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

increasinG tRust with eId for Developing buSiness

D2.1 Business Services and Technical Architecture

Document Identification			
Status	Final	**Due Date**	30/06/2021
Version	1.0	**Submission Date**	02/07/2021

Related Activity	2	**Document Reference**	D2.1
Related Deliverable(s)		**Dissemination Level (*)**	CO
Lead Participant	INFOCERT	**Lead Author**	Cristina Andreoli Davide Zannirato
Contributors	ATOS Kompany ADACOM UAEGEAN	**Reviewers**	ATOS - Ross Little Kompany - Peter Bainbridge-Clayton

Keywords
GRIDS, eIDAS, AML, BAA, DC, DP, KYC, Identification, authentication

This document is issued within the frame and for the purpose of the GRIDS project. This project has received funding from the European Union's Innovation and Networks Executive Agency – Connecting Europe Facility (CEF) under Grant Agreement No INEA/CEF/ICT/A2019/1926018; Action nº 2019-EU-IA-0044. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

(*) Dissemination level: **PU**: Public, fully open, e.g. web; **CO:** Confidential, restricted under conditions set out in Model Grant Agreement; **CI:** Classified EU RESTRICTED, EU CONFIDENTIAL, **Int =** Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

Document Information

List of Contributors	
Name	Partner
Juan Carlos Pérez Baun	Atos
Ross Little	Atos
Alberto Crespo	Atos
Peter Bainbridge-Clayton	Kompany
Russell E. Perry	Kompany
Dominik Tiefenbacher	Kompany
Carina Wolf	Kompany
Dimitris Tsabiras	ADACOM
Constantinos Pretenteris	ADACOM
Nikos Feidopiastis	ADACOM
Serafeim Makris	ADACOM
Stamoulis Zamanis	ADACOM
Kostas Noussias	ADACOM
Davide Zannirato	INFOCERT
Cristina Andreoli	INFOCERT
Romualdo Carbone	INFOCERT
Pasquale Minervini	INFOCERT
Nikos Triantafyllou	UAEGEAN

Document History			
Version	Date	Change editors	Changes
0.1	29/05/2020	Cristina Andreoli – INFOCERT	First Table of Content and structure indication
0.2	18/06/2020	Cristina Andreoli – INFOCERT	Adjusted the Document information section. Inserted initial text in section in 2.1 and 2.1.3 (in INFOCERT's charge).
0.3	18/06/2020	Constantinos Pretenteris - Adacom	Added GR eIDAS node information
0.4	18/06/2020	Constantinos Pretenteris - Adacom on behalf of Nikos Triantafyllou - UAegean	Added info about eID nodes in Private Sector
0.5	28/09/2020	Juan Carlos Pérez Baún (Atos)	Added contribution on LoA, Spanish eIDAS node, Interoperability, DNIe.
0.6	17/05/2021	Cristina Andreoli	Review for preparation final version
0.7	27/05/2021	Romualdo Carbone	Inserted technical chapter

0.8	14/06/2021	Cristina Andreoli	Added architectural structure chapter (task 2.2) based on document dated 19.05.2021
0.9	30/06/2021	Cristina Andreoli	Version for quality review
1.0	02/07/2021	Juan Alonso, Juan Carlos Perez (ATOS)	Review of final version before submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	InfoCert (INFOCERT)	30/06/2021
Peer reviewers	Ross Little (Atos) Peter Bainbridge-Clayton (Kompany)	24/06/2021
Quality Manager	Juan Alonso (Atos)	02/07/2021

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AgID	Agenzia dell'Italia digitale (Agency for Digital Italy)
AML	Anti money Laundering
AMLD4	Anti-Money Laundering Directives
CD	Continuous Development
CDD	Customer due diligence
CI	Continuous Integration
CIE	Electronic Identity Card
CNS	Carta Nazionale dei Servizi (National Service Card)
DC	Data Consumer
DNIe	Documento Nacional de Identidad electrónico (eIdentity National Document)
DP	Data Provider
DS	Data Subject
EC	European Commission
eID	electronic IDentification
eIDAS	Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market
EU	European Union
FIs	Financial Institutions
GDPR	General Data Protection Regulation
ICAO MRTD	International Civil Aviation Organization, Machine Readable Travel Document
IDA	Identity Assurance
IdP	Identity Provider
IEC	International Electrotechnical Commission
ISO	International Organization of Standardization
JSON	JavaScript Object Notation
JWKS	JSON Web Key Set
KYB	Know Your Business
KYC	Know Your Customer
KYCC	Know your Customer's Customer
MS	Member State
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
LEI	Legal Entity Identifier
LOU	Local Unit Operator
OIDC	OpenID Connect
OIDC IDA	IDA OpenID Connect for IDentity Assurance
OP	OpenID Connect Provider
OS	Open Source

RP	Relying Party
SAML	Security Assertion Markup Language
SP	Service Provider
UBO	Ultimate Beneficial Owners
VM	Virtual Machine
WG	Working Group

Executive Summary

The Know your Customer – KYC procedure, definition that includes also the Know your Business (KYB) and the Know your Customer's Customer (KYCC), is becoming an increasing factor for worldwide businesses and activities, from public administration to private sector (above all financial, professional services, online retail or energy and telecom sectors).

The core need of the KYC process is the correct identification and authentication of the potential customer, natural or legal person, including natural person representing the legal person, and the plausibility of their activities.

GRIDS project has the objective to enable private players across Europe to effectively and simultaneously access and process KYC and eIDAS identity information, using eIDAS identity verification to create and maintain a consistent single view of their customers and perform effective and accurate screening, in order to guarantee compliance with applicable regulations mandating enhanced the due diligence procedures, thus increasing, where applicable, the operational efficiency of anti-money laundering and, more generally, preventing and recognising financial crimes.

GRIDS enables KYC Data Providers and Data Consumer to connect KYC information with eIDAS authentication data. This service may be defined as a new generation of "KYC as a Service", that makes the provision of commercial services based on EU interoperable authentication services more transparent and accountable and more respectful of citizens' privacy.

The access to and interoperability of strong means of secure electronic identification and authentication are based on the legal certainty provided by the eIDAS Regulation and its materialisation both technically and organisationally as well-supported nodes.

Indeed, the key attributes related to identity are obtained across borders and in a certified way by the foreign Member State eIDAS node from trustworthy sources, such as recognised identity providers asserting the authenticity of the electronic means of authentication and optionally additional attribute providers, in a transparent and reliable way, in accordance with eIDAS Regulation and General Data Protection Regulation (GDPR) principle of data minimization, among others. eIDAS nodes allow to link cross-border to the eID trustworthy source of information to make a check against the customer's claimed identity and also replace the need to additionally provide face-to face identity altogether, taking innovation one step further costly operator-managed video and biometric remote verification procedures when allowed by national law.

In specific sectors, as the financial and banking, compliance is also needed with additional regulations related to the prevention of financial crimes, like the Anti-Money Laundering Directive and second Payment Services Directives that request a safe data governance and streamlining of the related business operations.

GRIDS architecture enables such private sector to receive reliable identity data through a fully automatic and secure transfer from the eID itself to the end-receiving service provider for verification, all allowed thanks to a trustworthy interoperability infrastructure.

1 Introduction

1.1 Purpose of the document

This document refers to “Activity 2 - Business Requirements, Technical Design and Integration Planning” and represents the results of all the activities carried on inside the “Activity 2” which are both functional and technical.

From the functional point of view the present document is aimed to provide a general definition of the project GRIDS and its applications. Moreover, it defines a possible feasible framework between the subjects involved in the service. This analysis focuses in particular on which rules and legislations are applicable to GRIDS, especially in the framework of the eIDAS nodes.

From the technical point of view the main objective of the document is to offer a clear representation of the whole architectural design produced to realise the GRIDS platform.

1.2 Relation to other project works

This document is strictly connected to the Activity 4 Business Use Cases Definition and Activity 6 Marketing analysis. The general studies of GRIDS’s architecture and regulations that may have impact on it as presented in this document have been deeper analysed and applied in the most significant use cases as per Activity 4 and in the market investigation as per Activity 6.

At the same time technical architectural aspects are strictly related to activities performed inside Activity-3 and Activity-4.

1.3 Structure of the document

This document is structured in 4 major chapters.

Chapter 2 presents details about the regulations that may impact on GRIDS and all its components: starting from a general explanation of the applicable legislations and their requirements (eIDAS Regulation and applicable eIDAS nodes, AML, PSD2, GDPR), going into a more detailed description of the connection and influence between such laws and the KYC and KYC requirements.

Chapter 3 introduces a high-level implementation that enables readers to easily understand GRIDS architecture and flow: description of the implementation with GRIDS product with illustration of the business flow in a diagram.

Chapter 4 details the GRIDS Business Attribute Aggregator (BAA) high level design and architecture. The BAA enables the authentication of natural and legal persons over eIDAS and uses this assured identity data in the further collection of Know Your Customer (KYC) & Know Your Business (KYB) claims from Data Providers, that are connected over the GRIDS BAA.

Chapter 5 details the GRIDS testing framework and explains the entire workflow adopted as well as the objectives and differences compared to the typical test tasks for CI / DI. The two types of tests to be performed are described, which are summarized in automated tests and in-vivo test cases. For each type what is expected to be tested is described. For a better evaluation of the quality of the software produced, will be asked to submit evaluation reports, interviews, regarding the usability of the platform and their over all experience and their answers will be used to further evaluate and improve the impact of GRIDS.

2 Regulatory background

For the provision of cross border electronic services, such as GRIDS (increasinG tRust with eId for Developing buSiness), both the European and the national legislation and requirements have to be taken into consideration. The main European Regulatory frameworks that have impact to GRIDS structure and therefore have to be analysed are the eIDAS Regulation and each domestic eIDAS node, the Anti-Money Laundering Directive (AML) and each domestic AML law, the Directive on payment services in the internal market (PSD2) and the General Data Protection Regulation (GDPR).

