclosed attributes. In the general situation where the patient identifier is still to be acquired a second identification step is invoked. The identified individual is prompted to provide own patient identifier. At the end of this step Patient identification has been achieved. Country A is responsible for the verification of the individual's patient identifier, before disclosing the data (as per the current CBHIS implementation of manual insertion by the HP) ;

6.b. If the patient is a minor, the identification step will be executed by the guardian, who will be identified and authenticated before being prompted to provide the identification data of the minor. The audit trail will in addition include details of the guardian-minor relationship. Country A is in addition responsible for the verification of the guardian-child relationship against its records, before disclosing the data (according to national procedures) ;

6.c. if the person is unable to provide consent, an appropriate "break the glass" procedure will be designed; this situation will not involve electronic patient identification and as such will not be implemented in the scope of HEALTHeID ;

7. The Patient is asked to insert the session unique-Id ;

8. After a successful patient identification and authentication, the SP knows both HP and Patient identities ; if, for any reason, the Patient identification fails, the flow stops, and can be resumed from step 4. ;

9. The Patient is asked (by the SP) to allow the specific HP to access her/his medical data, in the context of the defined session. Within this step the Patient Information Notice (PIN) visualization and subsequent confirmation of consent to disclose the requested patient data to the HP should also be included. If Patient agrees, the SP stores that *authorization* (*different* from the previous one given to the IdP) which has a pre-defined time limit: the HP will be allowed to access patient's medical data for a certain period of time, to be parametrized and defined according to the use case at hand , e.g. for the emergency use cases addressed in HEALTHeID this time limit will be properly set, while the Patient's will

to disclosure information will be stored for a proper length of time in the audit trail for the purposes of future audit (usually 10 years or more to ensure that the HP is protected in the event of any complaint about data processing), also checking the full adherence to GDPR regulations ;

10. After a successful authentication, the HP browses the authorizations to access medical data she/he has at that moment; that list contains also the authorization given by the Patient in the steps above ;

11. HP decides to access to Patient's medical data ;

12. The Patient is made aware of that access through a real-time push notification (if she/he is using an App), or an e-mail, or an SMS; in any case, the notification contains the identity of the HP which is accessing the medical data stored in Country A ;

13. The process now proceeds involving the steps of the Patient Summary and ePrescription use cases, which are not affected by the implementation of the HEALTHeID Connector.

The following are the major pros and cons of this scenario.

Major strengths: full mobile-oriented solution; proper eIDAS Patient identification.

Potential weaknesses: The Patient has to insert manually the HP's unique ID. The Patient needs to have a smartphone or other mobile device, and a working Internet connection abroad, or a Wi-Fi connection available at the point of care. This should not be a real issue in the nowadays scenario, where the majority of people traveling across Europe bring a smartphone with them, typically using a roaming-cost-free internet connection, or by using a Wi-Fi connection available at the Point of Care.

Other considerations: It seems easier to design and develop a fully responsive web application (SP) instead of developing an App (which connects itself to the SP) to install into the Patient's mobile device. Need to verify that all piloting Member States allow Patient's authentication using a mobile device; information available at the time of writing tell us that Portugal, Italy and Germany support this scenario.

We can briefly represent the evaluation criteria with the table below:

Criteria	Met (Yes/Maybe/No)	Comments

Compliance with eIDAS regulations	Y	The Patient uses eIDAS IdP from his/her device
Privacy by design	Y	The Patient is asked to allow any access attempted by an HP
Security	Y	Separate devices, no need to share authentication means
Patient empowerment	M	Mobile-oriented solution, quite an easy user experience. *However*, HP's identity needs to be inserted manually by the Patient
Scalability	Y	Can be leveraged to study a scenario where a Patient from Country A is treated in Country B from an HP from Country C
Availability	M	It implies the Patient has a smartphone connected to the Internet

6.5 Solution B ("personal device", QR code-enhanced)

Solution B is very similar to solution A, but during step 3 the recognition of the HP is improved using a QR code. The usage of a QR code could really help the Patient during his/her user experience at the Point of Care, and avoid any possible errors that could occur if the HP's unique-id could be communicated and inserted using other means, like depicted in Solution A.

Moreover, the QR code can easily contain both an HP's unique-Id and HP's Country of Affiliation. This means that an automatic scan of the code could also recognize the HP's Country of Affiliation and invoke the "right" SP (step 5).

We can briefly represent the evaluation criteria with this table (grey=unchanged from Solution A):

Criteria	Met (Yes/Maybe/No)	Comments
Compliance with eIDAS regulations	Y	The Patient uses eIDAS IdP from his/her device
Privacy by design	Y	Patient is asked to allow any access attempted by an HP
Security	Y	Separate devices, no need to share authentication means.

