HEALTHeID

eIDAS – OpenNCP
Connector for eHealth

D2.1. HEALTHeID Functional Specification

Action 2017-EU-IA-0044

Co-financed by the Connecting Europe Facility of the European Union

Document Information:

Document status:	Final
Document Version:	1.1
Date	21-10-2019
Author(s):	Andrea Atzeni (POLITO), Andrew Short (AUTH), Maid Erovic (GEMATIK), Joao Pedro Cunha Gonçalves (SPMS), Alberto Zanini (ARIA), Abel Tenera (Caixa Magica), Marcello Melgara (ARIA)
Member State Contributor(s):	SPMS, Caixa Magica (Portugal), POLITO, ARIA (Italy), gematik (Germany), AUTH (Greek)
Stakeholder Contributor(s):	

Disclaimer

The content of this deliverable represents the views of the authors only and is their sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Innovation and Networks Executive Agency (INEA) or any other body of the European Union. INEA is not responsible for any use that may be made of the information it contains.

Table of Contents

1. About this document 8
1.1. Scope 8
1.2. Key words 9
1.3. Document outline 9
2. Use case scenario 10
3. HEALTHeID scenario 11
4. Functional Requirements 12
5. eIDAS architecture 13
5.1. eIDAS logical architecture and process flow 13
5.2. eIDAS Message Format 14
5.3. eIDAS attributes naming 15
6. OpenNCP architecture 17
7. Member specific eID schemes 21
7.1. Italian eID – SPID (Sistema Pubblico di Identità Digitale) 21
7.2. German eID - the German eIDAS-Middleware 27
7.3. Portuguese eID – Autenticacao.gov, from AMA (Agência para a Modernização Administrativa) 33
7.4. Greek eID – ermis.gov.gr, from HMAR (Hellenic Ministry of Administrative Reconstruction) 33
8. Member specific NCPeH adaptation 35
8.1. Portuguese OpenNCP adaptation 35
9. HEALTHeID architecture 37
9.1. Interfaces 39
9.2. Message Flow 43
10. Security considerations 47

List of Figures

Figure 1 - eIDAS logical cross-border architecture 13
Figure 2 - internal components of an OpenNCP-based NCPeH 18
Figure 3 - eIDAS-SPID connecting architecture 24
Figure 4 - Italian SP and foreign citizen of an eIDAS proxy-based country 25
Figure 5 - Italian citizen and foreign SP of an eIDAS proxy-based country 25
Figure 6 - Italian SP and foreign citizen of an eIDAS middleware-based country 26
Figure 7 - Italian citizen and foreign SP of an eIDAS middleware-based country 26
Figure 8 - Integration of the German eIDAS-Middleware into the eIDAS network 27
Figure 9 - Message flow of the authentification of German citizens 31
Figure 10 - Portuguese OpenNCP adaptation 35
Figure 11 - HEALTHeID architecture high level view – eIDAS proxy based scenario 38
Figure 12 – Message Flow 45

List of Tables

Table 1: eIDAS attributes list 16
Table 2: OpenNCP core components 19
Table 3: National components 19
Table 4: Definitions of SPID qualified attributes 22
Table 5: Present mapping among SPID and eIDAS attributes 23
Table 6: Attributes mappring (eID card – eIDAS) 30
Table 7: Portuguese extras description 36
Table 8: Description of operations for a successful encounter 46

History of revisions		
Date	**Comments**	**Author**
21-11-2018	First draft	Andrea Atzeni
06-12-2018	Addressed comments from Gematik, initial content regarding eIDAS and the Italian eID notified scheme	Andrea Atzeni
11-01-2019	Updated message flow for the proxy case, added German middleware message flow, introduced the description for the German national scenario, added the description of the eHDSI component, and integrated further comments from Gematik, Auth, SPMS, ARIA	Andrea Atzeni, Joao Pedro Cunha Gonçalves, Maid Erovic, Andrew Short, Alberto Zanini
07-02-2019	overall document revision, added details on the Italian eID, updated information on the Portuguese national eID schema, integrated further comments from ARIA.	Andrea Atzeni, Joao Pedro Cunha Gonçalves, Abel Tenera, Marcello Melgara
10-03-2019	Updated the overall schema and the data workflow	Andrea Atzeni, Joao Pedro Cunha Gonçalves, Marcello Melgara, Alberto Zanini
26-03-2019	Minor addition to the Encounter Management description, major addition to the Interface between the NCP HProxy and NCPeH (major addition), new Interface between the NCPeH A/B and eHDSI Central Configuration Services (new)	Joao Pedro Cunha Gonçalves
23-05-2019	Update based on the discussion of the Athens meeting (introduction of the HeID Client to maintain as much as possible the OpenNCP Portal structure, information on the Greek eID schema)	Andrea Atzeni
05-08-2019	Update based on the discussion of the Prague meeting (revision of the architectural and sequence diagram and corresponding descriptions)	Andrea Atzeni
21-10-2019	Revision and harmonization - the example stored data section has been removed since superseded by more recent work in the integration guide and around PIN, the sequence diagram has been updated for coherency with general use case discussion	Andrea Atzeni

Bibliography		
Id	**Document title**	**Author**
HeID-T1.2	Usability Requirements	HEALTHeID Consortium
eIDAS-Arch	eIDAS Interoperability Architecture v1.00 available: https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eidas_interoperability_architecture_v1.00.pdf	eIDAS Technical Subgroup
eIDAS-Message	eIDAS SAML Message Format v1.1 available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile?preview=/46992719/47190128/eIDAS%20Message%20Format_v1.1-2.pdf	eIDAS Technical Subgroup
eIDAS-attr	eIDAS SAML Attribute Profile v1.1	eIDAS Technical

Bibliography		
Id	**Document title**	**Author**
	Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eIDAS%20SAML%20Attribute%20Profile%20v1.1_2.pdf	Subgroup
SPID	SPID - Regole tecniche Available: http://www.agid.gov.it/sites/default/files/circolari/spid-regole_tecniche_v1.pdf.	Agenzia per l'Italia Digitale
SAML-SSO	Web Single Sign-On Interoperability Profile Available: http://xml.coverpages.org/WebSSO-InteropProfile200505.pdf	
eIDAS-IF	EU: COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1501&from=EN	
BSI TR-03130-3	Technical Guideline TR-03130-3; eID-Server – Part 3: eIDAS-Middleware-Service for eIDAS-Token; Version 1.0; 5th May 2017 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130/TR-03130_TR-eID-Server_Part3.pdf?__blob=publicationFile&v=4	
BSI TR-03130-1	Technical Guideline TR-03130 eID-Server – Part 1: Functional Specification; Version 2.1.2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130/TR-03130_TR-eID-Server_Part1.pdf;jsessionid=8240103ABE09D75661C53755250FF5CA.2_cid351?__blob=publicationFile&v=5	
TR-03124-1	Technical Guideline TR-03124-1 eID-Client – Part 1: Specifications; Version 1.3 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03124/TR-03124-1.pdf?__blob=publicationFile&v=2	
eHDSI-XCPD	XCPD Profile Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/35210463/eHDSI_XCPD_Profile_v2.2.0.pdf?version=1&modificationDate=1535557839560&api=v2	eHealth DSI provider
eHDSI-XCA	XCA Profile Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/35210463/eHDSI_XCA%20Profile_v2.2.0.pdf?version=1&modificationDate=1535557787829&api=v2	eHealth DSI provider
eHDSI-XDR	XDR Profile Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/35210463/eHDSI_XDR%20Profile_v2.2.0.pdf?version=1&modificationDate=1535557880669&api=v2	eHealth DSI provider
eHDSI-Audit	Audit Trail Profiles Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/35210463/eHDSI_Audit_Trail_Profiles_v2.2.0.pdf?version=1&modificationDate=1535472249756&api=v2	eHealth DSI provider

Bibliography		
Id	**Document title**	**Author**
eHDSI-SAML	SAML Profiles Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/35210463/eHDSI_SAML%20Profile_v2.2.0.pdf?version=1&modificationDate=1535472311374&api=v2	eHealth DSI provider
eHDSI-SMP	Service Location and Capability Lookup Profile Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/35210463/Service%20Location%20and%20Capability%20Lookup%20Profile_v2.1.0.pdf?version=2&modificationDate=1535557667008&api=v2	eHealth DSI provider
eHDSI-eADC	eADC Specifications Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/35210463/eHDSI_eADC_Specifications_v2.2.0.pdf?version=1&modificationDate=1532525892418&api=v2	eHealth DSI provider
eHDSI-X.509	X.509 Certificate Profiles Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/35210463/eHDSI_X.509_Certificates_Profile_v2.2.0.pdf?version=1&modificationDate=1535557731152&api=v2	eHealth DSI provider
eHDSI-Messaging	Messaging Profile Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/35210463/eHDSI_Messaging%20Profile_v2.2.0.pdf?version=1&modificationDate=1535472289110&api=v2	eHealth DSI provider
NCPeH-guide	Guideline on an Organisational Framework for eHealth National Contact Point	eHealth Network
eHDSI-PS	eHealth DSI Patient Summary and ePrescription *PS Functional requirements* Available https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Specifications?preview=/35210463/65979541/PS%20functional%20requirements_v2.2.2.pdf	eHealth DSI provider
ECRec_19_2_6	COMMISSION RECOMMENDATION of 6.2.2019 on a European Electronic Health Record exchange format	European Commission

1. About this document

This document is a milestone of Task 2.1 -"Functional Requirements and Design" which aims to define functional requirements to ensure compliance of the eHealth eIDAS eID implementation to the relevant eHDSI and eIDAS scenarios. Based on these requirements, the task will propose and validate the design of the reference implementation of the eHealth eIDAS Connector-B (a.k.a. HeID connector) as a generic software component encapsulating all necessary eIDAS functionalities into the eHealth DSI's eHealth NCP.

In the following the HeID connector functional specification is presented, addressing requirements and design, for citizen identification and authentication in cross border eHealth situations, elaborated under Activity 2.

As input sources, this activity gets

- Activity 1 output, namely D1.1 HEALTHeID vision and D1.2 HEALTHeID usability requirements. The production from Activity 1 focuses on the identification of non-functional requirements (nFR), i.e. policy, organisational and legal aspects, as well as relevant scenarios and usability guidelines.
- Applicable specifications and implementations, from eIDAS and eHDSI fields, to guarantee coherent adoption of protocols and maintain practical feasibility and integration of the developed components, i.e. the HEALTHeID Connector.
- A selected set of National specific situation, namely Italian, German and Portuguese ones, to exemplify the peculiarities of different National scenarios, both from eIDAS and eHDSI perspective.

This document aim is to integrate these input in a technically sound manner, providing a set of requirements for the HEALTHeID connector, coherent to the specifications developed in relevant scenarios for Patient Summary and ePrescription cases, as well as a reference architecture and message flow for the development of the HeID connector.

1.1. Scope

Given the COMMISSION RECOMMENDATION of 6.2.2019 on a European Electronic Health Record exchange format, in particular "Member States should ensure that citizens and their healthcare professionals have online access to their electronic health records using secure electronic identification means, taking into account the framework for security and trust established by the Regulation (EU) No 910/2014." the output of this document will allow the development, testing and delivery of the HEALTHeID connector to the European Commission (EC) and the Member States (MSs) as an open-source implementation, in a Technology Readiness Level (TRL) 6 environment, to link the national OpenNCP-based National Contact Points for eHealth (NCPeH) to the eIDAS node.

The definition is meant to be applied to the Use Cases identified in Activity 1.

1.2. Key words

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this interpreted as described in [RFC2119].

1.3. Document outline

Section 2 describes the scenarios relevant for this project, distilling the work done in Activity 1.

Section 3 introduces the purpose of HEALTHeID, in the light of eIDAS and eHDSI.

Section 4 presents the list of functional requirements.

Section 5 and 6 briefly presents the eIDAS and OpenNCP infrastructure and components to highlight in a later section how these two worlds can be connected.

