H2020-SC6-GOVERNANCE-2018-2019-2020

DT-GOVERNANCE-05-2018-2019-2020

D4.3 Components adaptation for SDG, OOP, eIDAS for National public services – Final

Project Reference No	959157 — ACROSS — H2020-SC6-GOVERNANCE-2018-2019-2020
Deliverable	D4.3 Components adaptation for SDG, OOP, eIDAS for National public services – Final
Work package	WP4: ACROSS Modules Set-Up
Nature	Other
Dissemination Level	Public
Date	31/7/2023
Status	1.0
Editor(s)	Iosif Kanakaris, Dimitrios Michail, Iraklis Varlamis/GRNET Heinrich Hammerstein, David Britnell/ DATAPORT
Contributor(s)	Ernst Thilo/ FRAUNHOFFER
Reviewer(s)	Vincenzo Savarino (ENG), Ernst Thilo (FHG)
Document Description	This document is the final report for the Task 4.1 of WP4, components adaptation for SDG, Once Only Principle and eIDAS use for authentication and authorization and documents the work undertaken, the interactions with the ACROSS platform and National services and the technologies used.

About

The project is co-funded by the European Commission's Horizon 2020 research and innovation framework programme. Spanning through three years, ACROSS consists of a consortium of 10 partners from 7 countries: Athens Technology Center (coordinator), Tecnalia, Dataport, Engineering, Fraunhofer, GRNET, TimeLex, The Lisbon Council, Waag and VARAM. The project kicked off its activities in February 2021, with an energising online meeting, where all partners took the floor to present their plans to make the project a great success.

DISCLAIMER

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V0.1	22/05/2023	Extension of ToC with the planned feature extension	GRNET
V0.2	25/07/2023	Draft for internal review	GRNET
V0.3	26/07/2023	Internal review	ENG, FHG
V0.4	27/07/2023	Modifications as per suggestions	GRNET, ENG
V1.0	31/7/2023	Final release	GRNET

Executive Summary

The main objective of the ACROSS project is to provide the means (tools, methods and techniques) to enable user-centric design and implementation of interoperable cross-border (digital) public services compliant with the current European regulations (e.g. the Single Digital Gateway (SDG) and Once-Only principle (OOP), European Interoperability Framework (EIF)), also considering the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) in order to ensure that people can use their own national electronic identification schemes (eIDs) to access public services available online in other EU countries and take advantage of trust services that work across borders and have the same legal status as their traditional paper based equivalents while ensuring data ownership and choice of level of information to be disclosed while navigating through their user journey.

This deliverable documents the result of activities undertaken in Work Package 4, Task 4.1 and provides a high-level description and also the code[29] of the technological components to integrate ACROSS Platform with eIDAS nodes of EU member states in which pilots are located (Germany, Greece, Latvia). This includes a third release of the components that is incorporated in the ACROSS application and provide identification against the eIDAS schemes of Germany, Greece and Latvia. As Latvia does not have a technical part in the work package, discussions between the developers from ATC and GRNET and the technical team responsible in Latvia, are ongoing. The Latvian eIDAS node is connected to the ACROSS application too, still, though what remains is to connect the Latvian to the Greek production node (connection with the Greek pre-production node is done). This is an external source of delay as we don't really know when the Greek production node will be available for connection with the Latvian. A different pathway has thus been discussed, where the choice of connection in the ACROSS application to the relevant eIDAS node will be based on their country of origin.

This document begins with an introduction to the main concepts of authentication and authorization as foreseen by the eIDAS regulation for Digital Identity and continues with a review of the current state of eIDAS node in the three countries of the project, Germany, Latvia and Greece.

In addition, this deliverable discusses in more details the requirements of ACROSS applications for authorisation and authentication, as they have been defined in detail in the project, more specifically in WP5 and WP6 and categorized in functional and non-functional ones.

Finally, the current deliverable describes the final design of the eIDAS connector, its architecture and interfaces and examines the different implementation alternatives.

Table of Contents

EXECUTIVE SUMMARY **4**

1. INTRODUCTION **10**

1.1. PURPOSE AND SCOPE 10

1.2. APPROACH FOR WORK PACKAGE AND RELATION TO OTHER WORK PACKAGES AND DELIVERABLES 10

1.3. METHODOLOGY AND STRUCTURE OF THE DELIVERABLE 10

2. THE MAIN CONCEPTS 2.1 DIGITAL IDENTITY AND THE EIDAS REGULATION **12**

2.2. AUTHENTICATION AND AUTHORIZATION 12

3. THE CURRENT STATE OF EIDAS NODES IN THE THREE PILOT COUNTRIES **14**

3.1. GERMANY 14

3.1.1. How does eID authentication work in Germany *15*

Communication relationship during eID authentication 15

German eID authentication flow with all involved actors 16

A) Initiation 17

B) Interaction 17

C) Completion 18

3.1.2. How Germany is integrated into the eIDAS interoperability framework *18*

3.1.3. How to connect ACROSS to the eIDAS infrastructure *19*

3.1.3.1 Overview 19

3.1.3.2 German use case: Middleware to Proxy 20

A) The simple perspective 20

B) The flow with all involved actors 20

Detailed flow description for German use case [20] 21

D) eID authentication in eIDAS member states from a German user perspective 22

3.1.3.3 Single point of contacts 23

3.1.3.4 Integration guide 23

A detailed eIDAS integration guide for Latvia, can be found here: 23

3.2. LATVIA 23

3.2.1. How eIDAS is used in Latvia *23*

3.2.1. How to connect ACROSS to the eIDAS infrastructure *26*

3.3. GREECE 26

4. REQUIREMENTS OF ACROSS APPLICATIONS FOR AUTHORIZATION AND AUTHENTICATION **29**

4.1 INTEROPERABILITY 29
4.2 SECURITY AND PRIVACY 29
4.2.1 Common *29*
4.2.2 Authentication *30*
4.2.3 Authorization *30*
5. IMPLEMENTATION, DESIGN AND ARCHITECTURE **31**
5.1 IDENTITY BROKERING TO EIDAS NODES 32
5.2 EIDAS KEYCLOAK EXTENSION 32
5.3 EIDAS SAML V2.0 IDP CUSTOM SETTINGS 33
5.4 IDP MAPPERS 34
5.5 CUSTOM AUTHENTICATION FLOWS 35
6. WORK DONE AND CURRENT STATUS **37**
7. CONCLUSIONS AND NEXT STEPS **38**
8. ANNEX - ACROSS REQUIREMENTS MAPPING **40**
9. REFERENCES - LINKS **45**

List of Figures

FIGURE 1-A SAMPLE OF THE GERMAN ID 15
FIGURE 2 – THE PROCESS FOR AUTHENTICATING A USER WITH EID 15
FIGURE 3 – GENERAL MESSAGE FLOW INITIATION (SAML) 17
FIGURE 4 – GENERAL MESSAGE FLOW DURING INTERACTION (SAML) 17
FIGURE 5 – GENERAL MESSAGE FLOW DURING COMPLETION (SAML) 18
FIGURE 6 – SUMMARY OF THE EIDAS NETWORK ACTORS FOR GERMANY AND THEIR ROLE IN THE NETWORK 19
FIGURE 7 – USER SERVICE CONNECTION USING EIDAS CONNECTOR WITH GERMAN MIDDLEWARE 20
FIGURE 8 – DETAILED INTERACTION-FLOW BETWEEN TWO EIDAS MEMBER STATES (ONE WITH MIDDLEWARE) 21
FIGURE 9 – USER AUTHENTICATION WORKFLOW FOR ALL PILOT PARTNERS BY USING KEYCLOAK [22] 22
FIGURE 10 – LATVIAN UNIFIED AUTHENTICATION MODULE (UAM) 24
FIGURE 11 – VPM EIDAS INFRASTRUCTURE 24
FIGURE 12 – KEYCLOAK ADMIN PAGE 34
FIGURE 13 – KEYCLOAK CUSTOM MAPPERS SETUP 35
FIGURE 14 – KEYCLOAK CITIZEN COUNTRY SELECTION 36

List of Tables

TABLE 1 – ACROSS REQUIREMENTS 40

List of Terms and Abbreviations

Abbreviation	Definition
API	Application Programming Interface
eIDAS	Electronic identification and trust services
EU	European Union
HTTPS	HyperText Transfer Protocol Secure
IAM	Identity and Access Management
IdP	Identity Provider
JSON	JavaScript Object Notation
JWT	JSON Web Token
LDAP	Lightweight Directory Access Protocol
MS	Member State

Abbreviation	Definition
MW	Middleware
OAUTH2	Open Authorization 2.0
OOP	Once-only principle
PA	Public Administration
PKI	Public Key Infrastructure
REST	Representational State Transfer
SAML	Security Assertion Markup Language
SDGR	Single Digital Gateway Regulation
SPI	Service Provider Interface
SSL	Secure Sockets Layer
TLS	Transport Layer Security

1. Introduction

1.1. Purpose and scope

The main goal of ACROSS is to provide a holistic solution that allows public administrations to deliver a user-centric interoperable cross-border mobility service compliant with the current European regulations where the private sector can also interconnect their services while ensuring the data sovereignty of the citizens. To this end one of the ACROSS objectives is to provide a set of components that will facilitate the security features needed by the user of ACROSS platform to be authenticated and authorized for using national services, against their country's eIDAS scheme.