- eIDAS Regulation: The European Commission has produced the eIDAS Regulation with the purpose of boosting efficiency and trust in cross-border digital transactions. This improvement can be obtained through the adoption of a framework based on the interoperability of national electronic identities (e-ID). eIDAS will support the growth of the European digital market, by offering infrastructures for public administration, businesses and citizens aimed to increase convenience and confidence in the digital environment.
- AML: The European Union adopted the first anti-money laundering directive in 1990 in order to prevent the misuse of the financial system for the purpose of money laundering. It provides that obliged entities shall apply customer due diligence requirements when entering into a business relationship (i.e. identify and verify the identity of clients, monitor transactions and report suspicious transactions). This legislation has been constantly revised in order to mitigate risks relating to money laundering and terrorist financing.
- PSD2: The original Payments Services Directive (PSD) was created in 2007 by the European Commission with the aim to create a single market for payments in the European Economic Area. The objectives of PSD2 are to make payments safer, increase the consumers' protection, foster innovation and competition while ensuring a level playing field for all players, including new ones.
- GDPR: This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. GDPR protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Following, a description of those main regulatory frameworks that have influenced the Business Services design.

2.1 Regulation (EU) No 910/2014 (eIDAS Regulation)

The European Commission proposed on the 4th of June 2012 a Regulation on **e**lectronic **ID**entification and **A**uthentication **S**ervices (eIDAS). The eIDAS Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (Regulation (EU) No 910/2014) was adopted by EU co-legislators on 23 July 2014[1].

The Regulation is applicable since the 1st of July 2016, the same day the Directive expired, still there were articles that continued to be valid. Since 29 September 2018 the eIDAS came into force and remains applicable.

2.1.1 General intro

The main part of the eIDAS Regulation (Chapter II) concerns electronic identification. Nevertheless, concerning eIDs, the Regulation focuses on the mutual recognition by Member States, whereas the trust services are treated as market services. The electronic identity part is not that developed, yet it establishes that its allowed to offer cross-border recognition to the existing electronic identity systems for access to online public services, if the electronic identity schemes have been notified to the Commission and cover certain requirements.

Notification to the national schemes is the main request for national electronic identification means to be recognized by other Member States to access online services provided by their public sector bodies. This means that the electronic identification scheme of a Member State is published in a list completed with notified electronic identification systems. In order to be eligible to be notified, they must comply with some conditions and, at the end, they must be accepted. In particular, they must meet the requirements of an assurance level (see next paragraph), must be used to access a public service in the Member State and must meet certain requirements to be interoperable.

2.1.2 Level of assurance

Established and recognised substantial/high levels of authentication assurance (Art. 8 - Level of assurance - LoA) and authentication schemes

- EU Regulation on levels of assurance[2]
- LoA for eID means
  - Low
  - Substantial
  - High
- LoA for natural and legal persons

The Level of Assurance (LoA) determines the grade of trust an eID mean provides when the identity of a natural or legal person is established, guaranteeing that the person providing an identity is the person who they claim to be. Several LoA have been established until now depending on the standard adopted by the different countries (ISO/IEC 29115:2013[35], NIST[36]).

In Europe the eIDAS Regulation[3] and Article 8 Assurance levels of electronic identification schemes establishes three different levels of assurance (low, substantial or high) depending on the degree of trust:

- **Low**: *"provides a <u>limited degree of confidence</u> in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to <u>decrease the risk of misuse or alteration of the identity</u>"*;
- **Substantial**: *"provides a <u>substantial degree of confidence</u> in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to <u>decrease substantially the risk of misuse or alteration of the identity</u>"*;
- **High**: *"provides a <u>higher degree of confidence</u> in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to <u>prevent misuse or alteration of the identity</u>"*.

According to the eIDAS regulation the authentication request sent by the service provider to the eIDAS network must include the required LoA. The eIDAS network will provide a valid authentication response when the LoA of the provided eID mean is equal or higher than the required LoA.

The mutual recognition of national eID means, issued by the EU Member States, is necessary for allowing the EU citizens cross-border operations. In order to assure the interoperability and make a comparison between the different eID means, the EC has developed the implementing Act providing the minimum technical specifications and procedures for assurance levels for electronic identification regulation[4], taking into account the international standard ISO/IEC 29115 and the Large-Scale Pilot STORK. Also, a document for guiding the application of the LoA to natural and legal persons[5] has been delivered. This allows to each Member States to compare each other their eID means.

Regarding the requirements to be fulfilled by natural and legal persons related to the authentication mechanisms, are provided in the following table:

Table 1: Requirements for authentication[4]

Level of Assurance	Elements needed
Low	1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity. 2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline. 3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.
Substantial	Level low, plus: 1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication. 2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.
High	Level substantial, plus: the authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

2.1.3 eIDAS nodes intended to be used and brief on national nodes

Cooperation between Member States on the interoperability and security of electronic identification schemes is essential to foster a high level of trust and security appropriate to the degree of risk in eIDs schemes.

For this reason the eIDAS regulation, together with the Commission Implementing Regulation (EU) 2015/1501[6] and Decisions (EU) 2015/1984[7] and 2015/296[8], defines the conditions, circumstances and procedures in which states will have to notify its own eID schemes and recognize notified eIDs schemes issued in other European countries in order to make it possible to use an eID of a member state to access the online services of the public administration or private entities in other EU member states.

Indeed, under eIDAS, citizens are granted the right to use their national eID to access public services in other countries.

An eIDAS-Node can either:

1. Request a cross-border authentication: when a Service Provider connected to a national eID scheme encounters a user from another Member State, this request is routed through the eIDAS-Node of the Service Provider's country (the Receiving Member State) to request the cross-border authentication from the eIDAS-Node in the user's country (the Sending Member State), through the eIDAS Connector.

2. Provide a cross-border authentication: the eIDAS-Node in the country of the user (the Sending Member State) requesting to use the service in another country will provide the cross-border authentication. This service of providing a cross border authentication can be operated in two ways:

   a) **eIDAS Proxy Service**: an eIDAS service operated by the Sending Member State and providing personal identification data;
   b) **eIDAS Middleware Service**: an eIDAS Service running Middleware. It also requires a Middleware Service plugin (provided by the Sending Member State) to be integrated into the eIDAS-Node of a Receiving non-Middleware country, operated by the Receiving Member State and providing personal identification data.

Due to the distinction between eIDAS Proxy Services and Middleware Services, there are four different possible combinations in terms of requesting or providing a cross-border authentication.

GRIDS has the intention to use Proxy to Proxy alternative for the interoperability and dialogues between the different eIDAS nodes and Service Providers.

2.1.3.1 ITALY: CIE, SPID and FICEP

Italy, with the European notification of SPID and the CIE, is one of the first country in Europe to have completed the community process of two different digital identity systems. The CIE and SPID are tools that are able to attest the digital identity across the European Union.

CIE

The Electronic Identity Card (CIE) has been notified to the European Commission and to the other member States with the publication in the Official Journal of the European Union C 309 of 13 September 2019, and has been integrated with the eIDAS node, in accordance with the namesake Regulation (EU) no. 910/2014[1].

From a functional point of view, the CIE 3.0 (the number refers to the version of the chip specifications) is a card that allows the verification of physical identity and digital identity, in line with what is necessary for recognition in Europe according to the eIDAS regulation[41].

The most important characteristic of the CIE is the contactless microchip integrated into the document that makes therefore the CIE a unique and secure tool for verifying the identity of the owner and for accessing the online services of public administrations and businesses. The personal and biometric data of the owner (photos and fingerprints) are securely stored inside the microchip, as well as the information that allows them to be identified online, digitally signed by the Ministry of the Interior. These data, with the exception of fingerprints which use is allowed only to the Police forces, can be read by the CIE simply with a computer to which a contactless smartcard reader is connected or with a smartphone equipped with an NFC (Near Field Communication) interface. Biometric verification

[1] Since September 2020, Member States have been obliged to also access their online services with CIE.

algorithms - such as those used at airport automatic gates - allow the cardholder to be linked to the document. The digital signature and other cryptographic security mechanisms make it possible to ascertain the authenticity of the data on the chip.

Thanks to the NFC interface it is possible to use it with smartphones and other terminals of possibility and it complies with the ICAO MRTD security requirements, to which all European identity cards will have to converge in about two years[2].

This application is also present in the Electronic Passport and in the Electronic Residence Permit. Using the same application for the three documents it is possible to exploit the same infrastructure for control, both on the territory and on the Italian or European border. Having the same specification as the passports, in fact, the CIE 3.0 can also be read at the crossings of the external European border.

From a functionality point of view, the "Digital Identity" is implemented by the ECC IAS (European Citizen Card, Identification, Authentication, Signature) application. On the card there is a private key and an X.509 authentication certificate, with the tax code, name and surname of the holder. The certificate is signed by the Certification Authority (CA) of the Ministry of the Interior, present in the lists of certification authorities published by the Authority 'Agency for Digital Italy' (AgID).

Furthermore, in addition to creating a digital identity tool in itself, the CIE can also be used as an authentication token for the other Italian Digital Identity instrument, SPID Level 3 (L3), as it is based on digital certificates and securely stored private keys.

The process of federating the service providers is extremely simple, as the system is presented as a SAML 2 identity server, SPID compatible. The CIE can be used as a tool to support the other Italian digital identity mechanism, SPID: a digital identity tool equivalent to an L3 SPID is thus created in which the link between the natural person, his personal data and digital identity is formed and guaranteed in full security by the State.

SPID

SPID is the is the acronym of Sistema Pubblico di Identità Digitale (Public Service for Digital Identity) and it is a full-digital identity schema defined and audited by the public supervisory body AgID and therefore by the Government.

SPID is based on a federated and collaborative model of private companies. The "digital identity providers" (IdP's) are, in fact, private companies accredited by the AgID for the provision of digital identity services. Citizens and businesses can freely choose their preferred digital identity provider from a market of different solutions, which will certify their identity in online transactions according to different levels of authentication assurance[42].

The first official step of SPID was taken at the end of 2014 with an implementation measure, the decree of the Presidency of the Council of Ministers of 24 October 2014. In mid-2015 the implementing regulations were issued and from 15 September 2015 accreditation began of the Identity Providers to the Agency. The first services have been active since 15 March 2016.