Section 7 and 8 present the peculiarities of a selected set of participating countries, respectively on eIDAS eID and on eHDSI OpenNCP side, to develop the HEALTHeID connector considering the specificities different member state.

Section 9 discusses the proposed HEALTHeID architecture introducing the components, the scope of the interfaces and the message flow among the components.

Section 10 discusses the security concepts relevant for the HEALTHeID architecture.

2. Use case scenario

According to 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 eIDAS architecture is particularly suitable to accomplish this requirement in a scalable and strongly secure way.

eIDAS assumes an electronic identification workflow, where the citizen coming from a country A requests a service from a Service Provider (SP) in a country B, 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 an eIDAS component provided by country A - this may be the Country-A eIDAS Node, or a component provided by Country-A but operated in Country B (i.e. the German Middleware Service case), in an interoperable transport form (i.e. through eIDAS SAML Assertions). Such assertions can be requested through an authentication request by a legitimate service provider (SP) through an eIDAS component (either the eIDAS Connector deployed in Country-B or through the German Middleware). These assertions adhere to international technical standards and provide intrinsic and extrinsic security safeguards (such as an electronic signature safeguarding integrity, authenticity, and correctness). The SP as a relying party may technically and legally trust the assertions contents as a reliable form of citizen authentication.

The project has studied several possible alternatives related to patient interaction, as detailed in [HeID-T1.2], trying to find the best possible solution with an appropriate trade-off between user-friendliness and security. Developing this discussion, it emerged that the target solution should have been "user-centric", with effective empowerment of the patient involved in the encounter with an HP, and possibly "mobile oriented". While our technical solution can be appliead to different scenarios identified in T1.2 with minor adaptation, we discovered that one of the most usable solutions is to assume that the Patient can use her personal mobile device to authenticate herself against her National eIDAS IdP and to authorise an HP to access her medical data. This scenario is described in [HeID-T1.2], while the architecture to accomplish that as well as the needed flow to implement it are described in the last part of the document, namely HEALTHeID architecture.

3. HEALTHeID scenario

As detailed in Activity 1 [HeID-T1.2], the current eHDSI specifications define a set of functional requirements for both the Patient Summary (PS)[1] and ePrescription/eDispensation (eP/eD)[2] As detailed in Activity 1 [HeID-T1.2], the current eHDSI specifications define a set of functional requirements for both the Patient Summary (PS) and ePrescription/eDispensation (eP/eD) use cases, where a patient from Country A (country of affiliation) seeks healthcare in Country B (country of treatment). To support such use cases, the eHealth DSI Technical Community made available the OpenNCP suite, a set of openly usable and adaptable components being able to provide a full NCP[3] or a subset of features, according to the specific country needs.

eIDAS introduces 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.

CEF provides a reference implementation following the eIDAS Technical Specifications v1.1, available under EUPL license, consisting of an eIDAS node components that can be used as a baseline to develop any country specific eIDAS infrastructure, and allowing to connect different countries to the cross-border EU eIDAS node infrastructure.

Aim of this project is the development of the HEALTHeID Connector. 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. Specifically, it is a component that allows interacting with the eIDAS infrastructure with the openNCP-based one.

The HEALTHeID connector, aiming to merge eIDAS and eHDSI worlds, must take into account the requirements coming from both frameworks, as well as non-functional ones identified in Activity 1 of this project. In the following section, these will be presented.

Also, the specific country situation must be identified, to coherently merge the two architectures and take into account the national specific peculiarities.

In the following, the usual eIDAS and eHDSI scenarios are presented in isolation, followed by the presentation of country-specific peculiarities of both.

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

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

3 National Contact Point, i.e. the country gateway to access to contact to access the national eHEALTH system

4. Functional Requirements

Functional requirements are distilled from output of the Activity 1. In particular, non-functional requirements determined in the deliverable D1.1. Also, they are adherent to the work done in [eHDSI-PS] as well as eIDAS technical specification and implementing acts.

They are organised detailing the number, the relevant non-functional requirements, the components involved and the action involved, associated to a specific keyword that express the mandatory (MUST) or optional (MAY) status of the requirement.

FR01 (derived from nFR1 and nFR5): The HEALTHeID Connector MUST adopt a coherent protocol profile to interact with the national eIDAS connector.

FR02 (derived from nFR1): The HEALTHeID Connector MUST have established a trust relationship with the national eIDAS connector.

FR03 (derived from nFR2 and nFR4 and nFR5): the HEALTHeID Connector MUST provide an interface for the insertion of the patient identifier.

FR04 (derived from nFR2) the HEALTHeID Connector MAY use the retrieved identification data to complete the patient identifier.

FR05 (derived from nFR3) The HEALTHeID Connector MUST adopt authentication schemes coherent with the LoA used in the eIDAS cross-border authentication scheme.

FR06 (derived from nFR5) the HEALTHeID Connector MUST provide an interface for the communication of the patient identifier towards the NCPeH component.

FR07 (derived from nFR06 and nFR07) the HEALTHeID Connector MUST ensure lawful processing of personal data presenting to the user textual information about the foreseen use of the data, and the context of use (e.g. a specific healthcare encounter, a specific period of time).

FR08 (derived from nFR06) the HEALTHeID Connector MUST provide an interface for the patient to provide an informed consent.

FR09 (derived from nFR09) the HEALTHeID Connector MUST provide adequate input/output interfaces to allow patient use of personal devices (like a personal smart-phone).

5. eIDAS architecture

The European Union Regulation No.910/2014 on electronic identification and trust services for electronic transactions in the internal market, adopted on 23 July 2014, a.k.a. eIDAS Regulation, provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities, ensuring that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available

The Commission has emitted "*a stable eIDAS compliant set of technical specifications which the Member States can use if they are providing their implementation. These technical specifications will be subject to further development in the normal course of events and any subsequent changes will form part of the timed release management process*" where are detailed (1) the interoperability architecture [eIDAS-Arch], (2) the SAML attribute format [eIDAS-attr], (3) the SAML message format [eIDAS-message], and (4) the requirements for confidentiality and how they can be achieved through SAML message encryption.

The eIDAS architecture exploits SAML elements and attributes, according to the SAML WebSSO-Profile [SAML-SSO]. The Metadata trust management is specified in eIDAS interoperability architecture specification, e.g. the metadata document MUST be properly signed according to the eIDAS specification.

5.1. eIDAS logical architecture and process flow

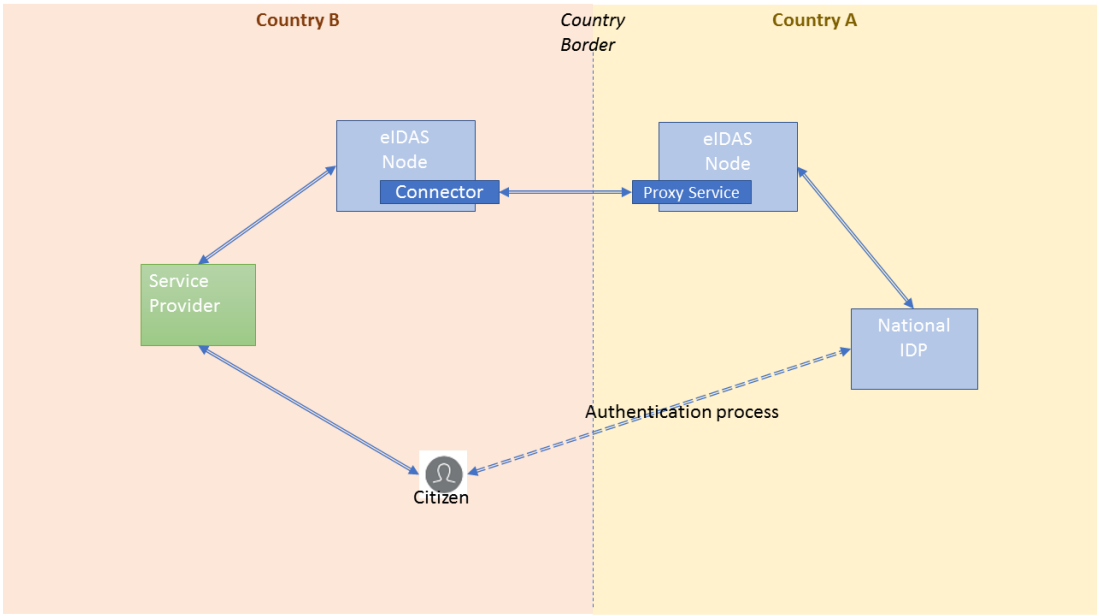

Figure 1 - eIDAS logical cross-border architecture

Fig.1 depicts the logical block diagram of the eIDAS architecture. According to this high-level architectural view, eIDAS specification foresees the following flow to authenticate a person in posses of a digital identity in the eID-scheme of the country A, to an SP established in Country B.

Note: the following flow omits a number of details (e.g. the role of the user agent, the required verification of the authenticity at each hop of the Request, the metadata exchange to establish trust among nodes) since it's purpose is to depict the logical interaction among components of the eIDAS infrastructure. For a finer-grain detail level, see [eIDAS-Arch] and related specifications.

1. the SP sends an authentication request to the eIDAS-Connector responsible for it. The request MAY contain an identifier identifying the Country B if known at this point
2. The eIDAS-Connector SHALL request the citizen origin country if this information was not already contained in the request.
3. The eIDAS-Connector SHALL send a SAML-Request to the eIDAS-Proxy Service of Country A.
    a. If the eIDAS-Proxy Service serves several eID schemes, the Service SHOULD provide a scheme selection interface for the user.
    b. If the requesting relying party is a private entity, the Service MAY reject the Request if the terms of access of the eID scheme are not fulfilled.
    c. If the requested (or higher) Level of Assurance cannot be fulfilled by the eIDAS-Service, the Request MUST be rejected.
4. The eIDAS-Proxy Service SHALL send the request to the National IdP
5. The Country A national IdP, according to the selected eID scheme at least on the requested Level of Assurance, perform the authentication of the person and SHALL send the SAML Response to the eIDAS Proxy Service.
6. The eIDAS proxy Service SHALL send a SAML Response to the requesting eIDAS-Connector containing an encrypted SAML Assertion.
7. The Connector MUST verify that the Level of Assurance indicated in the Assertion matches or exceeds the requested Level of Assurance, and send the received authenticated person identification data to the requesting SP.

Error handling SHALL follow the SAML specification.

5.2. eIDAS Message Format

The eIDAS interoperability framework allows for cross-border identification and authentication processes through the exchange of SAML 2.0 messages, including personal and technical attributes.

The use of SAML metadata is required between different eIDAS components. Before an actual SAML request or SAML response can happen, eIDAS components need to exchange Metadata for agreeing on key parameters of the transaction (like certificates to establish trust and supported attributes). The format of eIDAS metadata is described in [eIDAS message format], as well as the format for an aggregated list of the metadata locations across Member States.

Regarding attributes "*eIDAS-Services MUST support at least all mandatory attributes as specified in [eIDAS-Attr-Profile"]. Optional attributes of [eIDAS-Attr-Profile] SHOULD be supported. Other optional attributes beyond the ones defined in [eIDAS-Attr-Profile] MAY be supported. Attributes not defined in [eIDAS-Attr-Profile] MAY require bilateral agreement on acceptance between eIDAS-Connector and eIDAS-Service"*

Only attributes that are published in the SAML metadata of the eIDAS-Service can be requested by an eIDAS-Connector. Requested attributes by an eIDAS-Connector from an eIDAS-Service MUST be carried out by including them in a SAML AuthnRequest. Attributes requested but not supported by an eIDAS-Service MUST be ignored.

When requesting a minimum data set, at least all attributes defined as mandatory in this minimum data set MUST be requested. At least one minimum data set MUST be requested in each SAML Authentication request.