To this end, a set of modules have been developed, are used by the platform directly, having also the option of being customized to adapt to specific needs of the offered services, serving as middle layers between the platform, the services and the eIDAS network.

This is also in line with the SDG requirements for security and traceability, ensuring data access only to authenticated and authorized users according to their roles and access rights.

1.2. Approach for Work Package and Relation to other Work Packages and Deliverables

WP4 aims to provide a set of tools and technological solutions that implements the "borders" of ACROSS Platform; in details, these tools and solutions concern: authentication aspects compliant with eIDAS, user support tools to facilitate both the interaction of the citizens with User Journey Services and connection to public and private sector services.

The services and tools developed in this WP have been integrated into the platform created in WP5 and demonstrate the functionality of the use cases in WP6. To this end the approach followed by this WP was to identify firstly the main building blocks, capabilities, interfaces and interactions which will satisfy the identified functional and non-functional requirements as documented in deliverable *D5.1 System Architecture & Implementation Plan – Initial.* In turn, the information documented in *D5.2 System Architecture and implementation plan (final)* has been the basis for the concrete implementation of the specific architectural component.

1.3. Methodology and Structure of the Deliverable

This deliverable's purpose is to serve as a report of the final phase of implementation of the security components for authentication and authorization of a citizen, on the ACROSS platform. utilizing the eIDAS network and using their national eID providers.

The structure of the deliverable is as follows:

- **Chapter 2** goes into detail about the main concepts regarding the Digital Identity and eIDAS regulation, and explaining authentication and authorization and their relationships, albeit in a high level. Technical details are beyond the scope and skipped. This section is the same as in deliverable D4.1 as it serves as an introduction allowing the reader to understand the main concepts of the Digital Identity.
- **Chapter 3** describes the current state of eIDAS in the three pilot countries Germany, Greece and Latvia. There are no significant changes in their schemes as described in the previous deliverable.
- **Chapter 4** provides the Requirements of ACROSS applications for authorization and authentication in a detailed manner. This section is also the same as in the previous version.
- **Chapter 5** goes into detailing the Implementation, Design and Architecture of the components. It builds on the description provided in the first delivery going into more detail about what has been done and also providing the links to the code repository. The current implementation eIDAS schemes of Germany, Greece and Latvia are connected and tested, though connection between Latvia and Greece is still under development.
- **Chapter 6** describes the work done thus far, though in a high non-technical level. It also serves as an update to the intermediate release of the deliverable (D4.2) as the components now are connected to all the three eIDAS nodes (also Latvia), The work is on par with the requirements presented in deliverabe D5.2.
- **Chapter 7** provides the conclusions of the deliverable and describes possible next steps to be taken.
- **Annex (Chapter 8)** maps the requirements from D5.2 that are satisfied within this deliverable.

And finally, there is a **reference list** to go into more detail on the concepts described within this deliverable.

2. The Main Concepts

2.1 Digital identity and the eIDAS Regulation

The EU states offer the ability of Digital Identification via electronic means (eID) allowing their citizens to access public services offered online. The eIDAS regulation [27] states that by 29 September 2018 all online public services requiring electronic identification assurance corresponding to a level of 'substantial' or 'high' must be able to accept the notified eID schemes of other EU countries. Public administrations offering online services that match these requirements are therefore obliged to comply.

The Commission recently proposed a framework [28] for a European Digital Identity, which will be available to all EU citizens, residents, and businesses in the EU. Citizens will be able to prove their identity and share electronic documents from their European Digital Identity wallets with the click of a button on their phones. Under the new Regulation, Member States will offer citizens and businesses digital wallets that will be able to link their national digital identities with proof of other personal attributes (e.g. driving license, diplomas, bank account). These wallets may be provided by public authorities or by private entities, provided they are recognized by a Member State. The new European Digital Identity Wallets will enable all Europeans to access services online without having to use private identification methods or unnecessarily sharing personal data. With this solution they will have full control of the data they share[33].

eIDAS version 2.0 is the evolution of the earlier framework, in that it focuses in the sovereignty of the data (end-users are in complete control of their personal data), the OOP - Once Only Principle (data is acquired only once) through the usage of the wallet, and strong security features when storing and applying for services such as the ones offered in ACROSS.

This is WIP though and it won't be available and exploitable by the ACROSS project.

2.2. Authentication and Authorization

The **eIDAS** (**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices) is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. eIDAS oversees electronic identification and trust services for electronic transactions in the European Union's internal market. eIDAS has created standards for which electronic signatures, qualified digital certificates, electronic seals, timestamps, and other proof for authentication mechanisms enable electronic transactions, with the same legal standing as transactions that are performed on paper.

The digital identification of citizens in their electronic transactions requires a European-wide framework for digital authentication and authorization of citizens, with legal validity.

Authentication is defined as the act where a user is confirmed to be who they claim they are. It is usually the first step in the process of getting access to functions and/or assets meant to be used by them. The latter is called authorization. Authentication is usually performed through authentication factors such as username/password, one-time PINs, authentication apps, biometrics (e.g., fingerprint recognition), etc.

A combination of two or more authentication factors is usually used to ensure a strong validity of the process, before granting authorization to the user. Authorization is then the transparent process of granting access to the user to functions and resources of the system, in our case the ACROSS platform and the offered services.

3. The current state of eIDAS nodes in the three pilot countries

3.1. Germany

Germany is a federal republic with a fragmented public digital ecosystem. The federation is a union of 16 federal states that contain 11,000 local governments. Every entity (local governments, federal states, the Federation) provides online services for citizens, companies, and public administration authorities. In order to be user-friendly and not to force citizens to register a separate account in every portal, the Portalverbund and the state portals are interoperable. By registering an account at one portal (state or Federal), citizens are able to use all available German online services.

Online services are provided from the federal states by implementing the OOP. The access to online services takes place via federal user account and state user accounts. The aim is to generate an interoperability of all public services with every state user account or the federal user account, while there is no interoperable use of private services.

In Germany, identity management is handled at a decentralized level by the 16 federal states. The identity of citizens is verified by using the eID as a digital version of the German identity card. As an authentication protocol, SAML is used (OAuth 2 is in development). Generally, the citizens home state acts as identity provider.

The German eID system is based on government-issued chip cards using certified chips and strong cryptographic protocols, i.e.

- German identity cards (Personalausweis) issued to German nationals [8], and
- German resident permits (Aufenthaltstitel) issued to non-EU nationals living in Germany[9].

The German eID utilises two authentication factors to perform authentication, “possession” (eID card) and “knowledge” (6-digit PIN). The eID card stores the personal data and the relevant keys to enable authentication. The PIN is required to express consent and to start the authentication process.[10]

Figure 1-A sample of the German ID

3.1.1. How does eID authentication work in Germany

The technology of the German eID is based on the eIDAS token specification (BSI TR-03110) with the detailed system architecture as defined in (BSI TR-03127).[11]

The German infrastructure consists of a central eID server (on which the eIDAS software is also operated), the background systems and the websites of the service providers.

Communication relationship during eID authentication

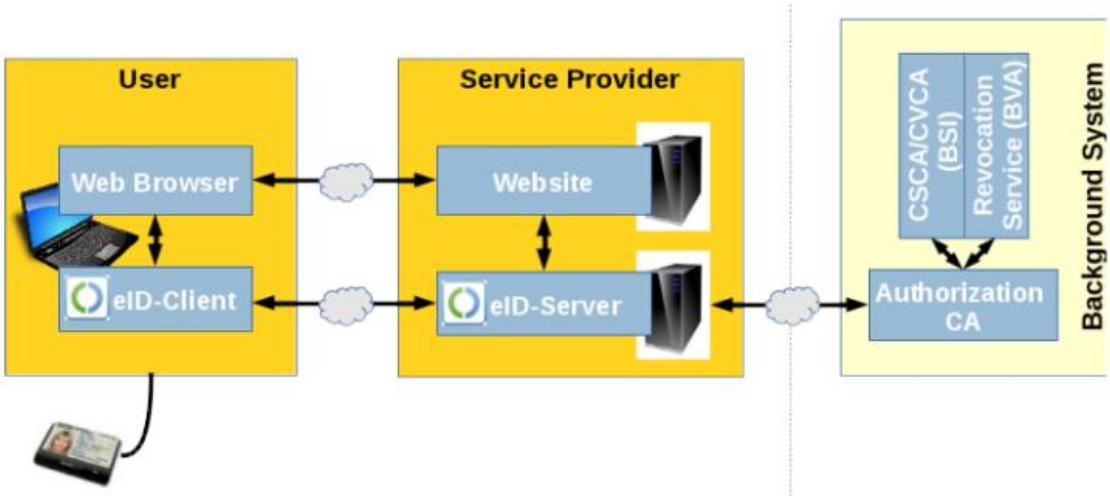


Figure 2 – The process for authenticating a user with eID

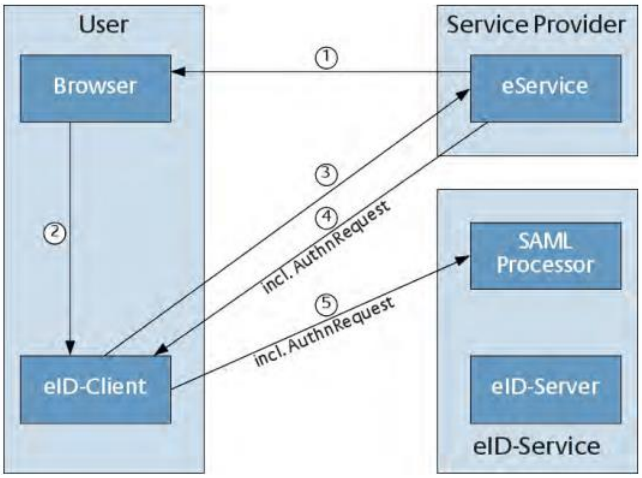
When German citizens want to authenticate themselves using their eID for the use of a web service, they have to follow the process that is shown in Figure 2 and is described below:

1. The user is visiting the service provider's website using a web browser.
2. The service provider sends an authentication request to the eID-Server and activates the eID-Client.
3. Citizens use their identity card (or resident permit) and a 6-digit PIN to start the authentication process in their browser using the eID-Client.
4. The eID-Client verifies that the web session certificate fits with the service providers (relying party) certificate.
5. If the verification is successful, the eID-Client sends the authentication response containing relevant data from the users eID to the eID-Server.
6. The eID-Servers delivers the authentication response to the service provider.
7. The service provider checks the authentication response and gives access to the requested service.[12]

German eID authentication flow with all involved actors

The authentication flow employed by the German eID server is depicted in Figures 3-5 that follow, which correspond to the three phases of the communication process for establishing authentication, namely the initiation, the interaction and the completion. The sequence of steps in each phase is summarized on the right of each Figure:

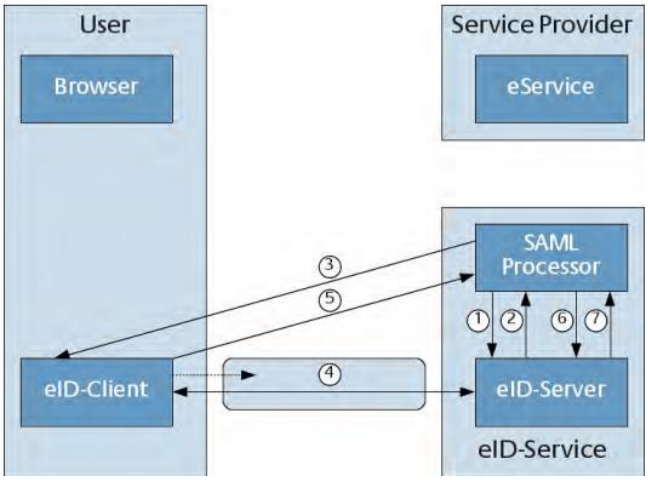
A) Initiation



1. Generate link to presumed tcTokenURL
1. Forward presumed tcTokenURL to eID-Client
2. Call tcTokenURL at eService
3. Redirect to SAML Processor incl. AuthnRequest
4. Call of SAML Processor incl. AuthnRequest

Figure 3 – General message flow initiation (SAML)

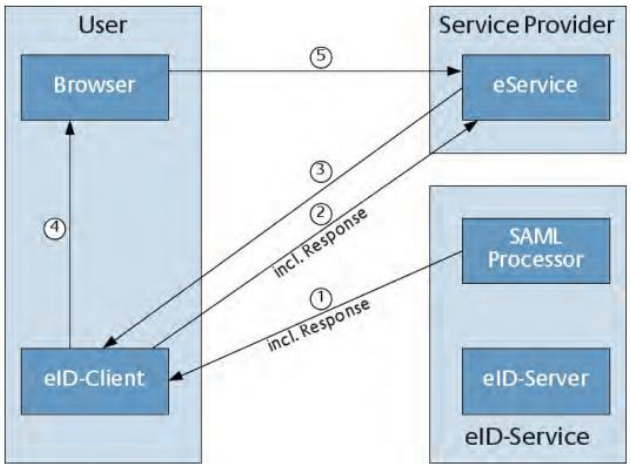
B) Interaction



1. eID-Interface: useID Request
2. eID-Interface: useID Response
3. Transmit TC Token
4. Establish secure authentication channel
5. Call RefreshAddress
5. eID-Interface: getResult Request
6. eID-Interface: getResult Response

Figure 4 – General Message flow during interaction (SAML)

C) Completion



1. Redirect from SAML Processor incl. Response
2. Call of eService incl. Response
3. Response from eService
4. Forward Browser to eService
5. Calling the eService

Figure 5 – General message flow during completion (SAML)

3.1.2. How Germany is integrated into the eIDAS interoperability framework

The integration of the German eID system into the eIDAS interoperability framework is done via the middleware integration model in accordance with the eIDAS technical specifications.[13] Germany, acting as the sending Member State, provides a middleware to the other Member States and the European Commission. This German eIDAS Middleware enables the server side of the German eID authentication procedure by implementing an adapted eID Server with an eIDAS interface that includes three interface components:

1) The **SAML Service** communicates with the eIDAS Connector where the eIDAS Middleware Service is deployed and acts as an eService that delivers the invocation link to activate the eID-Client to the browser and the TC Token to the eID-Client.[14]
2) The **Server-SAL** acts as Attached eID-Server, communicates with the Client-SAL (part of the eID Client) and implements the necessary functionality from the eCard API-Framework.[15]
3) The **PKI communication** component communicates with the Authorization CA to retrieve authorization certificates and black lists.[16][17]

The eIDAS-Middleware is open source (EUPL) and is provided as a virtual machine to the receiving Member States. Germany provides an authorisation certificate to each European Member State

(free of charge) to enable them to request person identification data from the German eID of a citizen.

The registration process is described as follows:

"Identification and the initial registration at a commissioned authorisation CA will be performed via the Point of Single Contact [eIDAS CN] according to a dedicated procedure [MW Integration]. After initial registration, the German eIDAS middleware automatically updates the authorisation certificates. Provisioning of authorisation certificates also includes the necessary eID revocation lists.
Authorisations for non-public sector bodies are issued by the Issuing Office for Authorisation Certificates (VfB) upon application via the standard procedure in accordance with [PAuswV] are authorised."[18]

3.1.3. How to connect ACROSS to the eIDAS infrastructure

3.1.3.1 Overview

The following graphic describes the in the eIDAS-Network involved actors:[19]

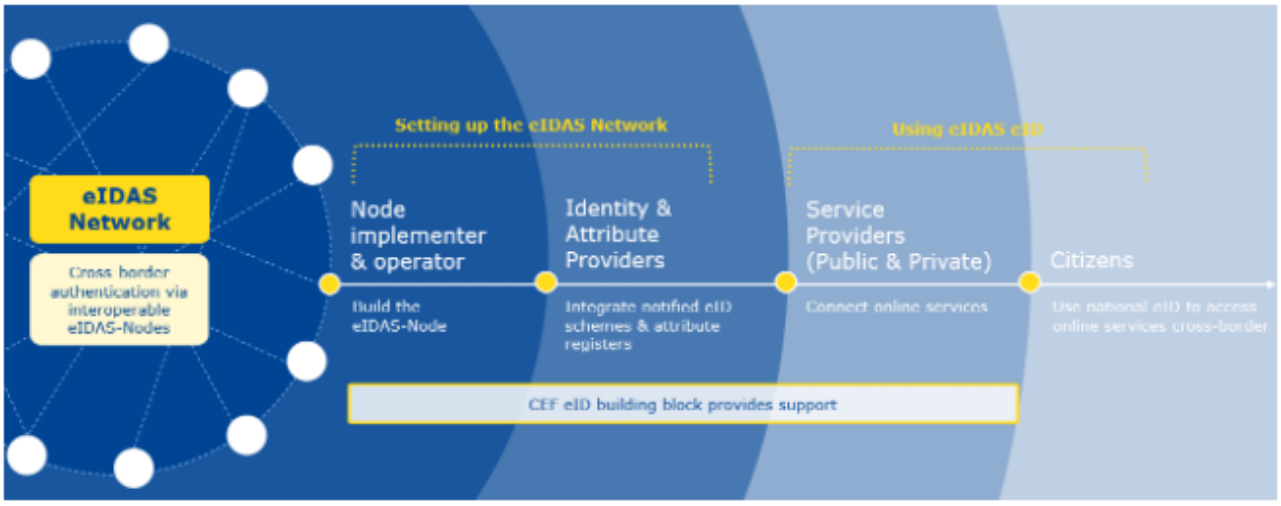


Figure 6 – Summary of the eIDAs Network actors for Germany and their role in the network

3.1.3.2 German use case: Middleware to Proxy

A) The simple perspective

In accordance with the middleware integration model described in 2.1.2 the user-service connection in general is displayed in figure 8:

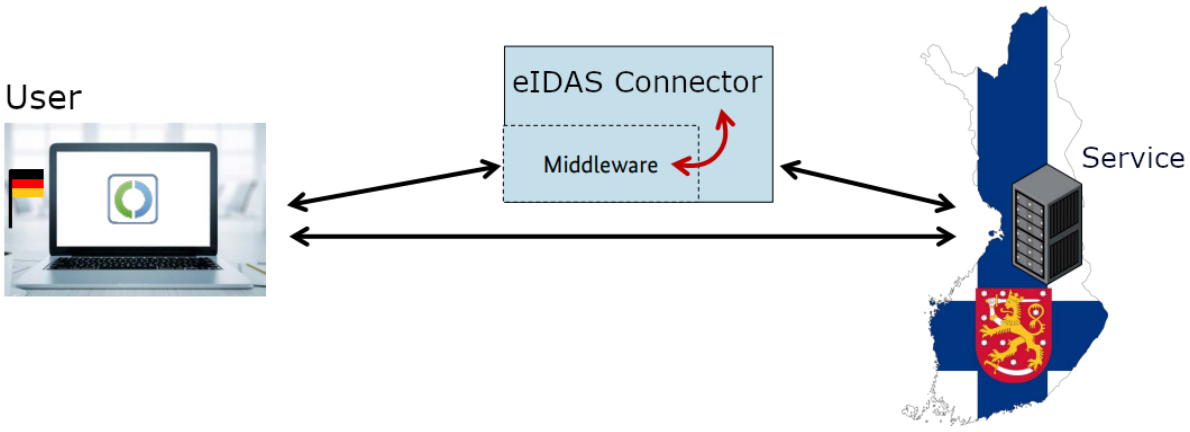


Figure 7 – User Service connection using Eidas Connector with German Middleware

B) The flow with all involved actors

The eIDAS solution for the use case "Middleware to Proxy" consists of two main actors; Member State A (a proxy-based EU-Member State e.g. Greece) and Member State D (a middleware-based EU-Member State e.g. Germany). The detailed flow between Member State A and Member State D is described in Figure 9 and the detailed flow description below.