Patient empowerment	Y	Mobile-oriented solution, quite easy user experience. HP's identity automatically detected through a QR code. If using an App, the Country of Treatment could be also automatically detected by a localization function (GPS)
Scalability	Y	Can be leveraged to study a scenario where a Patient from Country A is treated in Country B from an HP from Country C
Availability	M	It implies patient has a smartphone connected to the internet, able to scan a QR

6.6 Solution C ("personal device", SMS/link-enhanced)

The solution C is very similar to solution A, but in step 5 the Patient receives a link (through either SMS or email) that contains the HP-session-Id and other information, like the Country of Treatment. Once clicked, the link would initiate the web app, invoke the SP and relay the information (HP-session-Id, Country of Treatment), without any user input. This process replaces the former steps 3-4-5. Then, Patient authentication is performed in step 6. The user experience could be improved by displaying the HP's photo and name/surname when the Patient clicks on the link received. Doing so, the Patient would be sure that the link is "genuine" and actually assigned to that HP.

We can represent the evaluation criteria with the table below (grey=unchanged from Solution A):

Criteria	Met (Yes/Maybe/No)	Comments
Compliance with eIDAS regulations	Y	The Patient uses eIDAS IdP from his/her device
Privacy by design	Y	Patient is asked to allow any access attempted by HP
Security	Y	Separate devices, no need to share authentication means. No need to have an App installed, no security concerns

Patient empowerment	Y	Mobile-oriented solution, very easy user experience. HP's identity automatically detected through an SMS or e-mail
Scalability	Y	Can be leveraged to study a scenario where a Patient from Country A is treated in Country B from an HP from Country C
Availability	M	It implies the patient has a smartphone connected to the internet

6.7 Solution D ("HP-owned device")

The difference here is that HP and Patient use the same device, typically owned by HP, located at the point of care. The flow is the same as depicted in Solution A.

Major strengths: no need for the Patient to have a smartphone (or any other device).

Major weaknesses: poor user experience (device need to be shared); the IdP used by the Patient must implement an authentication scheme compatible with the "shared device" (e.g. if the IdP requires to send an SMS as two-factor authentication, a PC/tablet/kiosk cannot be used). This also has an impact on the Level of Assurance (LoA) of the authentication a user can gain: the impossibility to use a certain device leads to the impossibility to get a particular LoA (significant limitation).

The evaluation criteria are represented in the table below (grey=unchanged from Solution A):

Criteria	Met (Yes/Maybe/No)	Comments
Compliance with eIDAS regulations	Y	The Patient uses his/her eIDAS IdP, even if from a third-party device, but problems should arise if IdP requires a telco SIM in order to deliver an SMS to complete the authentication
Privacy by design	Y	HP device is integrated with the SP security system
Security	Y	HP device is integrated with the SP security system

Patient empowerment	N	Poor user experience due to the usage of the same device by the Patient and an HP
Scalability	M	Use cases where the patient is not at the Point of Care cannot be implemented
Availability	Y	It is independent ofo the patient smartphone availability

6.8 Solution E ("Patients-shared device")

In this approach, the HP uses his/her device, while the Patient uses a shared device, connected to the Internet, available for any Patient, installed at the point of care (e.g. a PC, or a tablet, or a "kiosk"). The flow is the same as depicted in Solution A.

Major strengths: no need for the Patient to have a smartphone.

Major weaknesses: potential security issues (Patient would be required to authenticate against his/her IdP using a shared device, which should be in any case hardened to avoid security breaches); the IdP used by the Patient must implement an authentication scheme compatible with the "shared device" (e.g. if the IdP requires to send an SMS as two-factor authentication, a PC/tablet/kiosk cannot be used). This also has an impact on the Level of Assurance (LoA) of the authentication a user can gain: the impossibility to use a certain device leads to the impossibility to get a particular LoA (significant limitation).

The evaluation criteria are represented in the table below (grey=unchanged from Solution A):

Criteria	Met (Yes/Maybe/No)	Comments
Compliance with eIDAS regulations	Y	The Patient uses his/her eIDAS IdP, even if from a third-party device, but problems should arise if IdP requires a telco SIM in order to deliver an SMS to complete the authentication
Privacy by design	Y	Being in a potentially open area, some data MUST be hidden from occasional observers
Security	M	The device is integrated with the SP security system, potential security issues could be present and must be avoided with a proper hardening of devices
Patient empowerment	Y	Usability might be higher, especially for the elderly, having a bigger screen than a smartphone (better User Interface design, better display of the PIN,…) The user may be skeptical to use the same device like all other Patients at a Point of Care
Scalability	M	Use cases where the patient is not at the Point of Care cannot be implemented
Availability	Y	It is independent of the availability of a patient smartphone In Pharmacies, it could be difficult to set up an ad-hoc kiosk

7. Conclusions

In this document, five scenarios have been studied and presented. Considering the coverage of the evaluation criteria in each scenario, Solution C seems to be the best possible approach to exploit the eIDAS patient's authentication and provide a good user experience. For example, Solution A, although similar, present one weakness, namely in term of Patient empowerment (Solution A), as explained in the tables above. The

evaluations made in this deliverable will be used in other HEALTHeID's deliverables to identify and develop the most suitable solution, which will be based (fully or partially) on the ideas addressed in this document.

End of document