The eIDAS Regulation enables citizens/patients identification and authentication using their national eID credentials via a trust network of national eIDAS nodes. The eIDAS nodes mandate a notification process of national eID on a voluntary basis. Any Member State can decide if and which national eID system(s) will be notified to the EC. When the notification process (i.e. review of the notified eID) ends, the recognition of eID schemes is mandatory for other MS participants for accessing public online cross border services. According to the notification process and the interest in this project, there can be four different eID scheme types

- *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
- *peer-reviewed* - The eID scheme has been peer-reviewed by other Member States' representatives.
- *pre-notified* - The Member State has officially communicated its intention to notify its eID scheme to the European Commission.
- "*under consideration*" - The country has the intention to communicate an eID scheme but no official communication is still available (possibly, the scheme has been used in cross-border testing among eIDAS nodes in different countries).

5.3. eIDAS attributes naming

The eIDAS specifications [eIDAS-attr] describe the list of qualified attributes supported by eIDAS-IdP, reported below ("NC" means Nationality Code in ISO 3166-1, "Date" format refers to the XML Schema instance namespace definition of dates, represented as a string in the format "YYYY-MM-DD").

Note: only the natural person attribute list is described since the legal person set is out of HEALTHeID scope.

Name	Person type	Format	Notes
PersonIdentifier (mandatory)	Natural	String	(NC e-ID) + "/" + (NC SP) + "/" + (unique identifier of user's e-ID)
FirstName (mandatory)	Natural	String	
FamilyName (mandatory)	Natural	String	
DateOfBirth (mandatory)	Natural	Date	
BirthName	Natural	String	
PlaceOfBirth	Natural	String	Name of the city in which the user was born

CurrentAddress	Natural	XML	Base64 encoding of an XML sequence of strings:
			`<eidas:LocatorDesignator>`
			`<eidas:ThoroughFare>`
			`<eidas:PostName>`
			`<eidas:PostCode>`

Gender	Natural	String	"Male", "Female", "Not Specified"

Table 1: eIDAS attributes list

6. OpenNCP architecture

The eHDSI reference implementation of a National Contact Point for eHealth – OpenNCP -, follows an architecture emerging from the combination of IHE profiles. In this perspective, the NCPeHs act as gateways (corners 2 and 3) in a typical 4-corner architectural model, employing standardized IHE-profiled transactions across borders, while leaving to the deploying countries the decision on the message format and profile to be used in the communications towards the national infrastructure (corners 1 and 4). The main business transactions between NCPeHs rely on profiles of the:

- IHE XCPD, for discovery of patient demographic information in his/her country of affiliation [eHDSI-XCPD];
- IHE XCA, for accessing metadata of the patient's clinical documents as well as accessing a specific clinical document [eHDSI-XCA];
- IHE XDR, for submitting a clinical document to his/her country of affiliation [eHDSI-XDR].

Authentication of the end-user (HP), as well as the establishment of a treatment relationship between the former and the patient, is performed at the national level. Such authentication and treatment context claims are brokered by NCPeH-B towards NCPeH-A. The former vouches for the accuracy, integrity and authenticity of such claims, and the latter verifies their integrity and authenticity, establishing the eHealth Direct Brokered Trust Model. This brokerage is possible due to the usage of a slightly modified version of the IHE XUA profile. Claims are consolidated in SAML 2.0 assertions that are communicated alongside the previously mentioned IHE X* messages [eHDSI-SAML].

The profile on IHE ATNA and ETSI REM [eHDSI-Audit], as well as its mandatory dependence on IHE CT, provide the requirements for enriching the NCPeH secure node with auditability and non-repudiation mechanisms, in a timely-consistent way.

The NCPeH collects statistical data on the usage of the 3 main IHE profiles used for the business transactions (XCPD, XCA, XDR) [eHDSI-eADC].

NCPeHs' metadata include certificates, endpoints and international search masks. These are shared via the eHDSI Central Configuration Services [eHDSI-SMP]. The eHDSI certificates profiles [eHDSI-X.509] define the profiles of certificates to be used for Website Authentication (i.e., mutual TLS authentication) and Signature.

The eHDSI Messaging Profile [eHDSI-Messaging] summarizes the underlying standards stack used in the NCPeH.

With regards to the interaction between corner 1 (HP Portal, i.e., the eIDAS Service Provider) and corner 2 (NCPeH-B), the OpenNCP currently provides a non-standard interface, based on SOAP web-services, that portals can use to call the NCPeH cross-border services.

The following picture shows the internal components of an OpenNCP-based NCPeH.

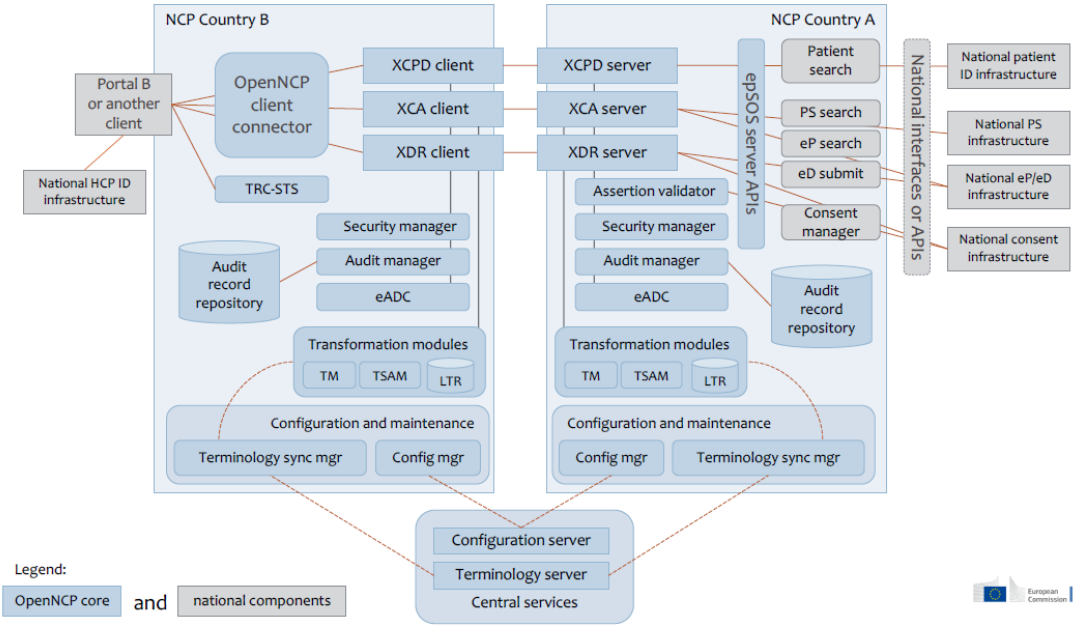

Figure 2 - internal components of an OpenNCP-based NCPeH

The following table summarizes the OpenNCP core components (identified in blue in the previous picture).

Component	NCPeH (A/B)	Description
OpenNCP client connector	NCPeH-B	Allows portals (or other clients) to call the IHE clients. It exposes a non-standard SOAP interface.
XCPD/XCA/XDR client	NCPeH-B	IHE clients that call services exposed by other NCPeHs to implement the cross-border exchanges.
TRC-STS	NCPeH-B	Secure Token Service that issues an NCPeH-B-signed Treatment Relationship Confirmation SAML assertion.
Security manager	NCPeH-A/B	Implements PKI operations, e.g., digital signatures generation and validation.
Audit manager	NCPeH-A/B	Establishes communication towards the OpenATNA-based Audit Record Repository in order to assemble and persist audit messages. This repository can be consulted through a Web user interface.
eADC	NCPeH-A/B	Automatic Data Collector, persists IHE-transactions statistical data.
Assertion validator	NCPeH-A	Validates SAML assertions used in the IHE transactions.
XCPD/XCA/XDR server	NCPeH-A	Exposes IHE services to other NCPeHs.

Component	NCPeH (A/B)	Description
eHDSI server APIs	NCPeH-A	Set of interfaces that connect the IHE services to the national infrastructure through the National Connector.
Transformation modules (TM, TSAM, LTR)	NCPeH-A/B	Transformation Manager (TM), Terminology Services Access Manager (TSAM) and Local Terminology Repository (LTR) work together to perform the semantic transformations of clinical documents.
Configuration and maintenance (Terminology sync manager, Configuration manager)	NCPeH-A/B	Terminology sync manager (TSAM-Sync) synchronizes the semantic assets from the Central Terminology Server (CTS) to the LTR. Configuration Manager performs CRUD operations on the NCPeH configuration properties database (some of these properties are fetched from the Central Configuration Server – SMP).
Configuration and maintenance (OpenNCP-Gateway)	NCPeH-A	Web-based backoffice which allows the creation, signature and publishing of the NCPeH configuration (metadata) in the Central Configuration Server (SMP).

Table 2: OpenNCP core components

With regards to the national components (identified in grey), we have the following:

Component	NCPeH (A/B)	Description
Portal B or another client	-	End-user solutions and other middlewares of country-B that provide cross-border eHealth features to health professionals.
National HCP ID infrastructure	-	Health professionals identity provider of country-B.
Patient search / PS search / eP search / eD submit / Consent manager	NCPeH-A	Implementations of the interfaces provided by the epSOS server APIs, that connect the NCPeH-A to the national infrastructure. Together they form the National Connector, which is a component developed by each country.
National interfaces or APIs	-	Interfaces used by the National Connector to call the different national services.
National patient ID/PS/eP/eD/consent infrastructure	-	National registries and/or repositories of patient identification data, patient consent and clinical data (PS and eP/eD).

Table 3: National components

The previously detailed components can be correlated with the initially summarized description of the profiles and protocols provided in the beginning of this section. An exception is made for the Policy Manager and the HP Identity Assertion. The OpenNCP bundles a default implementation of a policy manager, which is responsible for implementing access control policies on NCPeH-A side. Similarly to the National Connector, countries can provide their own implementation of a policy manager, fine-tuned for their national specificities, thus discarding the default one. With regards to the HP Identity Assertion, [eHDSI-SAML] states: "eHealth DSI does not make any assumptions on whether NCP-B or a national service within country B acts as the initial Identity Provider that verifies the identity and authenticity of an HP. The only constraint imposed by eHealth DSI is that NCP-B vouchers for the issued assertions and therefore is considered as the Identity Provider with respect to NCP-A as the assertion consumer." Therefore, the eHDSI HP Identity Assertion may be generated by the national infrastructure of country-B (e.g., this is the situation of those countries relying on the eHDSI-distributed OpenNCP Portal) or by the NCPeH-B itself.

7. Member specific eID schemes

The EU national eID infrastructures historically emerged in isolation, developed considering only specific national (or even regional) requirements. Cross-border eID was not a priority in many countries, so every EU state developed its own set of rules and technological implementation. This section details a subset of national eID used in the context of eIDAS, i.e. involved in the eIDAS notification process, thus in the scope of HEALTHeID project relevant as examples of differences among Member States.

7.1. Italian eID – SPID (Sistema Pubblico di Identità Digitale)

In Italy, the *Sistema Pubblico di Identità Digitale* (SPID) addresses e-ID interoperability at the national level. It is composed by a set of trusted private and public services that can handle authentication of Italian citizens and companies for the public administration. SPID credentials are required to access public services, simplifying the interaction between entities and increasing security of the user authentication. Various credentials can be used, ranging from traditional ones based on smart-cards (e.g., the citizens' service card, CNS) to modern systems (e.g., one-time password generators, implemented as smartphone applications or via a hardware device). SPID has to interact with the eIDAS platform to provide authentication of Italian citizens in a cross-border environment.
SPID components, as described in the technical specifications [SPID] consists of a set of

- *SPID Identity Providers* (SPID-IdP) - public or private subjects that handle registration and emission of e-ID credentials for users.
- *SPID Service Providers* (SPID-SP) - public or private subjects that can request users' authentication to SPID-IdP.
- *SPID Attribute Providers* (SPID-AP) can be used in conjunction with SPID-IdP to provide certified properties of the authenticated user to SPID-SP.

SPID components interact with each other using the SAML 2.0 language, for whom a specific profile has been defined.

Definitions of SPID qualified attributes are reported in the table below. "Date" format refers to the XML Schema instance namespace definition of dates, which are represented as a string in the format "YYYY-MM-DD". No attributes are mandatory, according to SPID technical specifications.