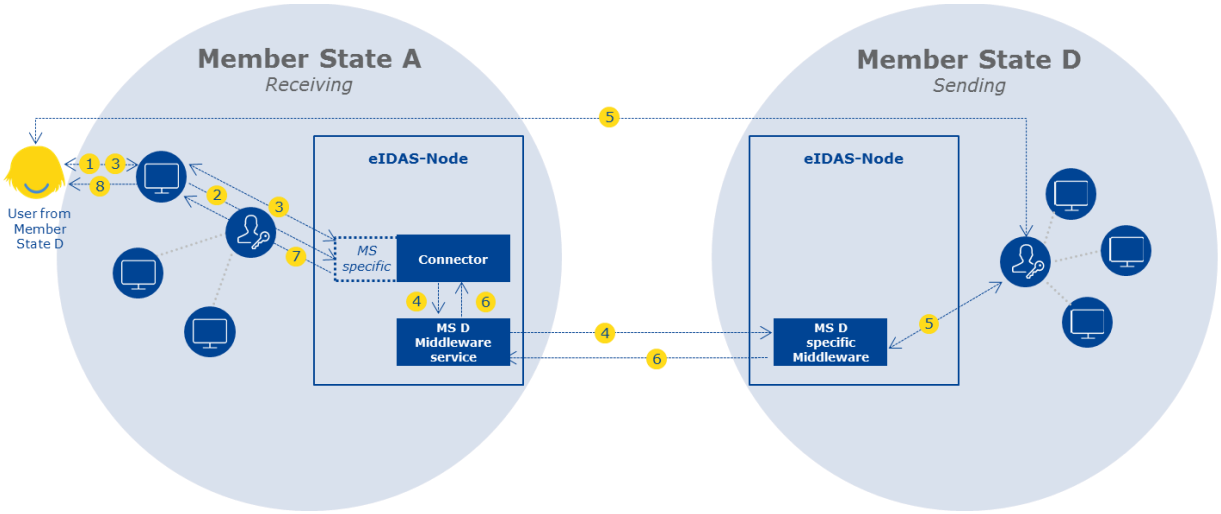


Figure 8 – Detailed interaction-flow between two eIDAS Member States (one with Middleware)

Detailed flow description for German use case [20]

1) The user of Member State D (a Middleware scheme-based country) requests access to the Service Provider in Member State A (a Proxy scheme-based country).
2) The Service Provider sends a request to authenticate the user, usually via the National Identity Provider that forwards it to the eIDAS-Connector. The Member State specific implementation translates the country ID protocol to the eIDAS protocol. (In some cases, the Service Provider can send this request directly to the Connector in the same country.)
3) On receipt of the request, and if the home Member State of user was not already pre-selected by the requesting relying party, the eIDAS-Connector asks the user for their country of origin.
4) When the country of origin is selected, an eIDAS Request is created by the eIDAS-Connector and then sent to the Member State D Middleware-Service which conveys it to the Member State D Specific Middleware.
5) The user authenticates using their national electronic identity in their country D. Depending on the implementation there may be two additional steps within step 5 for the user:
    a) To select the attributes to be provided (therefore giving consent);
    b) To agree the values of the attributes to be provided.

Note: Depending on the Middleware solution, there may be a variation to step #4 and #5. User authentication may be performed directly by the MS D Middleware Service hosted by Member State A.

6) Once the user is authenticated, the Member State D Specific Middleware responds back to the Member State D Middleware-Service hosted in Member State A with the identity information of the user. This is used to create the eIDAS Response which is sent to the eIDAS-Connector in Member State A.
7) The Member State specific part in the eIDAS-Connector uses the eIDAS Response to reply to the **Service Provider; again, usually via a local Identity Provider.**
8) The Service Provider grants access to the user if the authentication is successful.

D) eID authentication in eIDAS member states from a German user perspective

eID authentication within ACROSS will be managed with keycloak using an integrated eIDAS-extension. Keycloak is connected to the pilot partners eID Server to make eID-authentication with national eIDs feasible. Depending on their nationality users will be either forwarded via proxy to authenticate at their national eID-servers (Greek, Latvian) or – in the German case – authenticate at the German eID Server by using the eIDAS Middleware installed on a virtual machine accessible via ACROSS (figure below).[21]

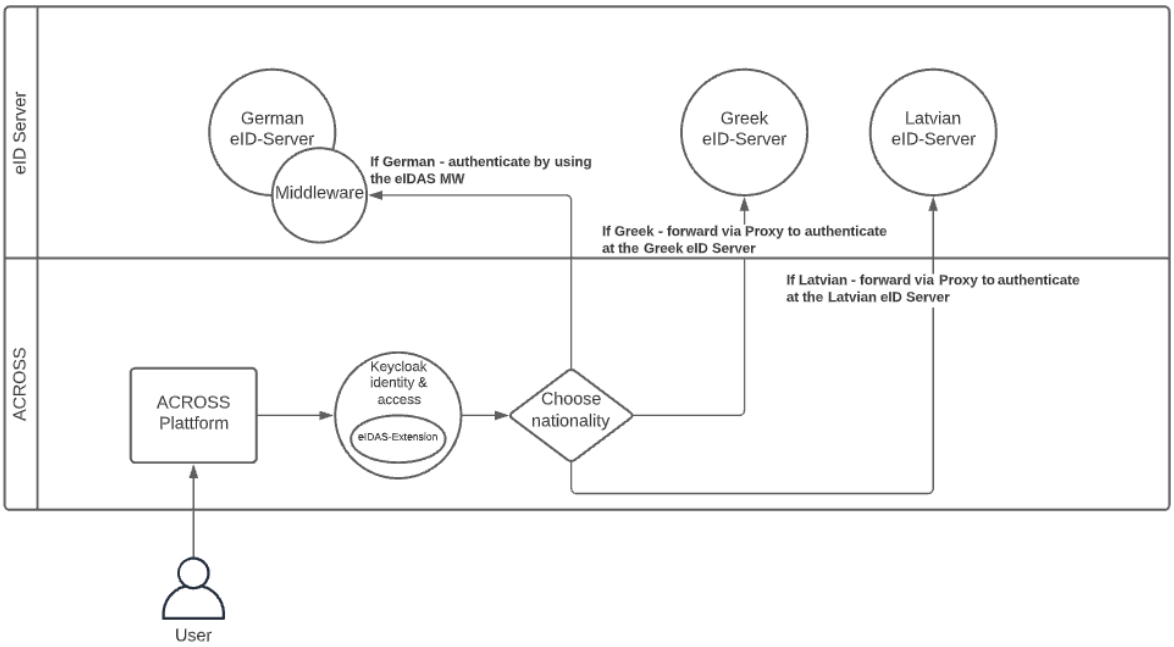


Figure 9 – User Authentication workflow for all pilot partners by using keycloak [22]

1. User is visiting the ACROSS-Platform
2. User logs in with his ID-Card by choosing his nationality
3. For Germans the user gets redirected to the eIDAS-Middleware
4. The eIDAS-Middleware contacting the German eID-Server and verifing the identity of the user
5. After successful authentication the user is being redirected to the ACROSS-Platform

3.1.3.3 Single point of contacts

Further information on how to connect to the eIDAS-Network should be available by using this contact-list:

https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/eIDAS+Points+of+single+contact

3.1.3.4 Integration guide

A detailed eIDAS integration guide for Latvia, can be found here:
https://ec.europa.eu/cefdigital/wiki/download/attachments/82773190/eIDAS-Node%20National%20IdP%20and%20SP%20Integration%20Guide%20v1.4.1.pdf?version=1&modificationDate=1529678642645&api=v2

3.2. Latvia

3.2.1. How eIDAS is used in Latvia

Central part of eIDAS usage in Latvia is Unified Authentication Module (in Latvian – *vienotās pieteikšanās modulis* (VPM)). This module authenticates users using all Latvian authentication credentials (eID, e-signature, i-banking, and username + password (in very specific cases)). This module is centrally managed by State Regional Development Agency (SRDA). If eIDAS authentication is needed by the servicer owner, it can be included in VPM for particular service by request. VPM is integrated in the national platform, thus it is possible to access services using eIDAS (needs further exploration service-by-service) but currently only three services are available for cross-border authentication (none are relevant to ACROSS).