It guarantees all citizens and businesses privacy and a unique and secure access to the digital services of the Public Administration and member companies ('Service Providers') with a single login. SPID ensures the maximum confidentiality of data and is designed to increase transparency on the management of its data and provide services according to the principle of minimum data. The Service Provider cannot store the user data it receives from the IdP and it is absolutely forbidden to track the activities of an individual.

With the establishment of the Public Digital Identity System - SPID, Italy aims to create an electronic identification system that has adequate characteristics so that its use by citizens and businesses is possible even outside the Italian territory and, through which, public administrations - first of all - and

[2] Further specification about ICAO standards and MRTD in the official ICAO documentation[37].

private companies can allow citizens / businesses to access their services through a single digital identity[11].

According to the Code of Digital Administration - CAD (legislative decree) 82/2005, as last amended by Legislative Decree 217/2017, "*the SPID system is constituted as an open set of public and private entities that, after accreditation by the AgID, and identify users to allow them access to networked services*"[10].

SPID is based on three levels of cyber authentication security (Art. 6 DPCM October 24, 2014)[9][42]:

1. Level 1 (Level of Assurance LoA2 of the ISO/IEC DIS 29115 standards) consists in userID and password that guarantee the identity ascertained during the authentication activity with a good degree of reliability. A moderate risk is associated with this level and is compatible with the use of a single-factor authentication system: the credential will therefore be a password of at least 8 characters, to be renewed every 180 days, formulated according to the usual security criteria. This level can be considered applicable in cases where the damage caused by improper use of the digital identity has a low impact on the activities of the citizen / company / administration.
2. Level 2 (Level of Assurance **LoA3** of the ISO/IEC DIS 29115 standards) consists in userID, password + additional authentication factor and guarantees the identity ascertained during the authentication activity with a high degree of reliability. Indeed, in addition to the password, it will be necessary to enter the code coming from a variable key device (so-called One Time Password) which could also be an application on the mobile phone. The operator shall make available two-factor computer authentication systems, not necessarily based on digital certificates, whose private keys are stored on devices meeting the requirements set out in Annex 3 to Directive 1999/93/EC of the European Parliament. This level is associated with a considerable and compatible risk with the use of a two-factor computer authentication system not necessarily based on digital certificates; this level is adequate for all services for which an improper use of digital identity can cause substantial damage.
3. Level 3 (Level of Assurance **LoA4** of the ISO/IEC DIS 29115 standards) consists in userID, password + additional authentication factor based on digital certificates and guarantees the identity ascertained during the authentication activity with a very high degree of reliability. The Operator shall therefore make available two-factor computer authentication systems based on digital certificates, the private keys of which are stored on devices meeting the requirements set out in Annex 3 to Directive1999/93/EC of the European Parliament. A very high risk is associated with this level and is compatible with the use of a two-factor computer authentication system based on digital certificates and custody criteria for private keys on other devices; this is the highest level of guarantee and to be associated with those services that can suffer serious and serious damage for reasons attributable to identity abuse; this level is adequate for all services for which an improper use of the digital identity can cause serious and serious damage.

From 28th February 2021 the use of SPID and CIE is mandatory for any eGov service provided by public administration; the use for privates is optional.

SPID and CIE can be used only to access online services and they are not suitable to initiate a payment, lacking the compliance to PSD2 Directive requirements, especially the so-called “dynamic linking”. With the digital certificate present into CIE there is the possibility to sign documents, generating an eIDAS compliant advanced signature.

CNS

For the sake of completeness, there is a third identity schema that is called CNS – Carta Nazionale dei Servizi (National Service Card). It is an old but still diffused chip-based card that was defined to access online public services, mainly health-related (i.e Patient Record). CNS can be issued only by public administrations, eventually outsourcing technical activities to a Certification Authority, and contains a digital certificate that can be unlocked using a PIN code. The use of CNS is still considered valid to access online services.

FICEP

FICEP is the first Italian cross-border server whose implementation allows the circularity of (Italian) digital identities among all member states of the European Union[12]. The Agenzia per l'Italia Digitale (AgID), together with the University Politecnico di Torino and the telecomunication company Telecom Italia S.p.A., has received the was commissioned to build the Italian eIDAS node[3].

The main objective is the interoperability of national electronic identity solutions and therefore to allow citizens to interact with online service providers across European borders by adopting their own electronic identity, issued by a qualified entity of their state[4]. Thanks to FICEP project Italian citizens are allowed to access the online services of other EU countries, using the credentials obtained in the public system SPID digital identity, as well as with the Electronic Identity Card (CIE). At the same time, European citizens in possession of national digital identities recognized in the eIDAS environment, can access the services of Italian public administrations. Indeed, since 29 September 2018, all public administrations that offer digital services through SPID or CIE make these services accessible to European citizens with digital identity (eID) recognized in the eIDAS environment.

FICEP aims to design and develop an architecture for interconnecting the eIDAS and SPID platforms, based on components, named SP Proxy and IdP Proxy, that should expose different interfaces in both domains and handle mapping of messages through certain translation rules. Interfaces follows requirements in both eIDAS and SPID communication protocols, based on different profiles of SAML 2.0 language[5].

2.1.3.2 SPAIN: DNIe and Cl@ve

DNIe

In 2005 is regulated the use of DNIe (electronic Identity National Document) and e-Signing certificates[14]. DNIe started to be issued in March 2006 by the Spanish police. This eID card contains a chip where the citizen personal identification data and electronic signature certificates are included. This technology allows the Spanish citizen accessing online public services by using their eID, and also digitally sign documents. At the end of 2015 this type of DNIe stopped to be issued. Currently two versions of the DNIe coexist DNIe and DNI 3.0.

DNI 3.0

From December 2015 the Spanish police issue the DNI 3.0[14], which provides a higher level of security and improving the user experience. The new one eID card includes the Near Field Communication technology (NFC). This allows to citizens the access to online services by using the DNI 3.0 on smart devices.

Online services and Cl@ve

According to the EU eIDAS regulation on the access of the European citizens to online services provided by public bodies[16], the Spanish government launched the Spanish eIDAS node on December 2016[17] allowing Spanish citizens and business companies accessing online services provided by the Spanish general administration, by the Autonomous communities of Spain, and by the local authorities. Additionally, allows a cross-border access to online services in other EU countries, through the eIDAS

[3] See the public announcement CEF-Telecom eID 2014 call.

[4] An implementation of eIDAS requirements has been developed under CEF eID program, which is strongly bound to the technical outcomes of research projects STORK and STORK 2.0[13].

[5] Translation functionalities should be designed in form of a shared software library, in order to simplify management of mappings during development phase.

network. The Spanish eIDAS node allows the interoperability needed for connecting the Spanish identity provider systems with the eIDAS network and the recognition of the eID issued by other EU Member States[15].

The Spanish eIDAS node is developed based on the eID building block provided by the Connecting Europe Facility (CEF) and following the standard SAML 2.0[15].

The integration of the public administrations with the Spanish eIDAS node is done through the Cl@ve[18] platform. The purpose of this platform is providing identification and electronic authentication by using concerted keys (user and password) for accessing public online services. Also, allows electronic signature. Cl@ve allows public administration applications to define the LoA needed during the authentication process, depending on the data to be managed and level of security for accessing the service. Besides the use of concerted keys, Cl@ve also allows the use of DNIe[19]. The use of concerted keys and cloud signing services offered by Cl@ve requires the citizen being register previously by in-person or online (using DNIe) sign-up [15].

The integration of private sector with the Spanish eIDAS node is not yet agreed. In some cases, under the umbrella of EU ENISA granted projects the integration has been made directly to the Spanish eIDAS node (e.g. LEPS[20] project), but how the private sector will be integrated to the eIDAS network is yet under study. Although different approaches can be followed (integration through Cl@ve or directly) and the technical solutions have been tested in pre-production environment, a political decision on this matter waits. Figure 1 shows the alternatives for integrating public and private sector online services with the Spanish eIDAS node.

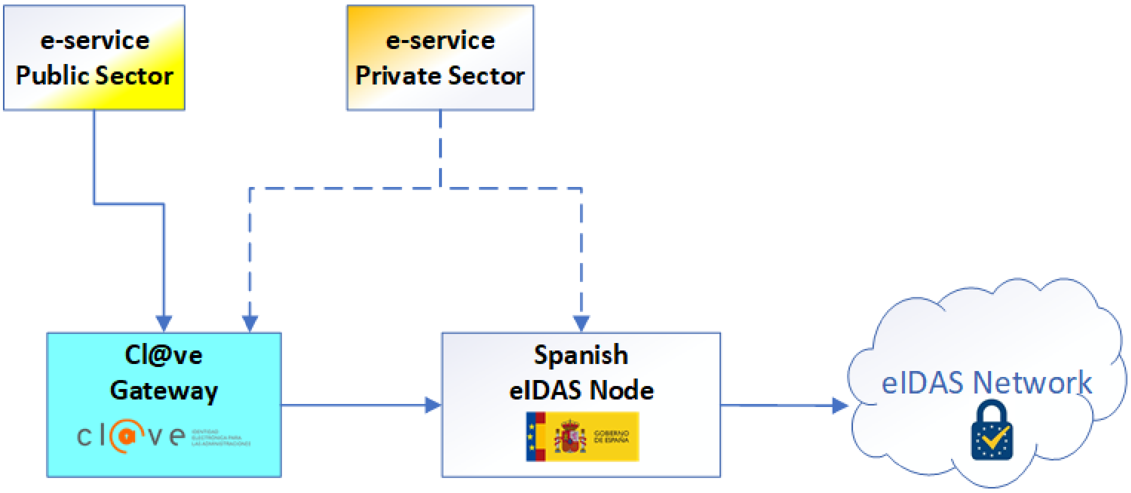


Figure 1: Integration of public and private sector e-services with the Spanish eIDAS node

The uptake of DNIe for accessing online services provided by the private sector is still low. Several initiatives have been developed during the last years for increasing its use, involving banks, financial institutions, postal services, insurance companies and telecoms in Spain. Table 1 provides some examples of projects successfully integrated Spanish eIDAS node with online private and public services in Spain.