Name	Attribute type	Format	Notes
spidCode	Primary	String	SPID-IdP identification code (4 letters) + e-ID unique identifier (10 characters)
Name	Primary	String	
familyName	Primary	String	
placeOfBirth	Primary	String	Identification code of the city or the foreign nation (Agenzia delle Entrate)

Name	Attribute type	Format	Notes
countyOfBirth	Primary	String	Identification code of the county [4] (2 letters)
dateOfBirth	Primary	Date	
Gender	Primary	String	"M", "F"
companyName	Primary	String	
registeredOffice	Primary	String	The legal residence of enterprise, represented as a concatenation of the following sub-strings: • Street type • Address • Civic number • Zip code • City • Province
fiscalNumber	Primary	String	ETSI EN 319 412-1 specification for CF attribute: "TINIT-CF"
ivaCode	Primary	String	ETSI EN 319 412-1 specification for PartitaIVA attribute: "VATIT-PartitaIVA"
idCard	Primary	String	Concatenation of the following sub-strings: • Type of document • Number of document • Issuer • Issuing date • Expiration date
mobilePhone	Secondary	String	
email	Secondary	String	
Address	Secondary	String	The citizen's residence, represented as a concatenation of the following sub-strings: • Street type • Address • Civic number • Zip code • City • County
expirationDate	Secondary	Date	Expiration date of e-ID
digitalAddress	Secondary	String	Italian certified e-mail system, also known as *Posta Elettronica Certificata* (PEC)

Table 4: Definitions of SPID qualified attributes

[4] County, or province (*"Provincia"* in Italian) is an area that contains several towns of the same administrative unit.

SPID attributes are defined by simple types, such as string or date elements. Complex attributes are defined as sequences of strings concatenated with the addition of single spaces between parts. Instead, eIDAS complex attributes are described by XML structures, which are encoded in Base64 strings before being added to assertions. Present mapping among attributes is defined below (limited to the natural person set)

eIDAS attribute	SPID attribute	Notes
PersonIdentifier	spidCode	Derived
FirstName	name	May change if the user modifies his/her name
FamilyName	familyName	
DateOfBirth	dateOfBirth	
BirthName	name	
PlaceOfBirth	placeOfBirth	
CurrentAddress	address	
Gender	gender	In eIDAS, `"Male"`, `"Female"`, `"NotSpecified"`. In SPID, `"M"`, `"F"`
	fiscalNumber	SPID-SP is interested in the Italian fiscal number of the user, which is not compatible with the tax reference adopted in a foreign state.
	countyOfBirth	
	idCard	
	mobilePhone	
	Email	
	expirationDate	
	digitalAddress	

Table 5: Present mapping among SPID and eIDAS attributes

At the architectural level, the connection between the Italian national eID schema and SPID has been done, inside the FICEP project, developing two “proxy” components, acting as translator between the eIDAS and SPID SAML profiles, as depicted in Fig. 2

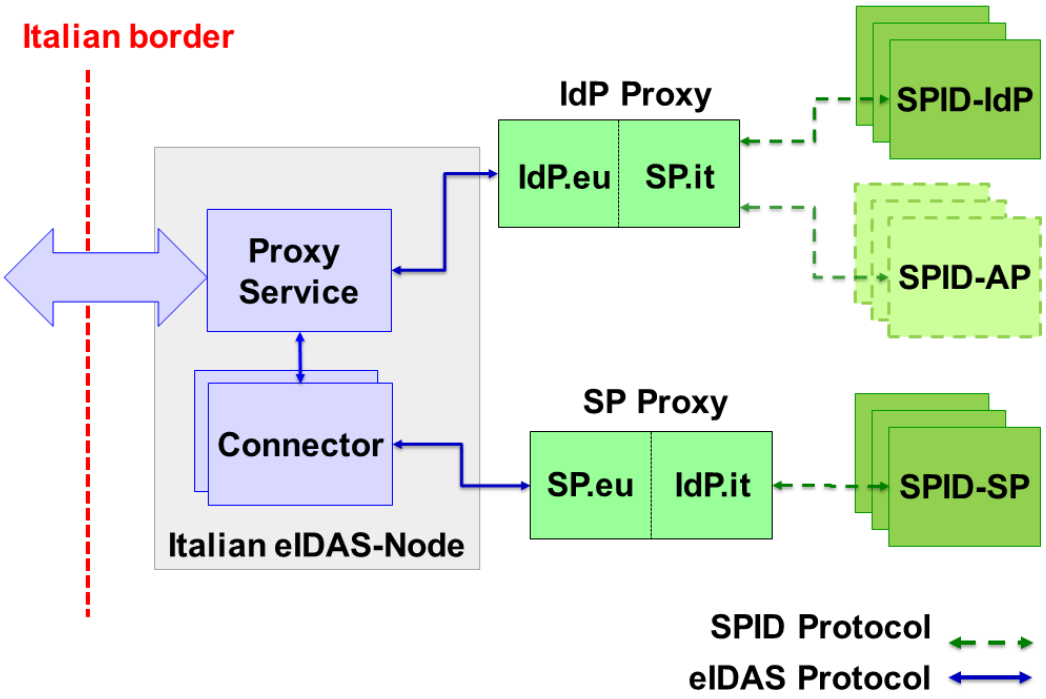

Figure 3 - eIDAS-SPID connecting architecture

According to the Italian translation architecture, an SP-Proxy has been introduced to allow Italian SP to provide access to foreign citizens. From the point of view of a SPID-SP, the SP-Proxy mimics a SPID IdP, while the SP-Proxy internally translated the SPID request in an eIDAS request, thus acting from the point of view of an Italian eIDAS connector like an eIDAS SP.

On the same vein, the IdP Proxy allows italian citizens possessing a valid SPID eID to access a service from a foreign SP. The IdP proxy acts, from the point of view of the eIDAS node (Proxy Service) like an "eIDAS" IdP, and from the point of view of an italian IdP like a SP requesting for citizen authentication.

eIDAS accept two architectural paradigms, proxy-based and middleware. According to that, there can be four combinations considering the two variables type of eIDAS paradigm and local or foreign citizen.

Considering the Italian level, they are described in the following figures.