A bit old infographic in English here:

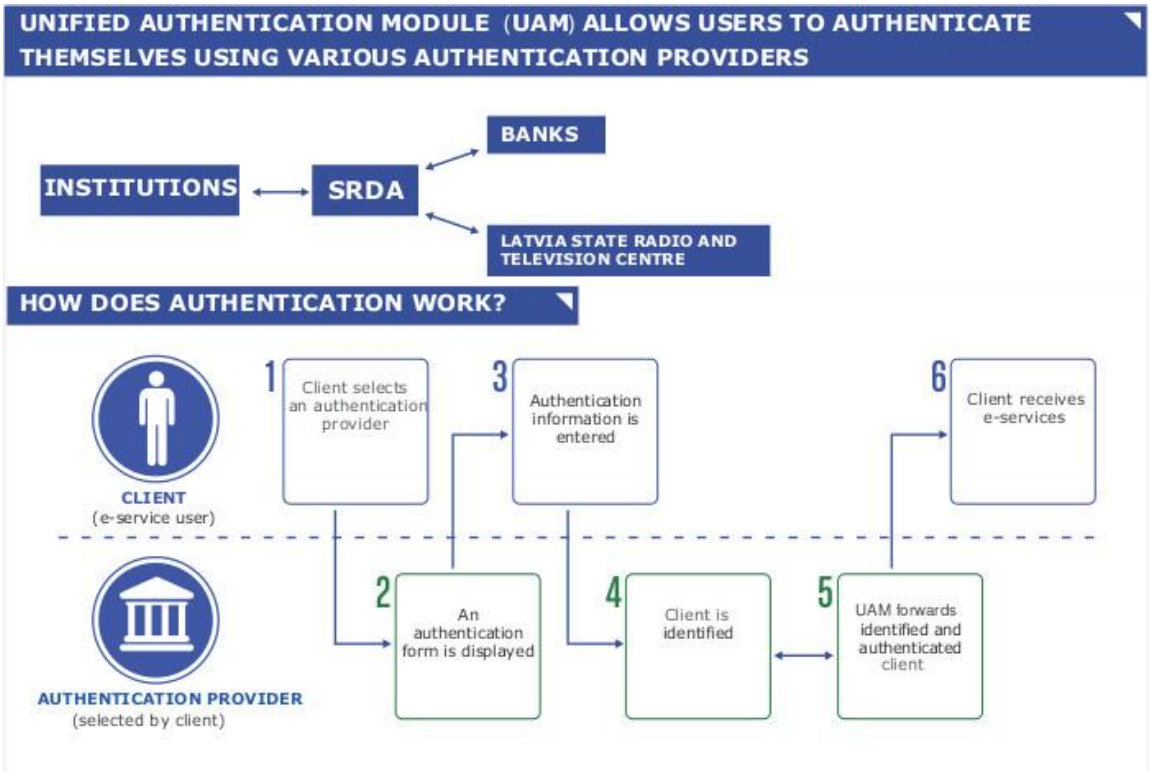


Figure 10 – Latvian Unified Authentication Module (UAM)

A presentation in English on how to introduce VPM for your service:

https://viss.gov.lv/lv/Informacijai/Dokumentacija/Koplietosanas_komponentes/~/media/354D8A778F0A4F9FB6AAE 0AE782F356C.ashx

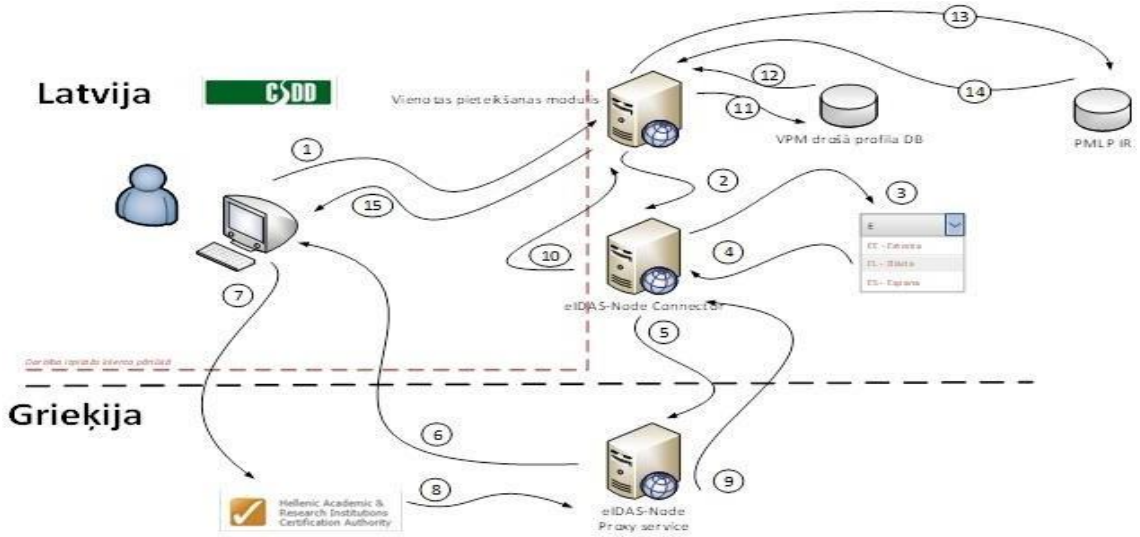


Figure 11 – VPM eIDAS Infrastructure

In order to introduce eIDAS authentication, service owners must ensure personal code validation (latest versions of LvpPersonCodeValidator or IsPersonCode method). eIDAS authentication receives information from the user's home country (eIDAS node-to-node communication), which is forwarded to Latvian Office of Citizenship and Migration Affairs (OCMA). OCMA generates unique personal code for a foreigner which starts with 38. VPM forwards this code to the service owner and performs authentication granting access to the service (see picture in Latvian)

There are four types of Electronic Identification Means (EIM) in Latvian eID scheme. One of them "eID karte" is also physical identification document – Identity Card, as defined in Personal Identification Documents Law [30].

Latvian eID scheme is PKI-based solution.

In case of EIM "eID karte", "eParaksts karte" and "eParaksts karte+" authentication is provided in accordance with the NCP+ policy, with authentication certificates where the private key resides in secure user's cryptographic device – smartcard. In case of EIM "eParaksts" authentication is provided in accordance with the NCP policy, with authentication certificates where the private key resides in secure key management application of user's mobile device. Identity data – the person's first name, last name, and unique identifier (personal code) – is stored in the public key of certificate.

These certificates are accessible on the smart card or in key management application of user's mobile device. Certificates of "eID karte" may also be stored in the public LDAP catalogue if user wishes it. Access to private keys for all EIMs is protected by 2 factors - PIN and possession of corresponding device (smartcard or mobile device).

Middleware of Latvian eID scheme is based on products TRUSTEDX EIDAS PLATFORM, KEYONE

PKI PLATFORM and SAFELAYER MOBILE ID of Spanish corporation Safelayer Secure Communications S.A. (https://www.safelayer.com/en/).

Following parties are involved in the management of the Latvian eID scheme:

- Registration and issuing authority and provider of EIM personalisation - Office of Citizenship and Migration Affairs (for "eID karte") and State join-stock company "Latvia State Radio and Television Centre" (for "eParaksts karte", "eParaksts karte+", "eParaksts").
- Certification Authority (CA), a qualified trust service provider according to the eIDAS Regulation - State join-stock company "Latvia State Radio and Television Centre" with responsibility to maintain certificate lifecycle: creation, activation, suspension, and revocation.

- Electronic Service providers – e-government and private entities providing electronic services that are using eID scheme. Currently there are over 140 government e-services available, mainly through https://www.latvija.lv/en .

Assurance requirements are based on the European legislation (i.e., the eIDAS Regulation, GDPR, etc.) and national legislation (i.e., the Latvian Law on Electronic Identification of Natural Persons [31], Personal Data Processing Law [32] and other national legal acts) for all parties involved. Additional normative requirements apply for the Qualified Electronic Identification Service Provider.

3.2.1. How to connect ACROSS to the eIDAS infrastructure

There is a working connection between Latvia and Germany (it uses Middleware connection, therefore in parallel there is work in progress on the new, direct connection). Connection with Greece is work in progress (connection to pre-production environment is established, work is still undertaken for the connection to the production node) as Greece introduced its node only recently.

Some more overview here (Section 4.2.3. Authorisation):

https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Latvia?preview=/77370111/148898035/LV_notificatio n%20form%20for%20eID%20scheme.pdf

3.3. Greece

The prevalent authentication model in Greece used to be that of Decentralized Direct Authentication. According to this, a person enters into a relationship of trust directly with the service provider and is authenticated directly to him. The result is the creation of many unrelated registers, in which data for the same entities are often kept, while in many cases these data do not coincide either due to their non-updating or due to incorrect initial entry procedure.

In addition, the citizen is burdened by the procedures of registration, issuance and management of multiple credentials, while public bodies are burdened with the cost of the procedures of maintenance / updating of files that contain identification and authentication elements. Until recently, a person could hold a digital certificate for authentication and signature. This credential provides the ability for high quality authentication (signature authentication) however it cannot be used in electronic services provided by other systems because it is not linked to authentication information required to provide the services.