Table 2: Projects integrating Spanish eIDAS node with private and public services

PROJECT	DESCRIPTION	DOMAIN
LEPS	Integration of Correos (the Spanish postal service) in pre-production environment. A mobile application for using DNIe 3.0 were implemented and tested.	Postal service

eID4Spain[21]	Integration of online public e-services provided by 4 Spanish local and regional administrations to the Spanish eIDAS node through CL@VE 2.0.	Public services

The following projects are integration examples of country eIDAS nodes with online services provided by the private sector in Europe.

Table 3: Projects integrating EU eIDAS node with private services

PROJECT	DESCRIPTION	DOMAIN
eIDAS2Business: Making Private businesses benefit from eIDAS[22]	Integrates private and public on-line service providers in Portugal to the Portuguese eIDAS node, for authentication purposes. The public AMA Autenticação.Gov portal and the private Oney banking and insurance services.	Banking and insurance
Opening a bank account with an EU digital identity[23]	A UK bank accepts the use of a French eID for opening a bank account in an online process. Integrates the French eIDAS node and use Mobile Connect standard for authentication through the mobile phone.	Banking sector

2.1.3.3 GREECE: GR eIDAS Node (HMAR)

Greece is part of the eIDAS network in both production and pre-production environments. Specifically, in Greece two eIDAS nodes are deployed (one for each environment) running version 1.4.3[24]. These nodes are maintained by the Greek Ministry of Digital Governance[25]. Currently any Service Provider is able to connect to both nodes after sending an official request to the competent authority and having it approved. However, since Greece does not have a notified eID scheme yet, connectivity at a production level, with other member state eIDAS nodes, is limited. Specifically, the lack of a notified eID scheme in Greece results in the situation that although citizens from any third-party MS connected to the Greek node can authenticate to any SP service connected to it, Greek citizens are unable to authenticate to SP service connected to other MSes eIDAS nodes (at a production level). The connectivity of the Greek eIDAS node in production and pre-production can be seen in the table below.

Table 4: Greek eIDAS interconnected counties

Pre-production
Belgium BE
Cyprus CY
Czech Republic CZ
Ireland IE
Italy IT
Lithuania LT
Luxembourg LU
Malta MT
Norway NO
Poland PL

Portugal PT
Slovakia SK
Slovenia SI
Spain ES
Production
Estonia EE
Germany DE
Italy IT
Lithuania LT
Luxembourg LU
Portugal PT
Slovakia SK

Finally, we must note that the Greek eIDAS strategy is being revisited as part of the creation of a national eID scheme. Thus, it is expected that in the near future the connectivity of the Greek eIDAS node will improve significantly.

2.1.3.4 AUSTRIA: Citizen Identity card and Mobile Signature

eIDAS has been implemented in Austria via two alternative forms of the so-called citizen card (Bürgerkarte) functionality:

- **Mobile Phone Signature:** This requires a ready-to-receive mobile phone. The mobile phone signature works with all mobile phones and is free of charge.
- **Smart card:** This requires a smart card with activated citizen card functionality (e.g. A-Trust cards, for the health insurance card only until end of 2019) and a smart-card reading device.

Both alternatives can be used for the creation of legally valid signatures in online procedures. These signatures are legally equivalent to handwritten signatures. This way, the mobile phone and an activated e-card become an Austrian citizen’s virtual ID, which can be used quite similar to a driving license. A user has also the possibility to sign documents or invoices electronically with his/her/its mobile phone signature or citizen card.

The central eIDAS node of the Republic of Austria enables EU citizens to log in to Austrian online applications with the electronic identity (eID) of their EU country of origin. The mutual recognition of national eIDs is taking place gradually in the EU. The Austrian procedure works as follows:

EU citizens will be redirected to the central eIDAS node of the Republic of Austria, provided by the Austrian Federal Ministry of Internal Affairs, if they have initiated a registration in an Austrian online application by clicking on "EU-Login". The further procedure is as follows:

1. An EU citizen selects a Member State.
2. He/she is then redirected to the usual login environment of the respective Member State.
3. There she/he can log in with her/his eID as usual.
4. After successfully logging in, the person is automatically redirected to the online application (from which he/she reached this selection page) and logged in there with the identity data of his/her eID.
5. At the same time, the EU citizen will be entered in the Austrian Supplementary Register for Natural Persons (*ErgänzungsregisterfürnatürlichePersonen* - ERnP) with his/her eID data the first time he/she logs in this way.

This means that he/she can also be successfully and uniquely identified in the context of future registration processes for Austrian online applications.

2.1.4 Interoperability of the Nodes (so-called eIDAS Network)

The European Interoperability Framework [29] (EIF) defines interoperability as:

"The ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems."[27]

With the aim of creating the EU single digital market, the setting-up of interoperable public services facilitates to EU citizens the cross-border use of online services, managed by public service providers. In this context, the eIDAS regulation is included under the umbrella of an interoperability framework where eligible trust services assure the user privacy, the authenticity and integrity of the shared data, and finally the confidentiality of the data for being compliant with the EU General Data Protection Regulation (GDPR)[26].

These basic requirements applying to connected systems working in an easy and effective way for sharing information, are integrated by the Implementation Act[6] regarding the eIDAS regulation[3]. They have been taken into consideration for delivering the last version of eIDAS Interoperability architecture specifications[28]. For fulfilling these requirements, the eIDAS network must provide the next:

- Preserve the user data privacy;
- Keep the authenticity/integrity of the user's data;
- Guarantee the confidentiality of the user's data;
- Assure secure communication channels during the identification/authentication process.

In 2013 the EU launched the Connecting Europe Facility (CEF) in Telecom[30] programme. With the aim to create a pan-European infrastructure for interconnecting the MS and facilitate cross-border communication between public administrations, citizens and businesses, the Digital Service Infrastructures (DSI) or building blocks[31] were deployed. Among these building blocks the eID[32] one is the key element provided by the EU for a cross-border eID interoperability to implement an eIDAS-compliant node.

The eIDAS network is based on EU country eIDAS nodes which make interoperability possible, allowing the mutual recognition of notified eID schemes by the EU Member States (MSs) under the eIDAS regulation. The eIDAS nodes are the core element of interoperability easing the connection between the digital services and the national identification systems. Also, it establishes the secure connection with nodes from other MS. In this way, each country eIDAS node allows the acceptance of citizen eID means issued by a sending MS for accessing online services offered by other country, the receiving MS.

The eIDAS node has twofold role, can act as an eIDAS-connector generating cross-border authentication requests, and as eIDAS-service generating cross-border authentication responses.

Figure 2 displays the main actors and eIDAS node components.

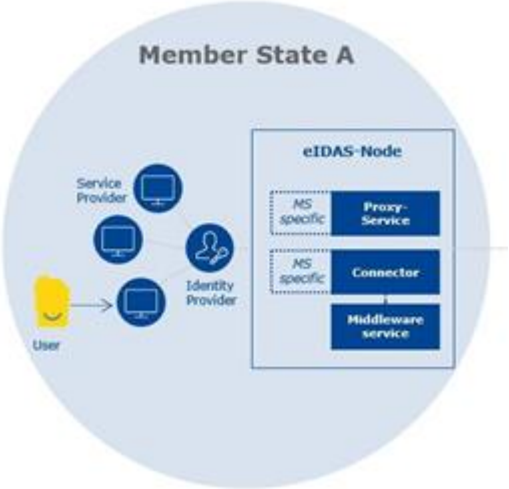


Figure 2: Actors and components of the eIDAS architecture [34]

Figure 3 shows the communication between two MSs through the connection between the eIDAS nodes for cross-border authentication.

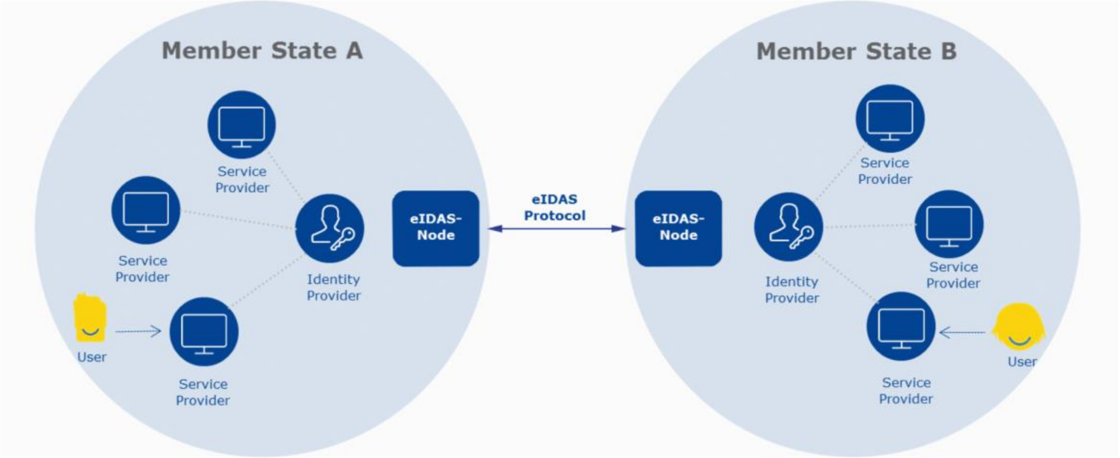


Figure 3: Example of eIDAS network authentication process[34].

The use of a common eIDAS protocol based on SAML and the common interfaces facilitates the connection of the eIDAS nodes of the eIDAS network. This communication enables interoperability between the different MSs, allowing EU citizens the use of their own eIDs to be accepted in other MSs, facilitating the cross-border online operations.

The MSs can develop different approaches for deploying the eIDAS nodes: a centralized approach deploying a single connector or deploying several connectors in a decentralized approach (see Figure 4).