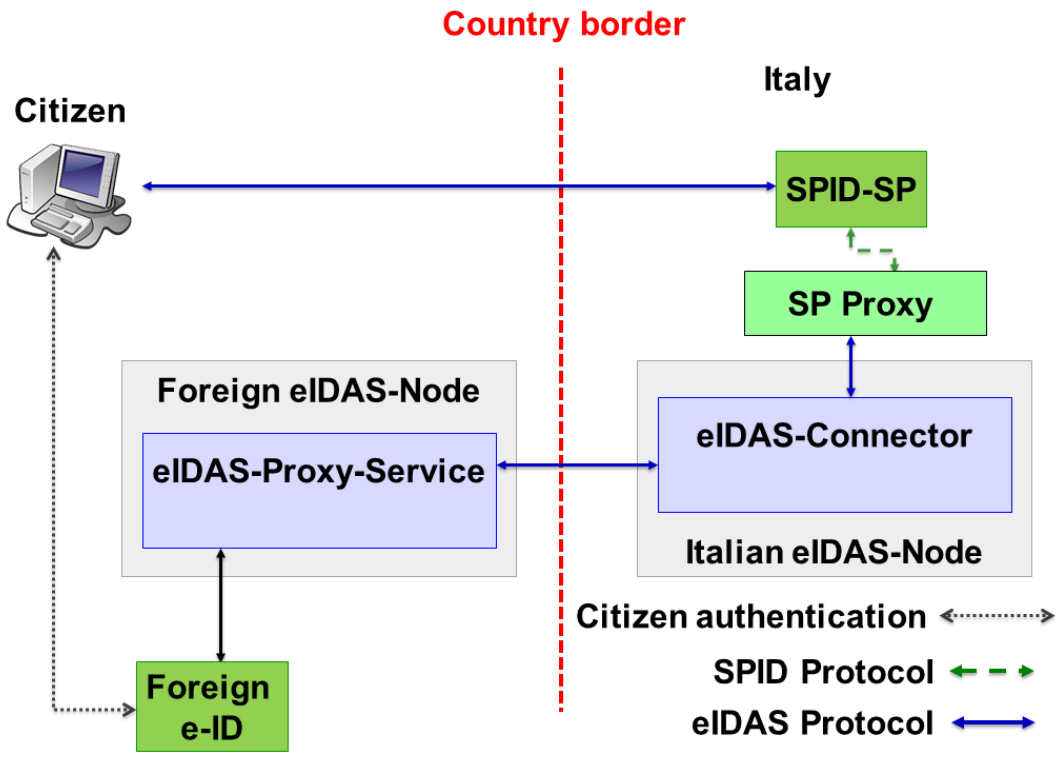

Figure 4 - Italian SP and foreign citizen of an eIDAS proxy-based country

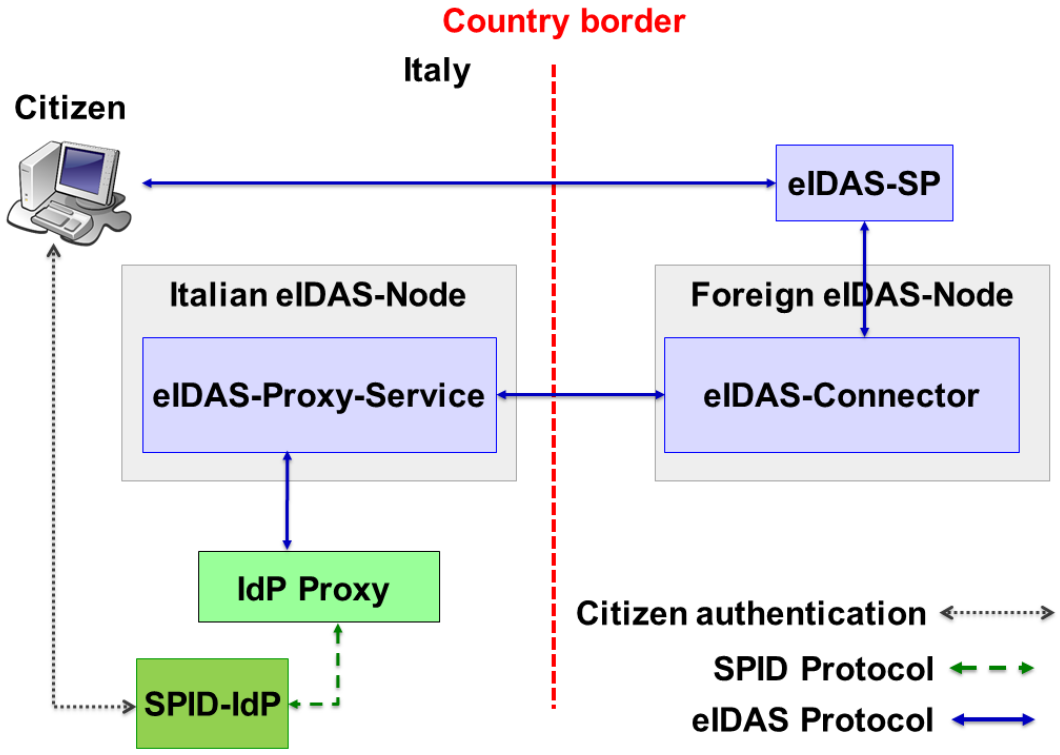

Figure 5 - Italian citizen and foreign SP of an eIDAS proxy-based country

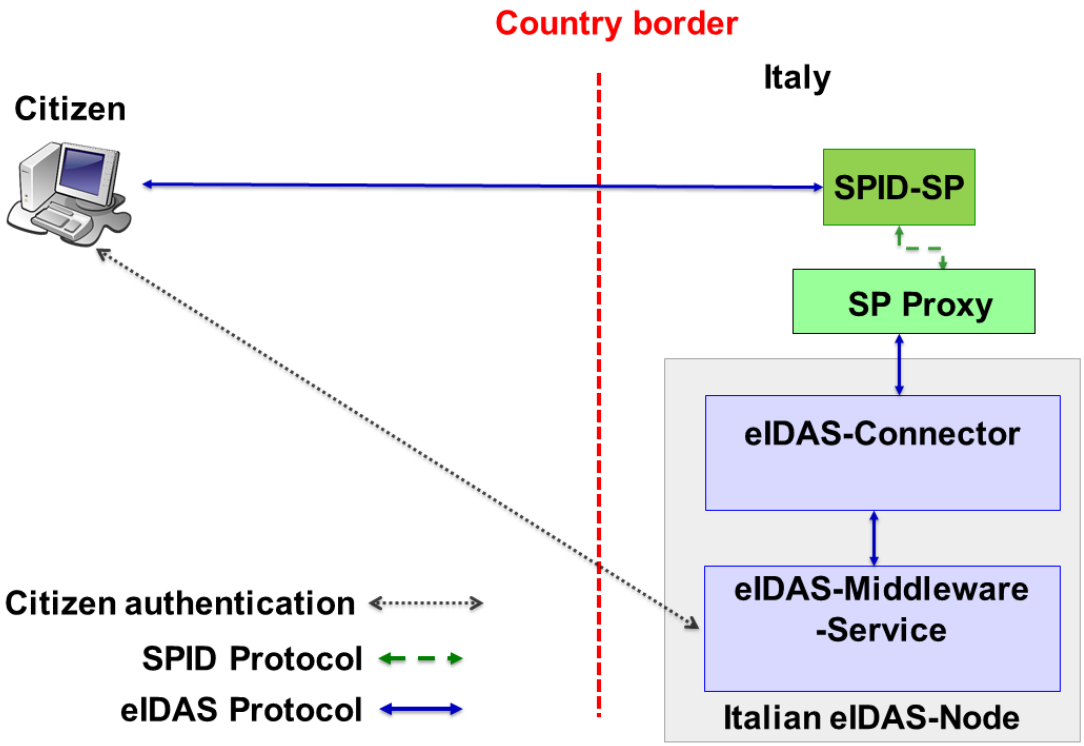

Figure 6 - Italian SP and foreign citizen of an eIDAS middleware-based country

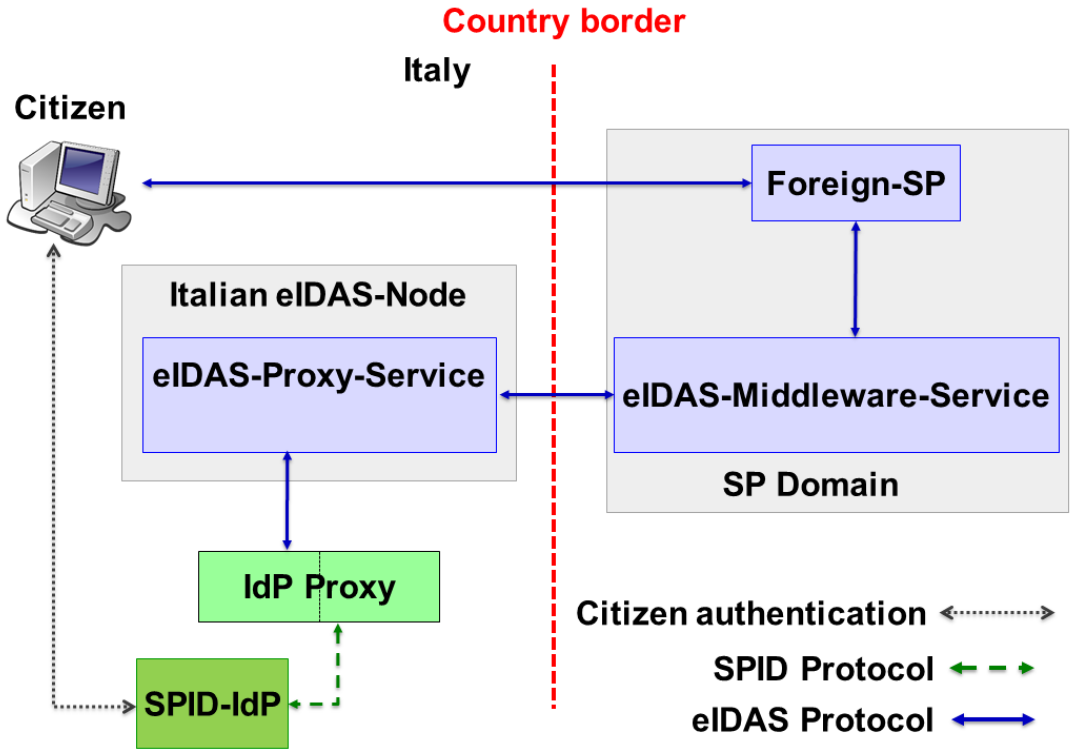

Figure 7 - Italian citizen and foreign SP of an eIDAS middleware-based country

7.2. German eID - the German eIDAS-Middleware

The German eID scheme fulfils all requirements of the eIDAS Level of Assurance 'high'. Due to the nature of the German eID scheme without a central component, the German eID scheme is integrated into the eIDAS Interoperability Framework [eIDAS-IF] via the middleware integration model in accordance with the eIDAS technical specifications [eIDAS-Arch].

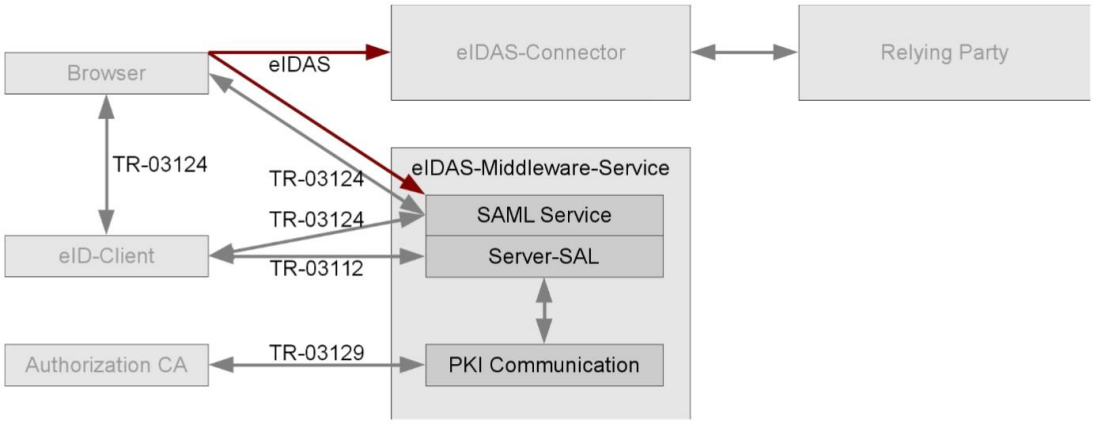

Figure 8 - Integration of the German eIDAS-Middleware into the eIDAS network

Online authentication with the German eID is based on a direct mutual authentication between the relying party and the user. This allows managing authentication without the need for a third party – e.g. (central) ID provider – to perform the authentication procedure. Instead, the authentication procedure is directly performed by the relying party and the German eID. An advantage of this setting is that it avoids the risk of a central security hotspot and/or tracking entity.

National eID Card

The identification means of the German eID scheme is the national eID card issued by the German government. The eID cards contain an eID functionality with a contactless chip that enables secure electronic identification of natural persons based on two-factor authentication. The chip of the German eID card stores the personal data of the holder and serves as security anchor for the protection of this data and the authentication of the holder.

User Environment

The environment of the user (citizen) consists of a computer (e.g. desktop PC, notebook, tablet, smartphone,...) and an eID Client (software). The local eID Client software manages the online authentication process on the client side and serves as the link between the German eID (middleware service), the user and the service provider. As such, it can display information about the service provider, may provide options to deselect access rights, enables PIN entry, and ensures the binding between the web session with the service provider and online authentication session with the service provider's eID server. The eID Client software is based on open specifications that can be

implemented by different vendors. Using certified eID Client software is recommended. One certified implementation – the AusweisApp2[5] – is provided by the German Federal Government.

Middleware Service

Germany provides middleware ('German eIDAS-Middleware') to the other Member States and the European Commission. The German eIDAS-Middleware implements an adapted eID_Server with an eIDAS interface based on Part 3 of Technical Guideline [BSI TR-03130-3], performs the server side of the authentication procedure with the German eID and needs to be operated by the receiving Member State. It also uses German authorisation PKI to ensure the authenticity and to determine the maximum access rights of the service provider. The interfaces according to figure 1, mapping of attributes retrieved from the German eID Card to the eIDAS attributes and further general requirements are described in the technical specification [BSI TR-03130-3] Part 3.

[5] https://play.google.com/store/apps/details?id=com.governikus.ausweisapp2

Attribute Mapping

The attributes retrieved from the eID card are mapped to the eIDAS attributes as follows:

eIDAS attribute	eID card attribute	Mandatory/ Optional	Notes
`FirstName`	`GivenNames`	M	String as retrieved from eID card
`FamilyName`	`FamilyNames`	M	String as retrieved from eID card
`DateOfBirth`	`DateOfBirth`	M	The date retrieved from the eID card is converted to the format YYYY-MM-DD.
`PersonIdentifier`	RestrictedID	M	The `PersonIdentifier` is a strict constructed as `DE/xx/yyyy`, where `xx` is two-letter country code of the destination country or international organization and `yyyy` is the return value of the RestrictedID function encoded as `hexBinary`.
`PlaceOfBirth`	`PlaceOfBirth`	O	If the `PlaceOfBirth` stored on the eID card is encoded as `structuredPlace`, only the component `city` is used. If the `PlaceOfBirth` is encoded as `freetextPlace`, the string is used as retrieved from the eID card.
`BirthName`	`GivenNames`, `BirtName` or `FamilyNames`	O	If `BirthName` is empty (implying that the current last name is the same as the name at birth), the concatenation of the contents of `GivenNames` (first names) and `FamilyNames` (last name) is returned. If `BirthName` is non-empty, the concatenation of the contents of `GivenNames` (first names) and `BirthName` (last name at birth) is returned.
`CurrentAddress`	`PlaceOfResidence`	O	If the data group contains a `structuredPlace`, the `currentAddress` is constructed as follows: • `AdminunitFirstline` is set to the content of

eIDAS attribute	eID card attribute	Mandatory/ Optional	Notes
			the element `country`; • `AdminunitSecondline` is set to the content of the element `state`, if present; • `PostName` is set to the content of the element `city`; • `PostCode` is set to the content of the element `zipCode`; • `ThouroughFare` is set to the content of element `street` up to the first numerical digit, removing trailing whitespace • `LocatorDesignator` is set to the remainder of the element `street`. If the data group contains the `noPlaceInfo` alternative, an empty address is returned.
`Gender`	N/A	Optional	The eIDAS attribute `Gender` is not supported.

Table 6: Attributes mappring (eID card – eIDAS)

Message Flow

This section specifies the establishment of a connection between eID-Client and German Middleware Service, including binding to a preexisting connection between web browser and Service Provider, for performing Online-Authentication based on Extended Access Control Version 2. The following sequence diagram represents the message flow of the authentification of German citizens.