With the advent of gov.gr portal for public services and the ecosystem of services of public administration a huge effort has been made to authenticate the user only once and allow those to be transferred to all other public services. The obligatory identification data are retrieved

when the person is registered in TAXIS in which he uses a specific username and password which, although it provides lower quality authentication, is connected with identification data (eg Tax Registration Number) that allow the provision of electronic services in terms of financial transactions with the public administration.

The same person can also be a user of the electronic prescription application and be registered in the services of IDIKA having corresponding credentials which are connected, on the one hand with identification data (eg Social Security Registration Number) but also with additional characteristics (e.g. .x. Doctor. Pharmacist etc).

In order to reduce the need for users to register in new service systems, the provision of electronic authentication and identification service has started by the General Secretariat of Public Administration Information Systems and the Independent Public Revenue Authority, which has as its basic identification number Tax Registry. This service can potentially be used by any system that has the Tax Registration Number as a mandatory field in the information it has.

At the same time, the National Network of Technology and Research Infrastructures for the Academic Community, has created a network of peer partners (Federation of Academic Institutions) and has established a network of trust between them so that users of a University can receive services from other Academics. Academic Community. This network in the exchange of information does not transfer identification data that are necessary for transactions with the public sector such as e.g. Police Identity Card Number, Tax Registration Number, Social Security Registration Number etc. It is particularly important to note that this Academic Federation is a member of a wider federation of academic institutions (GEANT network) across Europe that have followed across Europe (eduGAIN –Authorization & Authentication).

Finally, the Ministry of Civil Protection (Hellenic Police) and the Ministry of Digital Government, in the context of the adoption and implementation of Regulation (EC) 2252/2004 of the Council of the European Union, is planning for the new generation of police ID cards which will have on the one hand the means of physical identification and on the other hand the travel document. The new identities are expected to gradually replace the existing ones. In the context of their design, the additional functions and specifications that they must have, in order to be able to be used in electronic authentication and identification processes, are examined at the inter-ministerial level.

The main achievements of the Greek eIDAS node are the following:

- An integrated national identity provider within the eIDAS network with the adoption of standards (SAML eIDAS / SAML2int, OpenID Connect / OAuth2) and best practices (eg AARC Blueprint Architecture) and utilization of TaxisNET infrastructure.
- Interoperability with services that require shared e-authentication.
- Notification of the national eID scheme (eID Pre-Notification).

In addition, there is still work in progress on the:

- Development and improvement of the reliability of the National eIDAS node.
- Formulation of practical proposals for the wider utilization of digital certificate services and valid digital signatures by natural and legal persons.

4. Requirements of ACROSS applications for authorization and authentication

The module responsible for providing the means for authentication and subsequent authorization, is the "Identity and Access Management (IAM)" module as described in the D5.2 deliverable [23] section '4.1 Data harmonization and connectors':

The authentication will be provided against the relevant for the citizen eIDAS node (Req_37). The identified citizen will then be authorized to access services provided by the ACROSS-Platform. All mentioned and detected requirements are also listed in a table in the Annex.

4.1 Interoperability

The applications must support well known and widely supported open standards for authentication and authorization. All interactions with other modules and/or applications are implemented through REST mechanisms (Req_42).

All components have to support SSL/TLS 1.3 (and up) for a secured communication. The Communication from all clients with the Authorization Endpoint must utilize TLS (Req_41). It ensures that no data will be leaked. The clients must be able to support https. HTTP without encryption will not be supported (Req_38).

4.2 Security and Privacy

4.2.1 Common

For authentication and authorization OpenID [24][25] Connect is used based on OAuth 2.0. SAML eIDAS / SAML2int must be also supported (Req_43).

The information about an authenticated citizen or system will be transferred through a generated bearer token.

The bearer token will include an Object in JSON-Format encoded as JWT (JSON Web Token) (Req_40). The clients must support cryptographic properties to be able to decode this token (Req_39).

For authentication and authorization, the application must be able to decode the JSON Web Token to get all information about the signed in citizen or system for their purposes. The client must be able to support these protocols.

It must be ensured that all data submitted via the JSON Web Token to the applications is stored in a secure storage.[26] After the session of a user/system has been terminated it must be invalidated and deleted.

4.2.2 Authentication

The Authentication is providing a cross-border authentication to European citizens. It is integrated as an intermediate to the eIDAS-System.

So, the citizen is able to be authenticated by his/her national identity card. The data of the authenticated citizen is transferred in a JSON Web Token.

The applications must be able to handle and evaluate to deny or grant access provided by the IAM.

4.2.3 Authorization

All access to data and services will be managed by fine grained roles. They ensure that the specific citizen or system has only access to the data and services they are allowed to. This information will also be transferred inside a JSON Web Token. The applications of the ACROSS-Platform must be able to handle and evaluate these roles to provide only the access configured by the IAM.

5. Implementation, Design and Architecture

Best practices in dealing with authentication and authorization in modern applications dictate the use of an external component in order to delegate this responsibility. The idea is that an external Identity Management solution, which can be executed either locally or in a cloud-environment, provides the necessary components for both authentication and authorization. Delegating the responsibility to an external well-maintained and open-source system allows the developers of the applications to deal with the actual application at hand and not bother with the difficult task of securing the application and maintaining additional critical code components.

Many open-source solutions have emerged during the last few years which provide an arsenal of functionalities allowing applications developers to combine different types of authentication protocols and authorization paradigms. Examples are:

- Keycloak (https://www.keycloak.org/)
- WSO2 (https://wso2.com/identity-server/)
- FIWARE-IDM (https://fiware-idm.readthedocs.io/)

These tools support a large number of features which provide the necessary flexibility for developers to customize according to their requirements.

ACROSS incorporates the Keycloak identity management server in order to fulfill the requirements described in the requirements section. The following capabilities of the keycloak IdM are very important in order to generically cover the requirements of the ACROSS platform in terms of authn and authz.

1. support for storing users, groups and custom roles,
2. support for integrating with LDAP and directory services
3. support for “Identity Brokering” and thus acting as a Service Provider with respect to an external Identity Provider,
4. support for fine-grained authorization services,
5. open-source licensed (Apache License),
6. a large opens-source community backend by a big software vendor such as RedHat.

5.1 Identity Brokering to eIDAS Nodes

Keycloak as a technology supports the state-of-the-art protocols used in today's systems such as oauth2, OIDC and SAMLv2. Its support for "Identity Brokering" allows the application designer to delegate the IdP functionality to a third-party component, such as an eIDAS Node. When a user first wants to login the keycloak server redirects to the external IdP and after a successful authentication, the user is locally provisioned. During local provisioning a number of user attributes can be retrieved from the IdP and stored locally, after the user provides her/his consent.

The current state of identity brokering to external IdPs in Keycloak can be performed with standard protocols such as SAML v2 and OIDC. In the context of this work package a new keycloak extension is being implemented in order to facilitate the extensions of the basic SAML v2 protocol which are incorporated in the eIDAS Profile [1]. Keycloak supports the idea of extensions which using Service Provider Interfaces (SPI) [2] can extend the basic functionality of the server. SPIs allow the developer to provide custom functionality such as a) a custom authentication flow, b) a custom authenticator, c) custom providers, d) custom user attribute mappers, etc. In general through SPIs the developer is free to add custom functionality in almost all parts of the server's implementation.

5.2 eIDAS Keycloak Extension

The eIDAS Nodes use an extended version of SAML v2.0 which defines a number of SAML elements and attribute definitions which are not supported by default in standard SAML implementations. The extension [7] being developed in the context of T4.1 provides support for these extensions, by offering a custom IdP which can use this extended dialect. The supported extended dialect of the eIDAS nodes is v1.2 as described in the latest set of eIDAS-compliant technical specifications [3][4][5][6].

The extension provides the following components which are needed in order to connect to an eIDAS node using the extended definitions of the eIDAS technical specifications:

- Identity provider "eIDAS SAML v2.0" which is an extended version of the default "SAML v2.0" IdP.
- Mapper "Username Template Importer" which can be used to setup the ID or username for federated user lookup.
- Mapper "Attribute Importer" which can be used to import additional attributes.

- Authenticator "Citizen Country Selection" which can collect the citizen country before authentication.

These components are built to be fully compliant with the **Once Only Principle (OOP)**: users' data needed for accessing the services offered in ACROSS, need only to be registered once, in their respective national ID providers, and can be utilized for authentication and authorization services directly.

5.3 eIDAS SAML v2.0 IdP custom settings

During setup of the “EIDAS SAML v2.0” IdP the administrator is presented with additional eIDAS specific settings such as:

- The Service Provider Country of Origin
- Level of Assurance, e.g. http://eidas.europa.eu/LoA/low
- Whether the service if from the private sector or the public sector.
- The requested attributes that the service needs.
- etc.

The requested attributes are provided in a JSON format as can be seed in the following example. The administrator needs to setup at least the attributes which are required by the eIDAS specifications and can also request for additional optional attributes. Depending on the requested ones the user is presented with the necessary consent forms as described by the eIDAS technical specifications.

```
[{"Name":"http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier",
  "NameFormat":  "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":true
},
{"Name":"http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName",
  "NameFormat":  "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":true},
{"Name":"http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName",
  "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":true},
{"Name":"http://eidas.europa.eu/attributes/naturalperson/DateOfBirth",
  "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":true},
{"Name":"http://eidas.europa.eu/attributes/naturalperson/Gender",
  "NameFormat": "urn:oasis:names:tc:SAML:2.0:attrname-format:uri", "isRequired":false}
]
```

The following figure shows a small portion of the Keycloak admin page showing the custom eIDAS extensions.