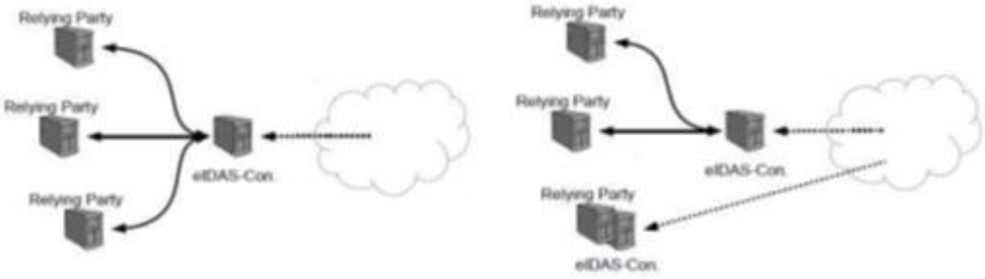


Figure 4: Centralized and decentralized approach[28]

In order to establish a secure connection between the nodes that guarantee the authenticity/integrity, confidentiality of the citizen's data and preserve user privacy, two secure identification schemes can be followed[28]:

- Proxy based scheme: SAML messages are signed and encrypted by certificates, which are exchanged through signed SAML metadata;
- Middleware based scheme: SAML messages are signed and encrypted by certificates, which are exchanged directly between nodes.

Each MS can adopt and develop their own protocols, approach and identification schemes for authentication at country level.

2.1.4.1 Nodes interoperability in GRIDS

Depending on the solution each MS adopt in terms of use a proxy service or a middleware service, the possible alternatives for performing the cross-border authentication are the next[34]:

- Proxy to Proxy[33]: a citizen from a country adopting proxy scheme is accessing a service from a country adopting a proxy scheme;
- Proxy to Middleware[38]: a citizen from a country adopting proxy scheme is accessing a service from a country adopting a middleware scheme;
- Middleware to Proxy[39]: a citizen from a country adopting middleware scheme is accessing a service from a country adopting a proxy scheme;
- Middleware to Middleware[40]; a citizen from a country adopting middleware scheme is accessing a service from a country adopting a middleware scheme.

The solution GRIDS followed is the Proxy to Proxy alternative. The selection of this eIDAS node interoperability solution is based on Greek eIDAS proxy node availability for testing the interoperability between countries such as Spain, Italy, Greece and other MS whose eIDS-node proxy service is up and running and whose eID schemes were notified under eIDAS.

Figure 5 depicts the authentication process when a citizen from the MS accesses a digital service in MS A (both MSs are implementing a proxy scheme-based country node).

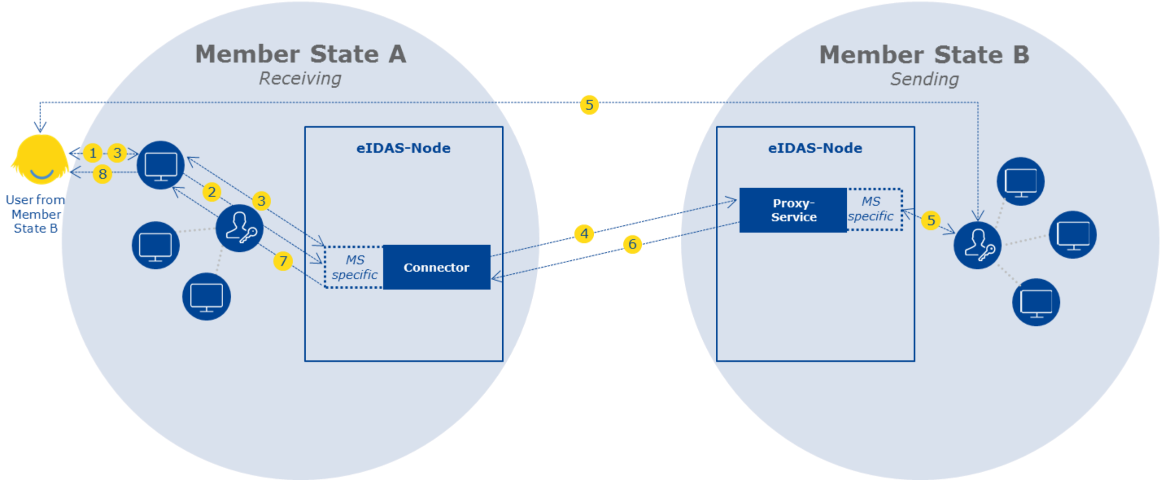


Figure 5: Example of eIDAS network authentication process[33]

A description of the steps indicated in Figure 5 is provided next[33]:

1. A user from Member State B requests access to an online service in Member State A;
2. The Service Provider in Member State A sends a request to authenticate the user;

3. The eIDAS-Connector asks the user for their country of nationality;
4. An eIDAS Request is created by the Connector and then sent to the eIDAS-Proxy-Service in Member State B;
5. The eIDAS-Proxy-Service translates the eIDAS Request into a request for the Identity Provider in Member State B. The user authenticates using their national electronic identity. Once the user is authenticated, their identity is returned to the eIDAS-Proxy-Service in Member State B;
6. The eIDAS-Proxy-Service in Member State B creates the eIDAS Response, containing the Identity Assertion, and sends it to the requesting eIDAS-Connector in Member State A;
7. The eIDAS-Connector in Member State A uses the eIDAS Response to create the reply to the Service Provider;
8. The Service Provider grants access to the user if the authentication is successful.

Figure 6 depicts how this generic authentication scenario is customized to GRIDS project including the specific actors participating in this process:

- Greek/Italian/Spanish citizens
- 360kompany is the Austrian Service Provider (SP)
- Greek eIDAS proxy node
- SP Hub connecting the SP with the Greek eIDAS proxy node
- Spanish/Italian receiving eIDAS proxy node

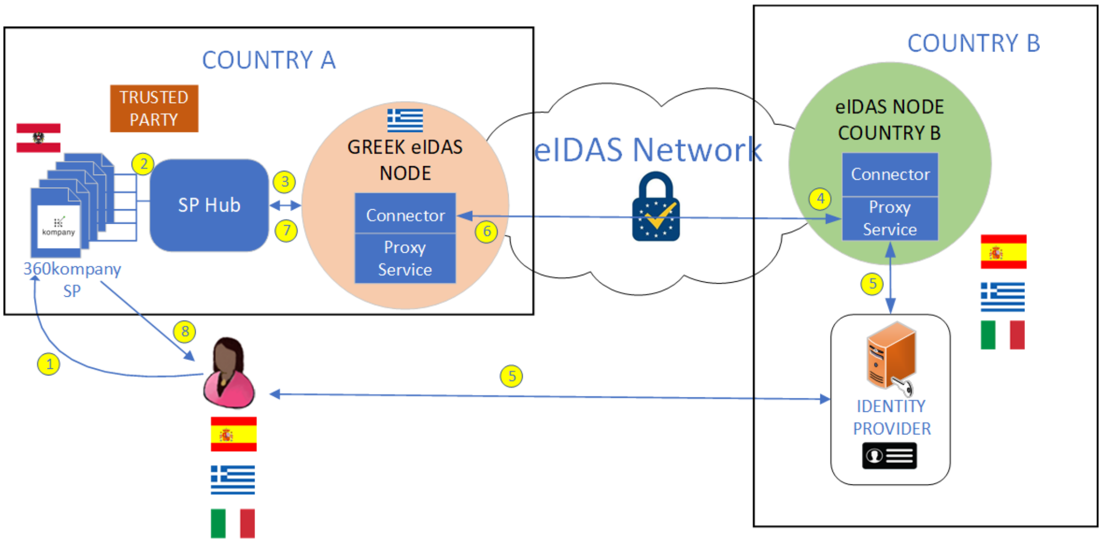


Figure 6: GRIDS authentication process

2.1.5 Can eID nodes be used in private sector?

The governance of the connection of private sector Service Providers (SP) to the nodes of the eIDAS network is not EU regulated. As a result, each member state defines its own national policy on the subject. In Greece private sector Service Providers can freely connect to the national eIDAS nodes (in the production and pre-production environments) after submitting the appropriate requests. A definitive list of which countries support the connection of private sector SPs to their national eIDAS nodes is not available. This is due to the fact that although in some countries there exist no explicit prohibition of such connections, in practice private sector SPs are rarely accepted to the eIDAS nodes. Thus, the overall assessment is that in most countries private sector SPs are not permitted to connect to the eIDAS nodes.

2.1.6 Mobile Authentication and trends in electronic identification

8 Member States provide citizens with NFC-enabled identity cards (Estonia, Germany, Hungary, Italy, Luxembourg, Malta, Poland, Spain) while others have mobile solutions based on other technologies like Bluetooth or SIM Cards (Czech Republic, Austria, Finland, Estonia, Belgium, Portugal, Denmark).

The use of eID for accessing digital services or performing online transaction in a cross-border way is being increasingly adopted across the world. There are several technologies involved in the identification and authentication increasing the security, privacy and the user experience. Technologies related with biometrics, smart cards supporting NFC, mobile apps and authentication protocols and frameworks such as OpenID Connect, OAuth 2.0, SAML or FIDO UAF/U2F, among others has been compiled and reported by the World Bank Group report[43]. The European Commission consider the eID as one of the main elements for assuring secure access to online services and performing electronic transactions[44]. The extended use of mobile devices drove the EU to adopt the use of mobile phone as a second factor authentication for increasing the security, e.g. for accessing to Eurostat microdata application system[45]. But the digital transformation and the fact that the digital world is becoming mobile, implies the citizens are expecting an improved user experience and be in control of their identity, which mean that mobile eID solutions for accessing public services must be implemented. With this objective 18 countries issued eID smart cards with a chip, and nine of them including NFC technology which facilitates the use of these eID means through the mobile phones[46]. Currently some of the notified eID schemes in 2020 support the use of mobile eID[48]. Namely the Denmark' NemID[49] allows Danish citizens to access online public and private services (e.g. online payment or banking services among others, the Netherland's DigiD[50] allows Dutch citizens get access to more than 650 digital services through the mobile app, and the Portugal's Chave Móvel digital[51] mobile eID scheme which allows the Portuguese citizens to access both private and public digital services [46].