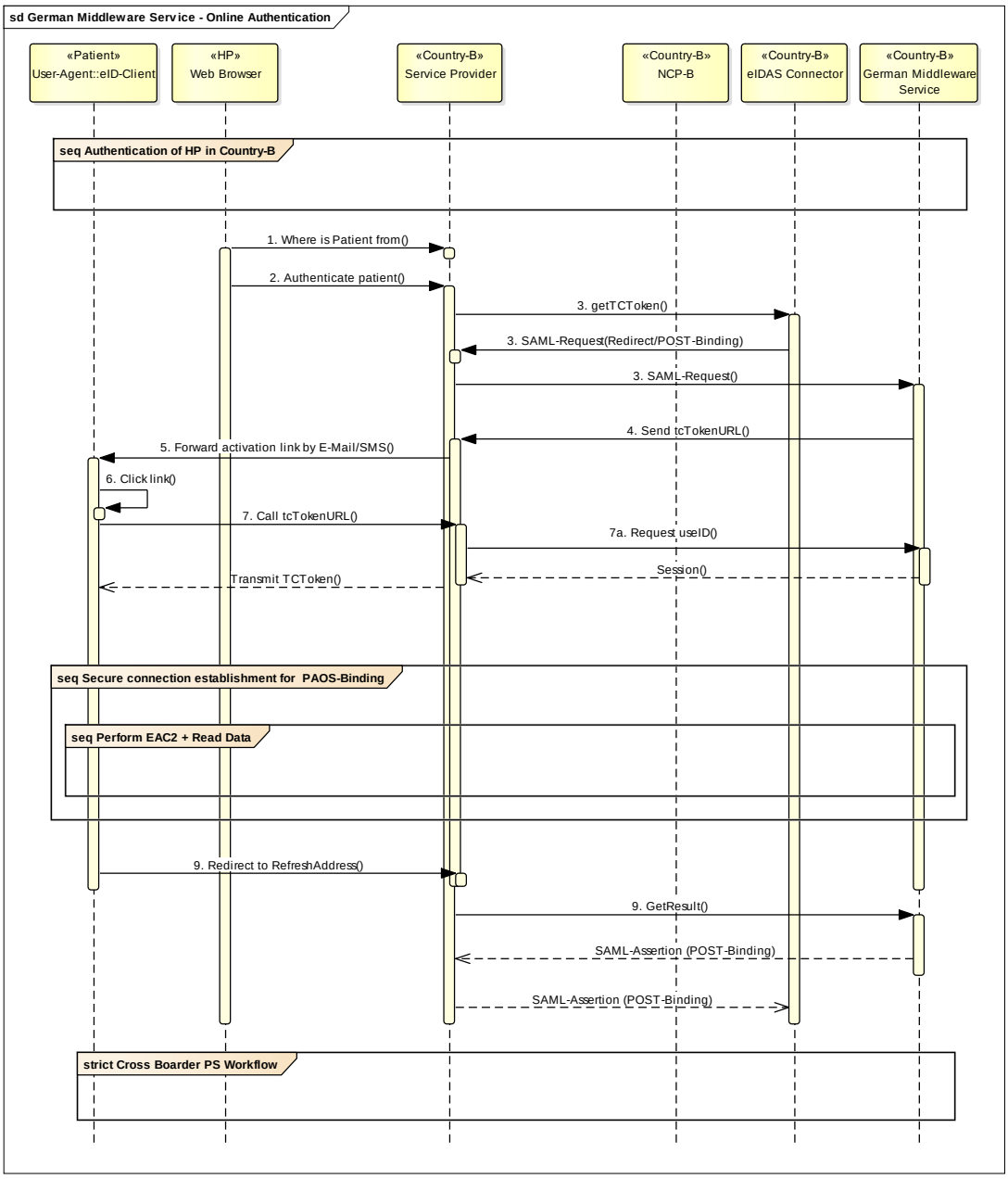

Figure 9 - Message flow of the authentification of German citizens

1. **Where is Patient from:**

   The HP accesses the Service Provider (Portal of OpenNCP) via the web browser and chooses to use eIDAS authentication of patients. An option for selecting the country of affiliation of the patient is provided by the Service Provider to the HP. The HP has entered the information about the Patient's E-Mail address or mobile number.

2. **Authenticate patient:**

   The HP initiates the process of patient authentication.

3. **getTCToken:**

   The eIDAS Connector calls the german Middleware Service with a SAML-Request as specified in [eIDAS-Message]. The SAML-Request is send using Redirect or POST-Binding, i.e. transported via the web browser of the HP to the Middleware Service.

4. **Send tcTokenURL:**

   The Middleware Service responds with a tcTokelURL.

5. **Forward activation link by E-Mail/SMS**

   The Service Provider prepares a link to the eID-Client including the tcTokenURL according to the format `eID-ClientURL/?tcTokenURL=URL`, where `eID-ClientURL` is defined as `eid://127.0.0.1:24727/eID-Client` for mobile operating systems. The Service Provider sends the link via E-Mail/SMS to the patient's smartphone.

6. **Click link:**

   The patient actively decides to use the eID-Function for authentication by clicking on the activation link and thus forwarding the tcTokenURL on his smartphone to the eID-Client (AusweisApp2[6]).

7. **Call tcTokenURL:**

   The eID-Client calls the tcTokenURL of the Service Provider. The TC Token is used to convey the necessary information for setting up a Trusted Channel between eID-Client and Middleware Service. Furthermore, the retrieval of the TC Token and the setting up of the Trusted Channel is part of the session binding mechanism. The TC Token must be provided by the Service Provider at the Token URL given in the embedded link.

   a. **Request useID:**
      The Service Provider calls the function `useID` (see [BSI TR-03130-1] Section 3.2.1.1: Request) at the eID-Interface of Middleware Service to request a valid session. The Middleware Service responds to the call of the function useID and opens a new session if the request was legitimate.

   The Service Provider answers the former request of the eID-Client by sending the TC Token including the necessary connection parameters for the eID-Client in accordance to [TR-03124-01] Part 1, Sections 2.4 and 2.5.1).

8. **Secure connection establishment for PAOS-Binding:**

   The eID-Client establishes a secure channel to the Middleware Service .

   b. **Perform EAC2 + Read Data**
      Online-Authentication is performed using the Extended Access Control protocol. As part of the authentication, the Middleware Service performs Passive Authentication and Revocation Check of the authenticated eID-Card.

[6] https://www.ausweisapp.bund.de/en/ausweisapp2-home/

9. **Redirect to RefreshAddress:**

   After authentication is concluded, the eID-Client redirects the Service Provider to the `RefreshAddress` contained in the TC Token, which points back to the Middleware Service. The Middleware Service responds with a signed and encrypted SAML-Assertion containing the result of the Online-Authentication in POST-Binding, which is sent via the browser to the eIDAS Connector.

7.3. Portuguese eID – Autenticacao.gov, from AMA (Agência para a Modernização Administrativa)

In Portugal, Autenticacao.gov is a public authentication platform, composed by a set of different authentication options, including mobile, citizen card, justice card, and others, used to authenticate a citizen both in public and in private services. New authentication options are under development, via SIBS (Sociedade Interbancária de Serviços), and via eIDAS, for cross-border authentication.

Name	Attribute type	Format	Notes
DateOfBirth	Primary	Date	Mandatory
PersonIdentifier	Primary	String	Portuguese citizen card number. Mandatory
FamilyName	Primary	String	Mandatory
FirstName	Primary	String	Mandatory
CurrentAddress	Primary	String	
Gender	Primary	String	"M", "F"
PlaceOfBirth	Primary	String	

7.4. Greek eID – ermis.gov.gr, from HMAR (Hellenic Ministry of Administrative Reconstruction)

In Greece, up to now there is no notified identification scheme. However, Greece recognizes identified schemes of other Member States.

Currently, ERMIS is connected as IDP with the preproduction eIDAS node, for testing purposes. Additionally, ERMIS is acting as Greece- internal IDP for several (Greek) SPs, connected to the Greek production eIDAS node, IDIKA is one of them.

The eIDAS connector supports the eIDAS SAML protocol and the attributes supported by the Greek eIDAS node are the following:

Name	Attribute type	Format	Notes
DateOfBirth	Primary	Date	Mandatory
PersonIdentifier	Primary	String	Greek citizen card number. Mandatory
FamilyName	Primary	String	Mandatory
FirstName	Primary	String	Mandatory
Gender	Primary	String	"M", "F"

8. Member specific NCPeH adaptation

As with happens with the eIDAS schemes, countries may also have their own specificities at NCPeH level. In this section, we identify the diversity of such specificities. We details in the following just the differences, the other participants stated they did not introduce modification in the OpenNCP structure at national level.

8.1. Portuguese OpenNCP adaptation

Portugal's NCPeH internal architecture doesn't differ that much from the OpenNCP default one presented in section 4, as it reuses most of the default components and configurations. Nevertheless, it developed some extra national components and applied some national configurations to default components, depicted in the following diagram:

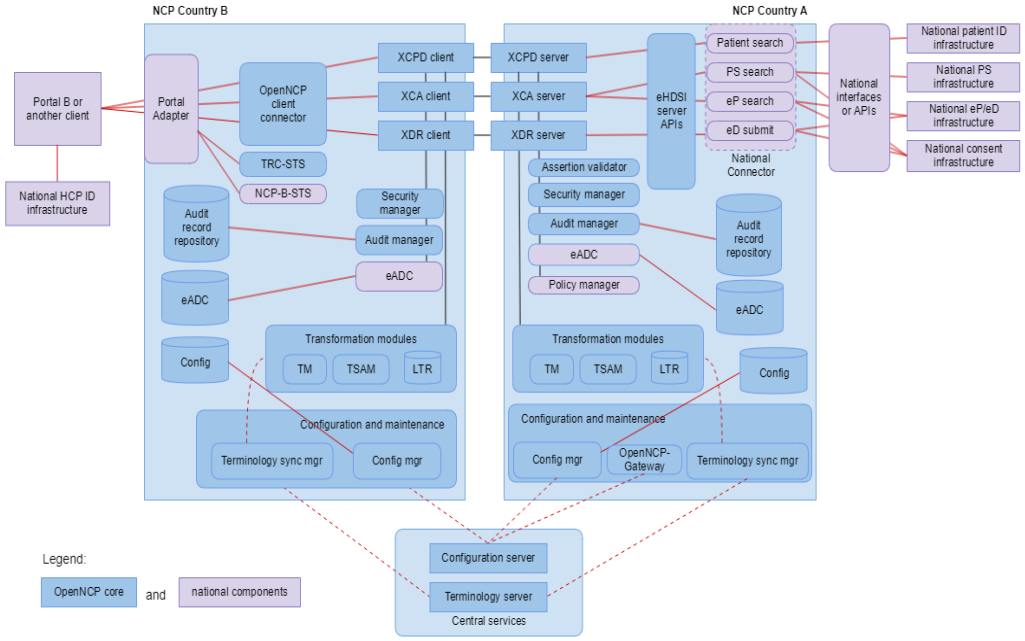

Figure 10 - Portuguese OpenNCP adaptation

Following is a brief description of the Portuguese extras (identified in purple in the picture):

Component	NCPeH-A/B	Description
Portal Adapter	NCPeH-B	HL7 FHIR-based adapter that mediates and orchestrates the communication between the OpenNCP client connector, the STSs and the national infrastructure in country-B (other middlewares).
NCP-B-STS	NCPeH-B	Secure Token Service that issues an NCPeH-B-signed HP Identity Assertion based on claims provided by the HP identity provider of country-B

Component	NCPeH-A/B	Description
eADC	NCPeH-A/B	This default component can have some national configuration of the statistical data collected. Currently it's using the configuration suggested by eHDSI Solution Provider, in accordance with the eHDSI KPI reporting needs.
Policy Manager	NCPeH-A	National implementation of the policy manager that defines the access control policies following country-A national requirements.
National Connector	NCPeH-A	National implementation of the connector to the national infrastructure of country-A, based on HL7 FHIR. It absorbs the features of the default Consent manager by integrating the consent validation step in the other main steps of the cross-border eHealth workflows.

Table 7: Portuguese extras description

When it comes to the identity traits used to uniquely identify a patient in the Portuguese national infrastructure, Portugal has defined that the national health system identifier (a 9-digit number printed in the citizen's card) is the one to be used by health professionals during cross-border encounters.

9. HEALTHeID architecture

The key issue to solve is how to interconnect coherently the eIDAS authentication and the eHealth services provided through the NCPeH infrastructure. The link between the two worlds is the patient identifier: the cross-border exchange of information in the eHealth domain requires the existence of patient identifiers to select the correct information from health information systems. Some Member States use their national citizen ID as patient ID in the context (e.g. the Italian notified eID contains an attribute, the Fiscal Code - "Codice Fiscale"- suitable to be used as Patient Identifier), while some others use a sector-specific patient ID.