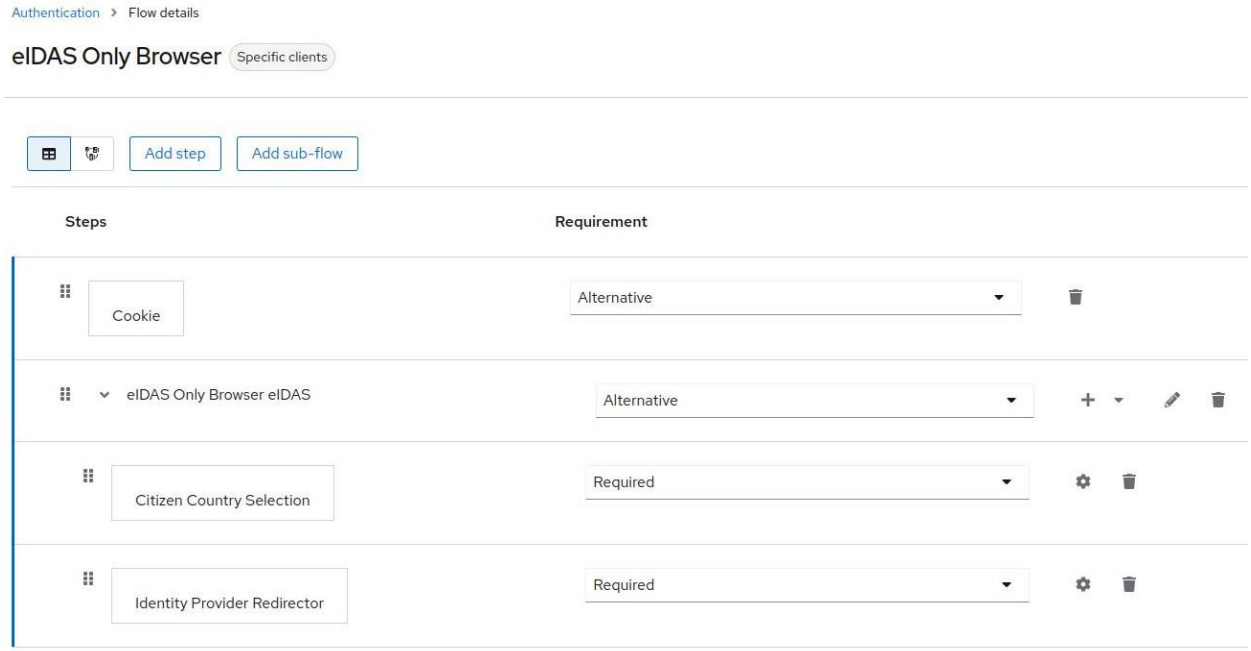


Figure 12 – Keycloak admin page

5.4 IdP Mappers

After the European citizen authenticates successfully in her/his country of origin, a set of requested attributes are safely transmitted back to the Keycloak server which acts as a Service Provider in this context. Using "mappers" the server is able to map these attributes either to user attributes, or groups, or more importantly to the user federated identifier. In order to simplify this procedure a set of custom mappers are developed in the context of T4.1 such as:

- Username Template Importers which can be used with ${ALIAS}.${ATTRIBUTE.PersonIdentifier} and a target of BROKER_ID. The important here is to use the PersonIdentifier since it uniquely identifies a user by prepending country codes.
- Attribute Importers to map additional attributes.

The following figure shows how the extension allows a user to setup these custom mappers.

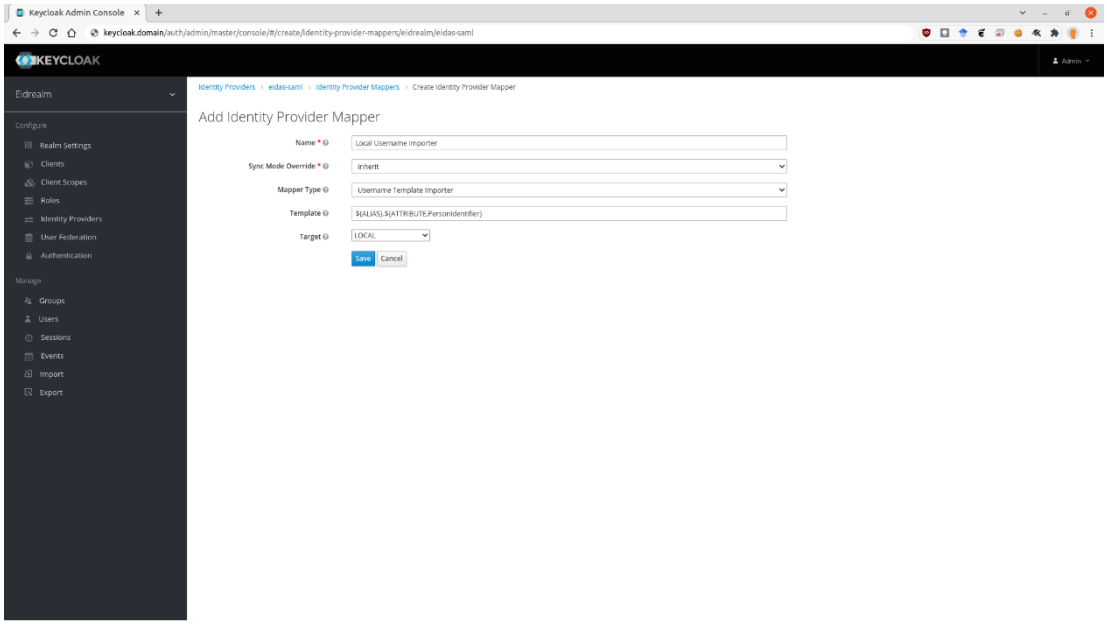


Figure 13 – Keycloak custom mappers setup

5.5 Custom Authentication Flows

During login using the eIDAS SAML v2.0 IdP Brokering extension, the user has to follow a custom flow. The first page should ask the user about her/his country of origin, then forward the user to the eIDAS specific connector. After the user authenticates successfully on her/his country's IdP and provides the necessary consents, the user should be redirected back to Keycloak and on the first login should create her/his account. The following figure shows one possible way to setup the authentication flow, using a custom "Citizen Country Selection" available in the extension.

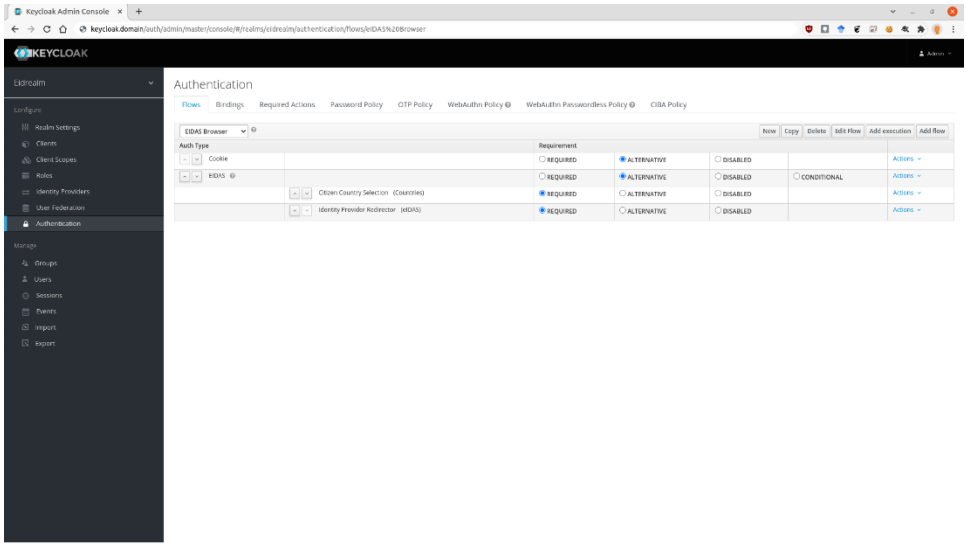


Figure 14 – Keycloak Citizen Country Selection

The "first-login" flow can be setup using the already existing functionality of Keycloak which provides flexibility to the administrator to setup the most common use-cases that arise in modern applications.

6. Work done and current status

The components are in their final version with full functionality provided to the application of ACROSS onn par with te requirements of deliverable D5.2.

The components are directly incorporated in the platform code without any further need to change the code, the only requirement is just to define the connection parameters of any eIDAS node (or intermediate proxies) for the three pilot countries (or any country having a working and notified eIDAS node for that matter).

The connection to German eID scheme is implemented through the use of the provided middleware, while the Greek and Latvian nodes are connected directly to the components.

The German node is connected to the Latvian and to the Greek node and allows for citizens of the respective countries to authenticate for services provided in Germany and vice versa.

Unfortunately, the Latvian and Greek nodes are not as of yet connected, Latvian node is only connected to the Greek pre-production (test) node, which doesn't allow for full authentication functionality. The reason is that the Greek eIDAS node is not as of yet fully notified [34].

However, the ACROSS developer team is testing some alternative scenarios that would possibly overcome this obstacle (i.e. the citizen chooses their country of origin which redirects to the respective node for authentication).

Once the user is authenticated, full access to ACROSS application should be granted.