Spanish case

In the context of the LEPS[20] project a mobile app were developed by University of Murcia in order to facilitate to Spanish citizens the access to the Spanish eIDAS node for authentication and registration purposes on the Correos (Spanish postal service) online services. The mobile app is a service provider agnostic, allowing eIDAS authentication for Spanish citizens on any Spanish service provider. The LEPS mobile app supports NFC technology in order to use the DNIe 3.0[52] issued by Spanish government. Technically, the LEPS mobile app was developed for Android platforms based on libraries provided by the Spanish Economy and Digital Transformation Ministry and the Spanish National Police. "The DNIDroid library has been adapted to be use as an external library. This middleware existed previously for the use in Java of the DNIe versions with contacts. And now it has been adapted for its proper functioning in Android and the contactless interface via NFC"[47].

From that time the Spanish government has launched several mobile apps[53] for accessing different public services such as DGT (Spanish General Directorate of Traffic), Spanish Welfare and Health, tax office or municipality services, among others.

Estonia case

Estonia is one of the most digitised European countries and one of the most advanced in terms of the implementation of eID solutions, credited by the International Telecommunications Union (ITU) as having "by far the most highly-developed national ID card system in the world".

Estonia uses multiple eID means issued by the public and private sector (mostly by banks). The most popular are following 7 eID means (the first six of which are state-owned and have been notified (all of them LoA "high") and 1 private eID mean which has not been notified). All means are issued only to a natural person. The means are as follows:

1. ID card

2. Digital ID

3. e-Resident’s digital ID

4. Mobile-ID

5. Diplomatic identity card

6. Residents permit card

7. Smart ID

Estonia have introduced digital identity solutions based on SIM cards. The Estonian Mobile-ID solution can be requested by the holders of an Estonian ID card or Estonian residence permit card from a telecom operator. The SIM card used for this solution is not a regular SIM card. It also includes a secure element on which sensitive information is stored. Identity information is derived from the eID card already in possession of the citizen and checked against the country’s identity database. A specific application, independent of the telecom operators, must be used in order to make use of the mobile identity to access eGovernment website and applications.

Mobile-ID allows people to use a mobile phone as a form of secure digital ID. Like the ID-card, it can be used to access secure e-services and digitally sign documents, but has the added advantage of not requiring a card reader.

Mobile-ID is a SIM card-based electronic personal identification service that allows end-users to access e-services, give digital signatures, and otherwise authenticate themselves through electronic channels. Private keys are stored on the mobile SIM card along with a small application delivering the authentication and signature functions.

The system is based on a special mobile SIM card with mobile-ID support, which the customer must request from the mobile phone operator. Each operator has their own rules about issuing mobile-IDs, such as age limits, service fees, user terms and conditions, etc. However, all mobile operators must follow the same national requirements, so mobile-ID is a safe solution and works the same way irrespective of the operator.

Three codes are needed for using mobile-ID which are under the disposable surface of the SIM card cover:

- mobile-ID PIN1 code – for identification or logging in
- mobile-ID PIN2 code – for giving digital signatures or confirming activities
- mobile-ID PUK code – for reopening locked PIN codes

Upon installing a mobile-ID supported SIM card, a mobile-ID menu will be added to the phone. This enables all activities related to mobile-ID, such as change PIN and PUK codes.

Italian case

The DigiMat shared laboratory, born from the collaboration between the Poligrafico and the Bruno Kessler Foundation (FBK) of Trento, has identified a catalogue of solutions for the identification and authentication of users of online services based on CIE 3.0, especially in the mobile field[41].

To the eIDAS scenario mentioned in the chapter 2.1.3.1 of this document, several others are added, such as:

- CIE as a second authentication factor on mobile: in the presence of credentials already assigned to a user in the context of an organization, the ID card can be used to generate a One Time Password (OTP) through a challenge-response mechanism based on its capabilities cryptographic. A possible application, tested within FBK, is to "virtualize" the badges of an organization: there is no longer a need to create a physical object to stamp, it is sufficient to make an application available that uses the tax code to connect the credentials provided by the company to the CIE certificate.

- CIE for desktop and mobile authentication: although Internet content is increasingly consumed via mobile, there are some cases in which the interaction takes place from the desktop. In these cases, the smartphone can be used as an NFC reader "connected" to the desktop through a push-notification mechanism that invokes an application capable of interacting with the CIE. A possible application is to be able to access the services of the Public Administration which, in some situations (for example, think about enrolling children in school), require the entry of a lot of data from the keyboard, an inconvenient operation from a smartphone.
- Digital on-boarding: a process of fundamental importance for market success in the banking and fintech sector in which there is a strong push towards the digitalization of services, in order to offer customers increasingly targeted and personal offers. The CIE can play an important role in the certain recognition and acquisition of data for the signing of a contract.

2.2 Anti-Money Laundering Directives (AMLD4)

The European Union adopted the first anti-money laundering directive in 1990 in order to prevent the misuse of the financial system for the purpose of money laundering. It provides that obliged entities shall apply customer due diligence requirements when entering into a business relationship (i.e. identify and verify the identity of clients, monitor transactions and report suspicious transactions). This legislation has been constantly revised in order to mitigate risks relating to money laundering and terrorist financing.

2.2.1 General intro – EU Directive

In 2015, the EU adopted a modernised regulatory framework encompassing

- Directive (EU) 2015/849 on preventing the use of the financial system for money laundering or terrorist financing (4th anti-money laundering Directive - AMLD4);
- Regulation (EU) 2015/847 on information on the payer accompanying transfers of funds – makes fund transfers more transparent, thereby helping law enforcement authorities to track down terrorists and criminals;
- AMLD4 went into effect 26 June 2017.

On 19 June 2018 the 5th anti-money laundering Directive (Directive (EU) 2018/843), which amended the AMLD4, was published in the Official Journal of the European Union (AMLD5). The member states had to transpose this directive by 10 January 2020. Several member states have achieved this and are at an advanced stage in their implementation, other countries have been encouraged to accelerate their progress and avoid delays and fines.

These amendments introduced improvement to better equip the EU on to prevent the financial system from being used for money laundering and for funding terrorist activities. These amendments were introduced to

- enhance transparency by setting up publicly available registers for companies, trusts and other legal arrangements;
- enhance the powers of EU financial intelligence units (FIU), and provide them with access to broad information for the carrying out of their tasks;
- limit the anonymity related to virtual currencies and wallet providers, but also for pre-paid cards;
- broaden the criteria for the assessment of high-risk third countries and improve the safeguards for financial transactions to and from such countries;
- set up central bank account registries or retrieval systems in all member states;

- improve the cooperation and enhance of information between anti-money laundering supervisors between them and between them and prudential supervisors and the European Central Bank.

Directive (EU) 2018/1673 standardizes the definition of crime related to terrorism and money laundering in the Member States, as well as the liability and sanctions of the parties involved for such activities. The current deadline for EU member states to implement AMLD6 on a national level is 3 December 2020.

2.2.2 Connection with KYC requirements

While the European AMLD regime is primarily a defence against misuse of the financial system, the AMLD5 already offers some helpful insights for organisations seeking to accelerate a digital onboarding process of their customers and reduce customer friction.

One of the core obligations of EU AML/CTF regime is the identification and verification of customers and ultimate beneficial owner (UBO) information. The AMLD4 required companies to create and maintain an internal record of their beneficial ownership. Pursuant to AMLD5 entities must declare relevant UBOs to the centralized national UBO register.

The information obtained on UBOs has to be adequate, accurate and current. This emphasis on the "currency" of data and providing up-to-date information is a key aspect of the AMLD5. Further, the regulatory expectation rises in relation to the use of primary source information. The verification of companies must be based on documents, data or information obtained from a reliable source which is independent from the customer. The most reliable source of this date, in a legal and evidential context, is the lawful source of that information (e.g. formal public registers, official records pursuant to national commercial and transparency registers; so-called primary sources).

Obliged entities (those businesses who have to follow the EU AMLD regime) have to identify the UBOs of their customers and to take reasonable measures to understand the ownership and control structure of their customer. This is usually a repetitive, multi-layer and cross-border process which requires the obliged entity to collect proof of registration data and excerpts from different national registers. Getting this information globally and efficiently is usually a complex issue, as many different registers need to be accessed with different languages, currencies and formats. Even one jurisdiction may have multiple registers and agencies distributing the corporate data which make such processes very time-consuming for the obliged entities.

Finally, what can arguably be considered the most revolutionary aspect introduced by AMLD5 is that it explicitly allows for eIDAS, the electronic signature standard in the EU. This eliminated the biggest blockers to a full digitisation of the customer on-boarding process for financial institutions. The eIDAS Regulation (EU) 910/2014, on electronic identification, authentication and trust services, aims at making national eID schemes interoperable across Europe in order to facilitate access to online services. eIDAS is primarily designed to tackle identification challenges experienced by digital public services. This means that eIDAS allows citizens to have a European national ID document with which the digital identification, strong authentication of people, and electronic signatures across borders in compliance with the EU AMLD regime is possible.

2.2.3 Some national AML legislations

Table 5: National AML legislations

Country	Action	Natural Person	Legal Person	Summary
Austria	1. Determination of Identity	Necessary information: - first and last name - birth date - place of residence Additional information:[6] - profession, employer - citizenship - country of birth - signature - email address, telephone number, etc	Necessary information: - company name - legal form - country of registration - registration number (if available) - registered office - from the authorized representatives (natural persons): first and last name, birth date and place of residence Additional information:[7] - VAT number - Group structure - email address, telephone number, etc	In general and theory, GRIDS meets the requirements defined by the Austrian supervisory body (verification via “qualified electronic signature”). However, it requires additional security measure (2nd layer after identification via GRIDS) in the sphere of the Data Consumer (bank) which requires additional efforts on the Data Consumer’s sphere. Currently, GRIDS does not fulfill the requirement of
	2. Verification of Identity	Superior rule: - Physical presentation of official photo ID (see definition of “official photo ID” below - As part of the verification of the information on the identity of the natural person present in person, a comparison must be made between the person depicted on the headshot and the person identifying him/herself.	Verification must be carried out on the basis of conclusive documents which are available in accordance with the legal standard customary in the respective jurisdiction where the legal person is registered. The minimum criteria (to be verified) are:	

[6] Such information is likely be required in order to be able to create a comprehensive KYC profile in accordance with the risk-based approach.

[7] See footnote 2.