The case can be even more subtle, since the patient ID, even if available at national level, may not be part of the data set retrieved after an eIDAS authentication exchange, due to the specific eID notified schema peculiarities (there may be many notified schemes per nation, and not all of them might have an attribute suitable as patient ID) and to the national rules on the matter (the Italian eIDAS node do not transmit the fiscal code in the response at the moment, even if at national level it is an issue under discussion).

The present NCPeH scenario foreseen an encounter between an HP and a patient, the authentication of the Patient through the HP, and the provision of the patient ID from the patient itself (as well as other relevant data to query the NCPeH infrastructure for patient data). As such, the patient ID is prone to errors and the authentication strength not always clear.

Thus, to provide a flexible solution suitable for all cases, the HEALTHeID connector must be able to differentiate on a national bases if any attribute is suitable for the purpose, in case yes, which one(s), in case not require it as an input from the patient, coherently to the present cross-border eHealth scenarios.

Since this procedure can be prone to error, it is necessary a verification step where the patient ID is sent to the country A national eHealth infrastructure, and then verified versus local databases.

The patient according to privacy concerns detailed in activity 1 deliverables, has the right to give his/her consent in for the specific eHealth treatment, and this consent has to be properly managed by the HEALTHeID connector.

In the following, the joint architecture to provide these functionalities is described. In particular, the figure 7, presents an high level overview of the resulting merged architecture, detailing only the very specific parts in scope of HEALTHeID project, while in the following sections the interfaces between them, and finally the overall message flow is depicted.[7]

[7] This section is the basis for the current components development of the HEALTHeID Project. Even if stable, the document is meant to be open to adapt to fundings during the scope of the Project, e.g. the on-going discussion on "Patient Consent" and Patient Information Notice may be reflected in the sequence diagram, namely in the Patient Consent related exchanges.

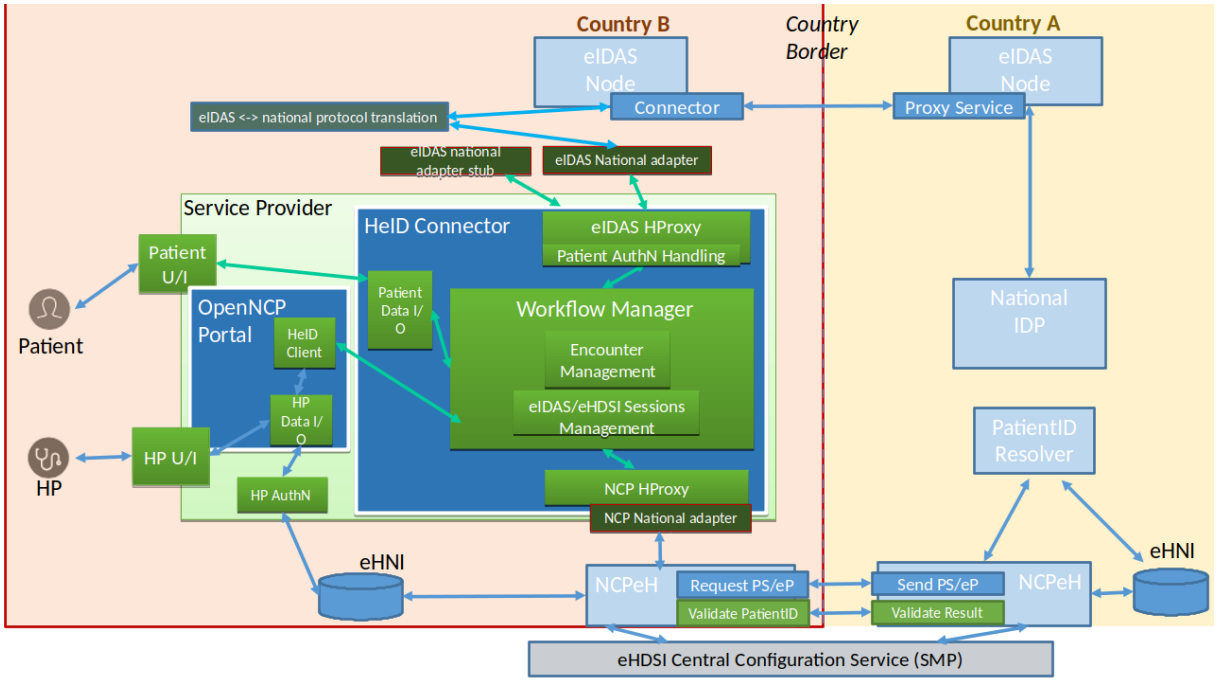

Figure 11 - HEALTHeID architecture high level view

The Service Provider in the picture is the components where the HEALTHeID connector (HeID Connector) will reside and act like the eIDAS SP toward eIDAS infrastructure and like OpenNCP Portal towards the eHDSI infrastructure. The Patient Data I/O is the web front-end to allow Patients to access the HeID Connector functionalities. The Workflow Manager is triggered by the Patient to initiate the eIDAS authentication, that will be performed by the eIDAS HProxy component, and manages the eIDAS response and the interactions with the NCP worlds, through the NCP HProxy. Since both NCP and eIDAS sides might have National specific peculiarities, a specifica National adaptor might be required to adapt to country-specific scenarios.

This architecture presents an overview of the whole involved Service Providers components, but only some of them are in scope in the development of the HEALTHeID connector.

The components inside the HeID Connector blue square are the specific ones, the other (inside or outside the service provider) are component mostly already existing or depending on the national specific scenario.

In particular, out of scope are:

- Authentication Handling of the HealthCare Professional, somehow performed according to local eH National specific scenario (through a local IdP)
- Creation of the encounter with the Patient, since, as in the previous point, it depends on the national specific installation
- Expiry, by policy, of the HP session (this is again subject to the national specific rules and scenarios)

However, inside the project is forseen the development of a prototype version and/or modification of some of the other blocks and functionalities out of scope, with the purpose of allow the testing of the HealtheID workflow.

On the contrary, in scope are the following functionalities:

- The Patient Authentication Handling, done through eIDAS infrastructure. In this regard, the Workflow Manager is in charge to start the authentication signalling to Patient I/O module to send an anchor to the Patient (e.g. QR code, SMS, email) in order to start the eIDAS authentication. The eIDAS authentication is started by the eIDAS HProxy components, which is able to get back the final result, after the eIDAS flow in place between the patient and the SP country, and communicate it to the workflow manager
- The Encounter Management, in particular the workflow manager, which is 1) able to manage the Patient Authentication result and data; 2) able to propagate it to the eHDSI flow; 3) able to ask to the Patient further data not present in the data set provided by the eIDAS authentication (e.g. Patient Identifier in some countries, which has to be verified through NCPeH of the Patient origin country) and the Patient Consent to the treatment. In this sense, the workflow manager acts as an orchestrator of the HeID Connector business and coordinates the chain of operations calls.
- The validation and verification of the Patient Identifier at Country A level, which is performed according to the National eH infrastructure peculiarities and that is national specific.

9.1. Interfaces

This section defines what interfaces are in or out of scope in the light of HEALTHeID, and what protocol is involved where relevant for the development. Since many details (and in some cases, also the involved protocols) may differ on the base of the national specific scenario, this document outline particularly the interface meaning, while different documents (e.g. related to eIDAS and NCP specification or to integrate the components developed in this project) are suitable to complement these description with low-level details.

Interface between eIDAS Connector and eIDAS Proxy Service

This interface is up to the eIDAS technical specification and out of scope of this document.

Interface between eIDAS Connector and eIDAS <> eIDAS National translation component

This interface is subject to national specification: some countries (e.g. Italy) adopt at local level a different Protocol and/or attribute set for the implementation of digital identity, some other countries reuse at the national level the eIDAS protocol, so no eIDAS translation is required at local level is required. Where a translation is required, the countries run or are running a specific project

to detail the involved protocols and profile, as well as to develop the related implementation[8]. Thus, the management of these specificities is out of scope of this project.

Interface of the eIDAS HProxy component

In order to provide a common interface, re-use as much technical specification available and not loose any information where possible, the eIDAS HProxy component adopt the eIDAS SAML profile for input/output communication.

Interface between eIDAS <>National translation component and eIDAS National adaptor

Since the eIDAS HProxy component expects eIDAS SAML profile, countries adopting a different local protocol have the responsibility to develop a National Adaptor to translate from national protocol to the eIDAS profile. This should have a minimum impact on the development side, since a translator component in such a country should be already available and possibly mostly re-usable for this task.

Interface between the HeID Client and the Workflow Manager

The Workflow Manager exposes a REST end-point to allow the HeID client, as the component inside the OpenNCP Portal to communicate with the HeID Connector, to trigger the eIDAS based access to eHEALTH services. To this goal, it is needed the communication is secured by a confidential and authenticated connection (e.g. through https).

Interface between the NCP Hproxy and NCPeH

This interface re-use the national specific implementation (e.g. SOAP-based) already developed, and thus under country-specific responsibility. Task of this project is to provide a stub for the NCP Hproxy component to allow each member state to build up the component merging their national specific peculiarities

The communication between the NCP HProxy and the NCPeH-B is mediated by the National Adaptor, which can act in two ways:

1) By directly calling the services exposed by the NCPeH-B. MS would provide an implementation where they would map the HeID message data to the data format of the services exposed by NCPeH-B. This replicates the way the current OpenNCP Portal calls the NCPeH-B, through the OpenNCP Client Connector Consumer module;
2) By mapping the HeID message data to a national specific format. This is needed whenever the NCPeH-B services exposed to country-B national infrastructure are not the OpenNCP Client Connector Consumer ones, but national specific ones. This is the case, e.g., of Portugal, where the NCPeH-B exposes HL7 FHIR services towards the national infrastructure. In this example,

[8] in Italy, which adopts SPID as National specification, FICEP project developed the nodes and related translation, and, in particular, developed a component named SP Proxy between SPID SP and eIDAS connector to translated eIDAS<>SPID profile

the National Adaptor would map the HeID message format to HL7 FHIR messages expected by the Portuguese HL7 FHIR-based Portal Adapter (which in turn calls the OpenNCP Client Connector Consumer).

In the end, the National Adaptor implementation choice would be a MS responsibility, but in both cases it is envisaged to be easily plugged into the NCP HProxy interfaces (e.g., following a similar approach to that of the NCPeH-A National Connector). The HeID project will provide an implementation of the first scenario.

Interface between the NCPeH A and NCPeH B

It is not changed in respect to OpenNCP specification, and out of the scope of this project

Interface between the NCPeH A/B and eHDSI Central Configuration Services

The current interface between the NCPeH-A/B and the eHDSI Central Configuration Services is not changed. Actually, we foresee that a new SMP file type will be available for publication by NCPeH-A and consumption by NCPeH-B. This new file is needed for any MS to publish their answer to the following question: “Does my eIDAS MDS contain an identifier suitable to be used as the patient ID?”. This information is then used later in the process to decide whether additional means (to those of an eIDAS authentication) for the provision of the patient ID are needed or not.

As such, profiling of this new SMP file is needed for future inclusion into the [eHDSI-SMP]. The following paragraphs describe such profiling, in accordance with the way it is done in [eHDSI-SMP] for the other SMP files.