Citizens of Germany and Latvia, are able to authenticate via the eIDAS, however the Greek node, although technically functional, does not as of yet provide connection to the Greek national IDp (taxisnet).

7. Conclusions and next steps

This document describes the result of the effort put as part of Work Package 4, Task 4.1 “Components adaptation for SDG, OOP, eIDAS for National public services” and its relations to other activities pertaining to the ACROSS platform. This document reports on the final version of the components, and its integration with the ACROSS platform.

The three pilot countries current situation of the eIDAS implementation has been described.

The requirements covered by the components have been specified and there has been a thorough description of the architecture and implementation procedures taken to commence development of the components. As a result, a final version of the components has been implemented in the ACROSS platform and is in working state against the German, Greek and Latvian eIDAS nodes. The components have taken into account the specifics of each implementation of eIDAS, i.e. the use of middleware applications in the German implementation.

The main goal of this document is to describe the final release of the Identification and Authorization Module and to detail the work put on development of the described components.

The code is in final version, is Open Source as per the requirements and is available on GRNET Github repository [29]

This ensures the re-usability of the components’ code into similar projects.

The main effort put on the time between the previous deliverable and this, was to take the steps needed to connect the Latvian eIDAS node. This has been achieved technically, with specifics remaining on the path.

Refinement of the components’ code, might be required taking into account the evolution of the ACROSS platform component and align with the other related components and modules, based on the requirements and architecture as described.

In this final phase further testing to ensure seamless integration with the ACROSS platform is required as per possible additional functional and non-functional requirements arising, and also to ensure compliance with the SDG, in line with the OOP (data should not be required to be input more than once).

As mentioned, the Greek eIDAS node, albeit functional, is still WIP, meaning that the node yet has to be connected to the Greek National eID scheme, which is TAXISNET. The work is progressing rather slowly [34] and we are not sure if it will be complete by the end of the the

ACROSS project. Anyway, the code used in ACROSS, is fully connected to the node, and as soon as the node is connected to TAXISNET, Greek users will be able to authenticate and be authorized to use any system that is using our components out of the box. The fact that the code is Open Source, ensures the usability in any future similar projects.

8. Annex - ACROSS Requirements Mapping

Table 1 – ACROSS Requirements

Id	Title	Description	Type	Category
Req_16	Open API access	Data and services available in the ACROSS platform have to be accessible via a set of APIs using standardized approaches (e.g. RESTful API).	functional	Platform architecture and interoperability
Req_18	Cross Border Authentication	The services deployed and executed in ACROSS platform should have the possibility to be integrated, if needed, with eIDAS system. The platform can optionally support single-sign-on mechanism to simplify authentication on multiple applications and services internally to the platform.	functional	Security and Privacy
Req_19	Reliability and Integrity	The implementation of ACROSS should follow open standards and use well-known and widely accepted technologies in order to ensure integrity. The ACROSS platform has to be reliable assuring integrity of the components/tools that are part of it.	non functional	Platform architecture and interoperability

Id	Title	Description	Type	Category
Req_20	Security access	Access to services and data has to be available to authorized users/applications only. Only audited applications are allowed to be deployed to ensure compliance with the security policies. Every security violation should be reported and the necessary actions to protect information and applications present in the platform has to be performed.	functional	Security and Privacy
Req_22	Privacy and Data Protection	The ACROSS platform has to be compliant with the EU legislation regarding privacy and data protection. It should adopt all the necessary technologies, standards and methods to protect privacy of the users of the platform services and to secure stored information that could be considered private.	non functional	Security and Privacy
Req_23	OpenID Connect - Role-Management	The clients using the ACROSS-Platform have to be authenticated and authorised to get only the permissions that are required. This has to be defined by roles.	functional	Security and Privacy
Req_24	OpenID Connect - Role-Management	For securely exchanging roles between two parties it is needed to define a data format	functional	Security and Privacy
Req_25	OpenID Connect - Client-Registration	It is needed to register the clients that want to use the ACROSS-Platform	non functional	Security and Privacy

Id	Title	Description	Type	Category
Req_26	OpenID Connect - Client-Registration	Definition of the client registration workflow	business	Security and Privacy
Req_30	Open source	I want the ACROSS reference architecture to reuse already available open source solutions and only create or improve those aspects that are not covered by the existing solutions	non functional	Platform architecture and interoperability
Req_32	Identity Certificate	I want to have a unique identity ACROSS ecosystem in the form of a certificate, so that secure and trusted connections to all parties, internally and externally (e.g public and private service) can be established during cross border service provisioning.	functional	Security and Privacy
Req_33	Accessibility	The front-ends of the system should comply with the current Web Accessibility Directives and in particular with EN301549 (included in WCAG-2.1)	non functional	Web&Mobile applications
Req_34	Confidentiality	The platform has to follow the 'privacy-by-design' and 'security-by-design' approaches and in particular should comply with the principle that users should provide only the information that is absolutely necessary.	non functional	Security and Privacy

Id	Title	Description	Type	Category
Req_37	eIDAS interoperability framework	The platform has to be integrated in the eIDAS interoperability framework. Secure connection to all relevant eIDAS nodes and other relevant eIDAS components must be ensured.	functional	Interoperability
Req_38	HyperText Transfer Protocol Secure	All user interaction has to be secured with the HyperText Transfer Protocol Secure (https).	functional	Security and Privacy
Req_39	Cryptographic properties	The clients must support cryptographic properties to be able to decode all tokens used during authorization and authentication (JSON Web Tokens).	functional	Security and Privacy
Req_40	JSON Web Token	For authentication and authorization, applications and clients must be able to decode JSON Web Tokens to get all information about the signed in citizen or system for their purposes.	functional	Authentication and Authorization
Req_41	SSL/TLS 1.3	All components have to support SSL/TLS 1.3	functional	Security and Privacy
Req_42	REST	All interactions with other modules and/or applications have to be implemented through REST mechanisms.	functional	Security and Privacy

Id	Title	Description	Type	Category
Req_43	SAML	Together with the standard OpenID Connect (oAuth2) the XML-framework SAML must be supported to ensure authorization and authentication with all eIDAS member states	functional	Authentication and Authorization
Req_44	Access handling	The applications must be able to handle and evaluate to deny or grant the access provided by the IAM.	functional	Authentication and Authorization

9. References - Links

[1] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile

[2] https://www.keycloak.org/docs/latest/server_development

[3]https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Interoperability%20Architecture%20v.1.2%20Final.pdf

[4] https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Cryptographic%20Requirement%20v.1.2%20Final.pdf

[5] https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Message%20Format%20v.1.2%20Final.pdf

[6] https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf

[7] https://github.com/grnet/eidas-keycloak-extension

[8] https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/eIDcard/eIDcard_node.html;jsessionid=ED5243CC2CEE424CDD2F17751FA72C9A.internet462

[9] https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/eRP/eRP_node.html;jsessionid=ED5243CC2CEE424CDD2F17751FA72C9A.internet462

[10] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper.pdf;jsessionid=8E7AE16354A30710E65B31E4A05C0EB7.internet461?__blob=publicationFile&v=1

[11]

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper_final.pdf%3bjsessionid=3807F628DC3E2D632A0DDC09C32925B8.internet471?__blob=publicationFile&v=1

[12]

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper_final.pdf%3bjsessionid=3807F628DC3E2D632A0DDC09C32925B8.internet471?__blob=publicationFile&v=1

[13]

https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/German-eID/eIDAS-notification/eIDAS_notification_node.html

[14]

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03124/TR-03124-1.pdf;jsessionid=D35CEB289CF8F98A2B686276C4F5BF50.internet481?__blob=publicationFile&v=2

[15]

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03112/TR-03112_node.html

[16]

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03129/BSI_TR_03129.pdf;jsessionid=69370B69358F6F191D8BCB1338133C3C.internet482?__blob=publicationFile&v=1

[17]

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130/TR-03130_TR-eID-Server_Part3.pdf?__blob=publicationFile&v=2

[18]

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper_v1-4.pdf?__blob=publicationFile&v=2

[19] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773200

[20] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Middleware+to+proxy

[21]

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_IF_Mapping_v1-4.pdf?__blob=publicationFile&v=2

[22] (Needs free registration to access)

https://lucid.app/lucidchart/f58f8463-6132-40d3-94ae-05ba8e86fb35/edit?invitationId=inv_b5101051-0ef7-4fb7-a5cb-ad6fca5269b0

[23] D5.2: System Architecture and implementation plan (final)

[24] https://openid.net/specs/openid-connect-core-1_0.html#RFC6749

[25] https://openid.net/specs/openid-connect-core-1_0.html#RFC6750

[26] https://datatracker.ietf.org/doc/html/rfc7519

[27] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Legislation+in+a+nutshell

[28] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

[29] https://github.com/grnet/eidas-keycloak-extension/

[30] Personal Identification Documents Law,

https://likumi.lv/ta/en/en/id/243484

[31] Law on Electronic Identification of Natural Persons,

https://likumi.lv/ta/en/en/id/278001

[32] Personal Data Processing Law (in Latvian only),

https://likumi.lv/ta/id/300099-fizisko-personu-datu-apstrades-likums

[33] https://utimaco.com/current-topics/blog/eidas-2-the-european-digital-identity-wallet

[34] Status of eIDAS in Europe, https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Country+overview

[35] D5.1 System Architecture & Implementation Plan – Initial.