		Accepted alternatives to superior rule: - Online identification (e.g., official photo ID in an online/video identification process) - Electronic ID card (requires inter alia an official photo ID including a picture of the person) - Qualified electronic signature* - Registered mail delivery - First payment via reference account * Data Subject makes a legal declaration in the form of a qualified electronic signature pursuant to Article 3(12) of Regulation (EU) 910/2014 (=eID). In addition, the one of the following requirements must be met - If the customer is a legal entity, the registered office of the legal entity must also be the registered office of the central administration and the customer must provide the obliged entity (bank = Data Consumer) with a written declaration to this effect; - If the customer has its registered office or place of residence in a third country, the obliged entity must obtain written confirmation from a credit institution with which the customer has a permanent business relationship that the identity of the customer has been established and verified within the meaning of the FM- GwG and that the business relationship is still ongoing. If the confirming credit institution has its registered office in a third country, credit institutions in this third country must be subject to	- legal existence - company name - legal form - power of representation - registered office	identification via online procedure or as an electronic ID card as the photo of the natural person (= management) would be required from an Austrian supervisory perspective.

		due diligence and safekeeping obligations that correspond to those of the 4th Money Laundering Directive. In addition, credit institutions in this third country must be subject to supervision with regard to compliance with the due diligence and retention obligations, which corresponds to the requirements of Art. 47 and 48 of the 4th Money Laundering Directive.		
	3. Identification of authorized representatives	n.a.	The identity of the authorized representatives (management, officers, etc) has to be determined and verified (see the process for natural persons). Further, the power of representation is to be reviewed.	
Italy	**Action**	**Natural Person**	**Legal Person**	**Summary**
	1. Determination of Identity	As per Art. 1 lett. n) and following of Legislative Decree 231/2007: Necessary information: - first and last name - birth date - place of birth - place of residence and domicile if different than residence - fiscal code Additional information: - profession, employer - citizenship	Necessary information: - company name - legal form - country of registration - fiscal code if available From the **authorized representatives** as per natural persons Necessary and Additional information. From the **Beneficial owner** as per natural persons Necessary and Additional information.	Substantial changes to the Italian AML law occurred with the Simplification Decree 76/2020 (issued during Covid emergency). Regarding identification process, the previous provision that required "the acquisition of the identification data provided by customer, upon presentation of an identity document in progress validity or

		- signature - email address, telephone number, etc - politically exposed persons information	Additional information: - VAT number - ownership and control structure - power of attorney of the legal representative - business registered information (es. Chamber of Commerce deeds) - email address, telephone number, etc	other equivalent identification document pursuant to of current legislation, …", has been deleted. Indeed, from July 2020, the art. 18 makes reference not only to 'documents', but also to 'data or information'. This new formulation leaves room for interpretation: SPID (digital identity notified eIDAS) is included; therefore, no copy of identity documents is needed. Guidelines from BankIT are expected.
	2. Verification of Identity	As per Art. 17, the obliged subjects to the AML legislation (e.i. financial institutions) carry out the due diligence of its customer (natural or legal person) and of the beneficial owner. Superior rule:	The customer supplies, under the own responsibility, the information necessary to allow identification of the beneficial owner. Appropriate risk measures must be adopted and aimed at identifying the effective ownership and	

		- verification of the identity based on documents, data or information obtained from a reliable and independent source (Art. 18). Basic identification method: - In person: presentation of a valid identity document or other equivalent identification document pursuant to of current legislation is required. A copy of such ID documents is taken in paper or electronic. Accepted alternatives to basic method: - Public deeds: identification data result from public deeds or authenticated private documents (art. 19 lett. a), point 1) - **Qualified electronic signature**: for customers whose identification data result by certificates qualifications used for the generation of a digital signature (art. 19 lett. a), point 1 and 2) - **Digital Identity SPID**: for customers in possession of a digital identity, with at least significant level of assurance, as described in the art. 64 of the Digital Administration Code, CAD - d.lgs 82/2005, (art. 19 lett. a), 2) - CIE (presented in remote; personal data and biometric data (photos, fingerprints) are contained in the chip): digital identity with at least a significant level of guarantee, issued under an electronic identification scheme included in the list published by the European	control structure of the customer such as the use of public registers, lists, deeds or documents with public access or requesting all data from the customer necessary to obtain the information useful for determining the actual ownership.	

		Commission pursuant to article 9 of EU regulation no. 910/2014 (2); (art. 19 lett. a), 2) - Online identification (e.g. an online/video identification process): by means of electronic identification procedures safe and regulated or authorized or recognized by the Agency for digital Italy (Agid) (art. 19 lett. a), 2) - Consular declaration: for customers whose identification data result from declaration of the representation and of the consular authority Italian (art. 19 lett. a), 3) - Already known individuals: for customers who have already been identified by the subject obligated in connection with another relationship (art. 19 lett. a), 4) - First payment via reference account (art. 19 lett. a), 4-bis) - Other remote methods any time authorized: for customers whose identification data are acquired through suitable forms and methods, identified by the sector supervisory authorities (art. 19 lett. a), 5)		
	3. Identification of authorized representatives	n.a.	The identity of the authorized representatives (management, officers, etc) has to be determined and verified (see the process for natural persons). Further, the power of representation is to be reviewed.	
Greece	**Action**	**Natural Person**	**Legal Person**	**Summary**

	1. Identity Verification Pursuant to Banking and Credit Committee Decision no. 281/17.03.2009, of Bank of Greece	Law 4557/30.07.2018 as amended by Law 4734/08.10.2020 is the basis of the applicable Greek institutional framework on preventing and combating money laundering and terrorist financing, and incorporates the provisions of Directive (EU) 2015/849 and 2018/843 of the European Parliament and of the Council. - Customer’s details to be checked at least: - Name - Surname - Father’s name - ID Card or Passport Number - Issuing Authority - Date and place of birth - Present home address - Contact telephone number - Occupation and occupation’s address - Tax Identification Number (TIN) - Sample signature If the customer acts through an authorized representative, then his/her identity will be verified, as well as his power to represent that customer.	Customer’s details to be checked at least: - Published Articles of Association - Company name - Registered office - Purpose - Members of the BoD - Legal representative(s) data - Minutes of the General Assembly for the election of the BoD - Minutes of the BoD for the powers granted to the persons representing the company (and can sign in its name) - Other persons’ data who are authorised to handle company affairs	Recent regulatory initiatives in Greece about identity verification performed by financial institutions, e.g. remotely, or through the connection with central databases of the Greek authorities, may pave the way to the application of GRIDS, for example through the connection of Greek banks with the GRIDS platform. Therefore, the GRIDS platform could be a suitable tool for a bank to identify their customers. However, the Bank of Greece would possibly need to further specify the requirements of the GRIDS application, by issuing guidelines to this end.

	2. Customer due diligence through eGov-KYC (Developed by the General Secretariat of Information Systems Ministry of Digital Governance) Pursuant to Ministerial Decision 9747/ 7.4.2021	Banks are connected with Greek tax and police authorities’ registries and accesses natural person’s information automatically. TIN is verified through tax authority (AADE). - ID Card Number is verified through Police Registry and the following data can be extracted online: - Name, Surname, - Father’s name - Mother’s name - Date & place of birth - Date of the ID card’s issuance Photograph - Address - E-mail - Mobile phone number - Landline number - income data, occupation data		
Spain	**Action**	**Natural Person**	**Legal Person**	**Summary**
	1. Determination of Identity	Necessary information: - Name and surnames - Birth date and place - Place of residence - ID: type, number, expire date, signature Additional information: - profession, employer - Nationality - country of birth	Necessary information: - Full Legal Institution Name - Trading name(s) used (if different of the above) - Legal form - Country of registration - Identification Number of Company - Registered office - from the authorized representatives (natural persons): name and surnames, birth date and place of residence	In general and theory, GRIDS meets the requirements defined by the Spanish supervisory body (verification via “qualified electronic signature”). Although currently biometrics or face

		- Contact: email address, telephone number, etc	- Full address of the head office location Additional information: - VAT number Contact: email address, telephone number, etc	recognition is not supported by GRIDS for online onboarding
	2. Verification of Identity	Presential: - Presentation of a valid ID (national ID, residence card, passport) with a picture. - Signature validation Remote: - Online identification (e.g., official photo ID in an online/video identification process, biometric authentication) - Electronic ID card (validated by governmental administration)	Verification must be carried out on the basis of conclusive documents which are available in accordance with the legal standard customary in the respective jurisdiction where the legal person is registered. The minimum criteria (to be verified) are: - legal existence - company name - legal form - power of representation - registered office	

2.2.4 AMLD for GRIDS

The European AMLD regime establishes the following requirements for the GRIDS solution:

In order to provide a compliant solution, the Data Subject is required to be identified via an eIDAS conformant national process. eIDAS-based IDs offer the possibility to provide a strong authentication of users (natural and legal persons), based on ID information endorsed by governmental authorities across Europe. Hence, an identification process in compliance with eIDAS Regulation is required to meet the online identification requirements as laid out in AMLD5.

However, the Data Consumer requires for the verification of its Data Subjects identified in accordance with eIDAS (and, hence, AMLD5) documents, data or information obtained from a reliable source, primary source, which is independent from the respective Data Subject. This also includes the identification of the UBO of such customer. In order to meet these AML requirements, the services from kompany as a Data Provider for GRIDS are required.

The Data Provider kompany is a government clearing house of registers and operates a real-time global register network providing direct access to business data on more than 110 million companies across 200 jurisdictions around the world. This data comes with the highest possible veracity, as it's retrieved straight from its primary source. Further, this data is time stamped and the data integrity is guaranteed, thus meeting the requirements for a true copy of business data.

Data Providers such as kompany are integrated into the GRIDS platform in a manner which enables them to provide extra information above and beyond the information which can be provided and/or validated by the eIDAS platform. The platform allows for Legal and Natural Person data to be passed from the eIDAS result through to data providers, and also for the Data Consumer to request additional information from the data subject in order to meet their KYB requirements. The nature of the information, and the manner in which it is processed is Data Provider dependent. For kompany, requests are company centric, and Natural Persons are only considered within the context of a company. In the event of authentication of a Natural Person with a corporate relationship, e.g. managing director, the Natural Person will be validated through the eIDAS platform, and extra information relating to the company will have to be provided by the Data Subject. This information, along with other information returned by eIDAS can be used by a Data Provider to make a determination as to the authenticity of the company, and the validity of the claim of the Natural Person regarding their rights pertaining to that company. For example, a Data Provider may validate that the company specified does have a managing director with the same name and address as that of the authenticated Natural Person.