Since this “eIDAS-eHealth Configuration” is not defined in [eHDSI-Audit], the following document identifier suffix shall apply:

- ehealth-108

Resulting in the complete document identifier: urn:ehealth:eidas::eIDASeHealthConfig##ehealth-108

Process	Opt	Usage Convention
ProcessIdentifier	R	MUST contain "urn:ehealth:ncp:<country>:eidas-ehealth"
ProcessIdentifier/@Scheme	R	MUST be ehealth-procid-qns
ServiceEndpointList	R	
Endpoint/@transportProfile	R	MUST be "urn:ehealth:transport:none"
EndpointURI	X	
RequireBusinessLevelSignature	X	
ServiceActivationDate	R	MUST contains the Date when the eIDAS-eHealth configuration has been issued
ServiceExpirationDate	O	MUST contains the Date when the service will be stopped

Process			Opt	Usage Convention
		Certificate	X	
		ServiceDescription	O	MAY contain the english description of the eIDAS-eHealth configuration
		TechnicalContactURL	O	MAY contain the information related to the technical contact
		TechnicalInformationURL	O	MAY contain the URL pointer to the remote eIDAS-eHealth technical description
	Extension		R	MUST contain the eIDAS-eHealth Configuration XML as direct children

The eIDAS-eHealth Configuration XML file could be described by the following XSD:

```
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns="http://ec.europa.eu/sante/ehncp/eidas"

        targetNamespace="http://ec.europa.eu/sante/ehncp/eidas"
xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="EidasEhealthConfiguration">

    <xs:complexType>

      <xs:sequence>

        <xs:element type="patientInput" name="patientInput"/>

      </xs:sequence>

    </xs:complexType>

  </xs:element>

  <xs:complexType name="patientInput">

    <xs:sequence>

      <xs:element name="patientInputNeeded" type="xs:boolean" />

      <xs:element name="patientIdMappableEidasAttribute" type="xs:string" />

      <xs:element name="patientIdMappableEidasAttributeOid" type="xs:string"
/>

    </xs:sequence>

  </xs:complexType>

</xs:schema>
```

The schema structure is very simple and contains 3 elements:

- patientInputNeeded: answers to the question "Do we need our patients to input their patientID (and other data)?";
- patientIdMappableEidasAttribute: Friendly name of the eIDAS attribute from which we can derive or map to the patientID;
- patientIdMappableEidasAttributeOid: OID of the beforementioned attribute.

Gazelle test assertions needed for scrutiny of this new SMP file (as part of the eHDSI Test Framework test plan) will be provided together with the final artifacts of the project.

The interfaces between different components of the service provider are based on KISS principle (e.g. JSON structure), and adaptable on the base of national specific cases.

9.2. Message Flow

Message Flow – presence of a "personal device", SMS/link-enhanced, cosidering the possibility Patient ID may not be amongst the disclosed attributes

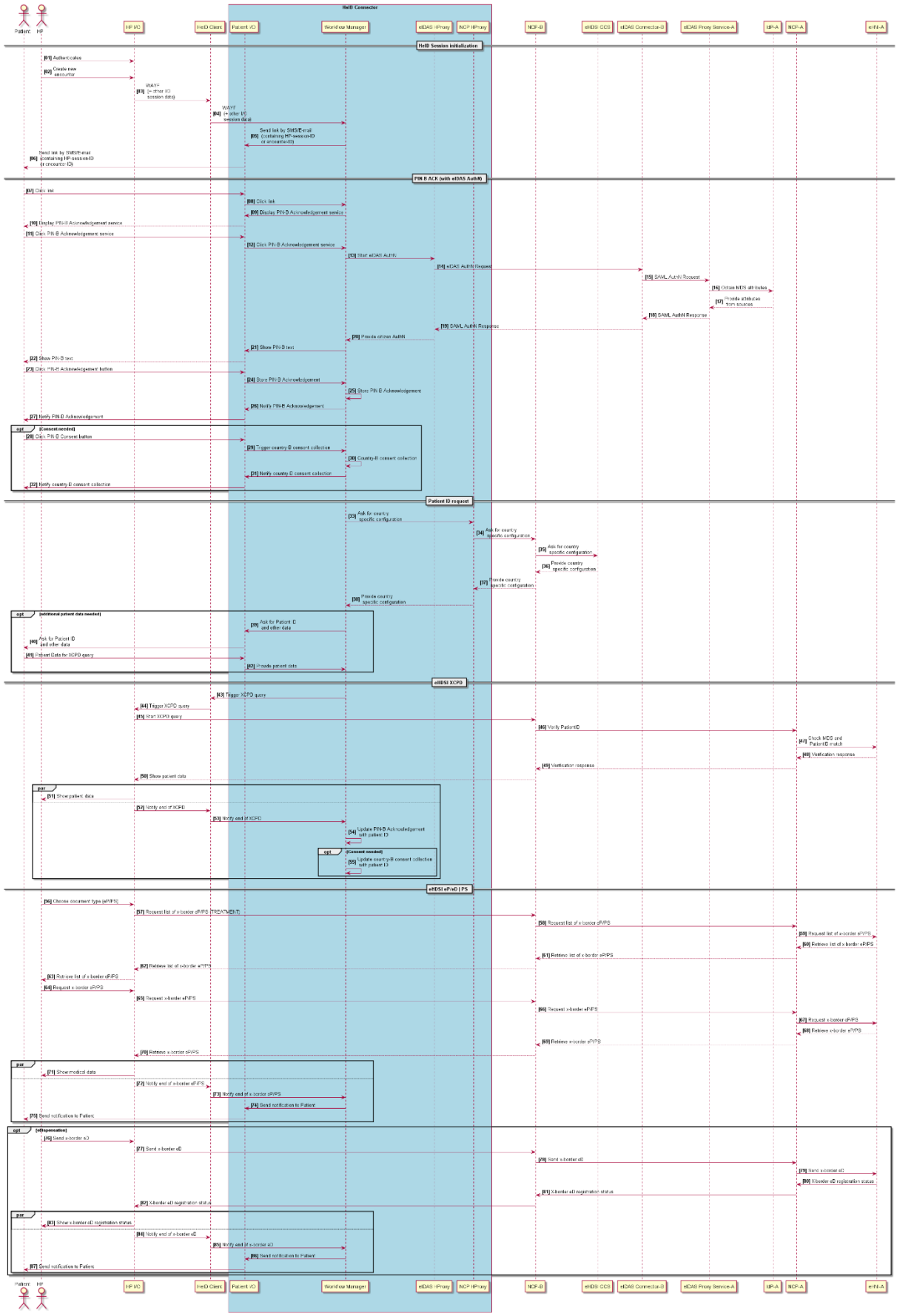
HeID Connector
Patient
HP
HP I/O
HeID Client
Patient I/O
Workflow Manager
eIDAS i-Proxy
NCP i-Proxy
NCP-B
eHDSI CCS
eIDAS Connector-B
eIDAS Proxy Service-A
I&P-A
NCP-A
e-INF-A
HeID Session initialization
PIN B ACK (with eIDAS AuthN)
Patient ID request
eHDSI XCPD
eHDSI eP/eD | PS
opt
par

Figure 12 – Message Flow

Assumptions:

a) Patient owns internet enabled personal device, able to receive SMS (or configured to receive email)
b) HP and Patient authentication process is successful
c) Patient is not a minor and is willing/able to provide consent
d) Patient ID is known by the Patient
e) Country A is able to verify that Patient ID and eIDAS minimum data set match
f) The table reports all the operation for a successful encounter (note, the first step – the HP authentication- relates to a different, country specific, scenario, so it is Out of Scope –OoS– from this deliverable)

Operation	**Description**
1	*HP opens the SP from a personal device (i.e. a notebook) and authenticates herself/himself using a specific, domestic Identity Provider – OoS*
2	HP creates a new encounter and provides the SP with mobile/e-mail of Patient (to be used in steps 3 and 28)
3-4	The HP I/O component sends session data (like HP-session-id) and other information, like the Country of Treatment, to the HeID Client, which acts as interface to the HeID Connector (in particular to the Workflow Manager)
5-6	The HeID Connector sends SMS/email to the Patient that contains the HP-session-Id and other information, like where to start the authentication
7-8	Patient clicks the link, invokes the SP, relays HP-session-ID (or Encounter-ID) as parameter and initiates Patient Authentication process from the user perspective
9-12	The Workflow Manager triggers the Patient Information Notice service to display it to the patient and get patient feedback
13-20	Patient is requested to provide to the IdP his/her credentials and eIDAS authentication is performed using his/her device
21-22	The Workflow Manager triggers the PIN-B text to the user
23-32	The PIN-B acknowledgement or the Patient Consent is collected by the Workflow Manager and the user is notified by that.
33-38	The workflow manager triggers the process to contact the central configuration service for specific country information (e.g. Patient ID available among the eIDAS data)
39-42	In case of need, the identified individual is prompted to provide own patient identifier and relevant data for the xCPD queries
43-50	The country A is responsible for the verification of the individual's patient identifier. This verification is triggered by the Workflow Manager, and performed by the HeID client, which acts

Operation	Description
	as the current OpenNCP Portal, respecting the principle of minimal modification (disruption) of components.
51-55	HP professional can see the verified patient data and the workflow manager is notified of the result of the xCPD query. Thus, the Workflow Manager can update the PIN-B (and consent if relevant according to the specific MS policy).
56-87	HP decides to access to Patient's medical data. The process now proceeds involving the steps of the Patient Summary and ePrescription use cases. Only addition to the normal flow, is the notification to the Pationt, through the Workflow Manager, of the x-border exchange (respectively steps from 72 to 75 and steps 84 to 87)

Table 8: Description of operations for a successful encounter

10. Security considerations

Security is critical for a Cross-Border eHealth Infrastructure (CBeHIF) to be used in an operational environment. According to [NCPeH-guide] an appropriate security policy aims to create a secure operational environment for the service deployment and for protecting the CBeHIS data and processes,. Furthermore, such security policy should be implementable and agreed by all MS.

A CBeHIS Security Policy is mandatory and is baseline versus auditing for all cross-border actors, specifying also the requirements of service providers and users.

Unavoidable principles are, according to [NCPeH-guida] that

- All CBeHIS data and processes must be adequately protected
- The network built among the CBeHIS MS should also not add any unacceptable new risk within any participating organisation.
- Appropriate technologies and procedures must be used to ensure that data is stored, processed and transmitted securely over the network built among the CBeHIS actors and is only disclosed to authorised parties.

The prominent addition in respect to the present CBeHIF is the eIDAs infrastructure.

The eIDAS-Network stakeholders expect the platform to provide secure authentication and certification of user attributes, meaning that a chain of trust is needed throughout the complete e-ID transactions.

Regarding the eIDAS eID infrastructure

- trust is created among the proxies by publishing the respective public-keys inside the \saml meta-data of the infrastructure stored in a central repository;
- man-in-the-browser attacks towards data privacy are avoided by requiring end-to-end encryption of all messages transported among the proxies;
- security is maintained at a high level by publishing minimum and suggested cryptographic solutions to be implemented by all proxies;

each national eID schema proposed for cross-border usage (``notified'' according to the eIDAS Regulation) is evaluated by a special body (the EU Cooperation Network) to assign a specific level of assurance based on a common understanding of its technical and procedural security status. This has been developed to provide an appropriate interoperability between different country eID schema, still maintaining an adequate protection level while data are in transit in the eIDAS infrastructure.

The SP, that hosts the HEALTHeID connector requires authenticity and integrity of the received person attributes, in order to assure their validity. It also needs confidentiality of the received identification data to fulfil his data protection legal obligations.

The citizen requires confidentiality too, so as to be sure that his private data aren’t being shared with malicious third parties. He also requires the eIDAS-Node to respect his own privacy, and not to store his data for unwanted use.

So, the following high-level security requirements result shall be adopted by any service that may interact with eIDAS-Network:

- confidentiality of user identification data;
- authenticity and integrity of user attributes;
- authentication and identification of the entities involved in the e-ID transaction.

Also [NCPeH-Guide] characterize Information security as the protection of:

- Confidentiality (information is protected from unauthorised access or unintended disclosure – only authorised users have access to the information and other system resources),
- Integrity (information is protected from unauthorised modification) and
- Availability (resources are available, without unreasonable delay - authorised users are able to access information and the related means when they need it).

and highlights that the CBeHIS Security Policy should ensure them, as well as means of proofs and checks, to establish users' trust in the given service.

The objective of a security policy toward all CBeHIF are manifold make CBeHIS actors sensitive to security risks and security controls to manage them.

To create a common agreed security framework for CBeHIS (and thus to promote cooperation between CBeHIS actors)

To ensure that the information system in place respects national and European legislation on privacy and data protection in force from one side, and that security measures are proportioned to the incumbent risks.