The data and company filings (documents) provided by the Data Provider kompany enables the Data Consumer to comply with the AMLD requirements (i.e., identifying and verifying).

2.3 EU Directive no. 2015/2366 on payment services in the internal market (PSD2)

The original Payments Services Directive (PSD) was created in 2007 by the European Commission with the aim to create a single market for payments in the European Economic Area. After ten years, the needs and capabilities of the market had changed so much that it was time for an update on the existing regulations.

2.3.1 General intro – EU Directive

In 2015 the EU adopted a new directive on payment services (Directive (EU) 2015/2366) to improve the existing rules and take new digital payment services into account (PSD 2). It promotes innovative mobile and Internet payment services and ensures a more secure environment for consumers. The directive had to be implemented in national law on 13 January 2018 at the latest. It includes provisions to:

- make it easier and safer to use internet payment services
- better protect consumers against fraud, abuse, and payment problems
- promote innovative mobile and internet payment services
- strengthen consumer rights
- strengthen the role of the European Banking Authority (EBA) to coordinate supervisory authorities and draft technical standards

One of the most important changes for organisations' compliance processes refers to Strong Customer Authentication (SCA), which came into force on 14 September 2019, as stated in the European Banking Authority's Regulatory Technical Standards (RTS). To comply with the SCA rule, payment transactions processed within the EU – excluding a restricted number of exceptions to allow for "frictionless flow" – require the customer's identity to be verified using at least 2 of the following

- something the customer (Data Subject) knows (e.g. Password, Pin)
- something the customer (Data Subject) has (e.g. mobile phone, wearable device, smart card)
- something the customer (Data Subject) is (e.g. fingerprints, facial features, voice pattern)

GRIDS is able to support such methods where the underlying eIDAS network and the jurisdictional infrastructure supports them.

2.3.2 Connection with KYC requirements

In a first step, GRIDS can enable the establishment of contracts of new financial service products during the on-boarding of B2B clients initiated through PSD 2 related services, by providing authentication of both Natural Person representatives and Legal Person (corporate) entities.

In a second step, GRIDS can effectively harmonize SCA for B2B end-clients across different markets to overrule local SCA processes that might only be available to B2B clients in a certain market, but not in another.

2.4 Regulation (EU) 2016/679 (GDPR)

The data protection package adopted in May 2016 ensures same data protection rights across the EU and regardless of where the data is processed. This package includes:

Regulation (EU) 2016/679 (GDPR), and

- Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data.

The directive protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities for law enforcement purposes. It will in particular ensure that the personal data of victims, witnesses, and suspects of crime are duly protected and will facilitate cross-border cooperation in the fight against crime and terrorism. The directive entered into force on 5 May 2016 and EU countries had to transpose it into their national law by 6 May 2018.

2.4.1 General intro – EU Regulation

The Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR). The regulation entered into force on 24 May 2016 and applies since 25 May 2018[26]. Authentication systems and the security requirements associated with them, as a fundamental prerequisite for strengthening consumer security and confidence in online transactions and ensuring that they are protected against the risk of fraud and other abuses.

The GDPR states that the information for a personnel reference must refer to a natural person. Indeed, the law defines Personal data only information[8] relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Therefore, data protection does not apply to information about legal entities such as corporations, foundations and institutions.

Amongst others, GDPR states a lawfulness, fairness and transparency principle that requests businesses to provide individuals with more detailed information in their privacy notices, explaining the legal basis for processing personal data, how they process personal data and when they respond to a data access request [61].

Like the Directive, the GDPR sets out a list of processing conditions (i.e. legal basis), for the processing of personal data. One of these conditions must be satisfied for each processing activity which a business undertakes[9]. The consent is one of the six legal grounds for lawful processing whereby for each data processing activity there needs to be at least one of these six in place [59].

2.4.2 Personal Data in connection with GRIDS process

The functionality of GRIDS requires the sharing of personal data of natural person and data of legal person amongst all parties involved: the DC needs End User information to provide him/her with the requested services, KYC/KYB procedure implies the exchange of such data and, above all, the End User and the Legal entity must identify and authenticate himself/itself with the applicable interface, as eIDAS Nodes.

In order to be in compliant with GDPR in processing of personal data, in GRIDS the consent has been considered the lawful bases for processing personal data.

Article 4 of the GDPR states the definition of consent as an unambiguous indication of a data subject's wishes that, with a clear affirmative action taken by the subject, signifies an agreement by him/her to the processing of his/her personal data [60].

GRIDS covers the consent lifecycle from start to finish: from data collection, presenting the consent in a clear and concise way, using language that is easy to understand, and be clearly distinguishable from other pieces of information such as terms and conditions, including contact details of the company processing the data and enabling data subjects to change or withdraw consent to deleting personal data whenever the purpose and duration of the data to which the data subject consented are finished. The parties involved in GRIDS keep clear records to demonstrate consent.

Furthermore, as the consent must be freely given, specific and informed, the data subject will be provided with a Privacy Notice that clearly specifies all related privacy information as duties and rights with a list of information to be given in the context of transparency. This list includes, in particular, the legal basis for the processing and the data retention period or criteria used to determine same.

Last but not least, in accordance with Article 5 of GDPR, a data controller and processor must ensure the personal data processed is:

- adequate – sufficient to properly fulfil the stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – not hold more than what needed for that purpose.

[8] Since the definition includes "any information," one must assume that the term "personal data" should be as broadly interpreted as possible. In particular, also the special categories of personal data, also known as sensitive personal data, must be considered. These data include genetic, biometric and health data, as well as personal data revealing racial and ethnic origin, political opinions, religious or ideological convictions or trade union membership.

[9] Where sensitive data is processed a separate list of processing conditions applies.

In order to respect the above mentioned data minimization principle and as better described in the chapter 4 of this document, GRIDS approach is collect and record only the amount of personal data needed to fulfil GRIDS purpose (i.e. eIDAS identification procedure) and adopt the base type specified by ISA Core Vocabulary rather than the complex data types required for full compatibility with the standard[54].

The data provided through GRIDS will be a superset of that provided through eIDAS, but will depend on the capabilities of the various Data Providers taking part in the platform. Each DP will be able to provide different data points and different data sets or documents depending on their capabilities, but a subset of data has been defined which covers the most relevant points, including business name, status, address, with documentation to back up that data.

- Based on ISA, the minimum data set for Natural Persons is the following:

Table 6: Minimum data set for Natural Persons

Attribute (Friendly) Name	eIDAS MDS Attribute
FamilyName	Current Family Name
FirstName	Current First Names
DateOfBirth	Date of Birth
PersonIdentifier	Unique Identifier

- The following Optional attributes may be supplied if available and acceptable to national law.

Table 7: Optional attributes for Natural Persons

Attribute (Friendly) Name	eIDAS MDS Attribute
BirthName	First Names at Birth
BirthName	First Names at Birth
PlaceOfBirth	Place of Birth
CurrentAddress	Current Address
Gender	Gender

- Even though GDPR requirements do not apply to Legal Persons, the same data minimization principle is applied to Legal Persons. Minimum data set for Legal Persons is the following:

Table 8: Minimum data set for Legal Persons

Attribute (Friendly) Name	eIDAS MDS Attribute
LegalName	Current Legal Name
LegalPersonIdentifier	Uniquenes Identifier

- The following Optional attributes may be supplied if available and acceptable to national law.

Table 9: Optional attributes for Legal Persons

LegalAddress	Current Address
LegalAddress	Current Address
VATRegistration	VAT Registration Number
TaxReference	Tax Reference Number
BusinessCodes	Directive 2012/17/EU Identifier
LEI	Legal Entity Identifier (LEI)

EORI	Economic Operator Registration and Identification (EORI)
SEED	System for Exchange of Excise Data (SEED)
SIC	Standard Industrial Classification (SIC)

3 High level process implementation (general use case)

In this section the implementation with GRIDS is described and illustrated on a general level. Further, it will be described how GRIDS will work as implemented in the technical-IT architecture. This description will be supported by a process flow which explains the actions of each party involved.

3.1 KYC and verification electronic kompany service

The process concerns the KYC check performed by any Obliged Subject pursuant to AML regulation. KYC check consists in a complete Customer Due Diligence (CDD) verification that includes the following phases:

3.1.1 Identification and Verification

The potential customer of a Data Consumer provides the Data Consumer with the information required in connection with the on-boarding process (information about purpose of business, personal information, etc). One key step in this CDD is the verification of the identification of the Data Subject pursuant to the applicable AML regime:

a. Natural person

Provided that the Data Subject is a natural person, this natural person identifies itself via GRIDS: The Data Subject uses its European national ID document in accordance with eIDAS regulation in order to meet the identification criteria pursuant to AML. Such digital eIDAS identification across borders is in compliance with the EU AMLD regime as outlined in item 2.

b. Legal entity

Firstly, the verification of the identity of a legal entity has to be determined on the basis of conclusive documents which are available in the jurisdiction of the legal entity (i.e., seat). In any event, the verification has to include the status (active/inactive), the name, the legal form, the power of representation and the seat of the legal entity.

Secondly, the natural persons representing the legal entity have to be identified and verified in accordance with the requirements for natural persons (see item a. above).

Thirdly, the identity of the ultimate beneficial owner of the legal entity has to be determined. The Data Consumer has to understand the ownership and control structure of the legal entity and has to know the UBO - Ultimate Beneficial Owners (s).

Note – GRIDS supports single authentication requests for a single subject only. So, if it is required that a Natural Person and a Legal Person validation is required through eIDAS, then two separate calls must be made. However, if the Legal person authentication can take place through the Data Provider mechanism, and appropriate information has been provided by the Data Subject then a single call can be made and the Data Provider can perform the Legal Person authentication.

3.2 Method of identification

The following figure displays the flow for the Identification of the users while interacting with the GRIDS network.

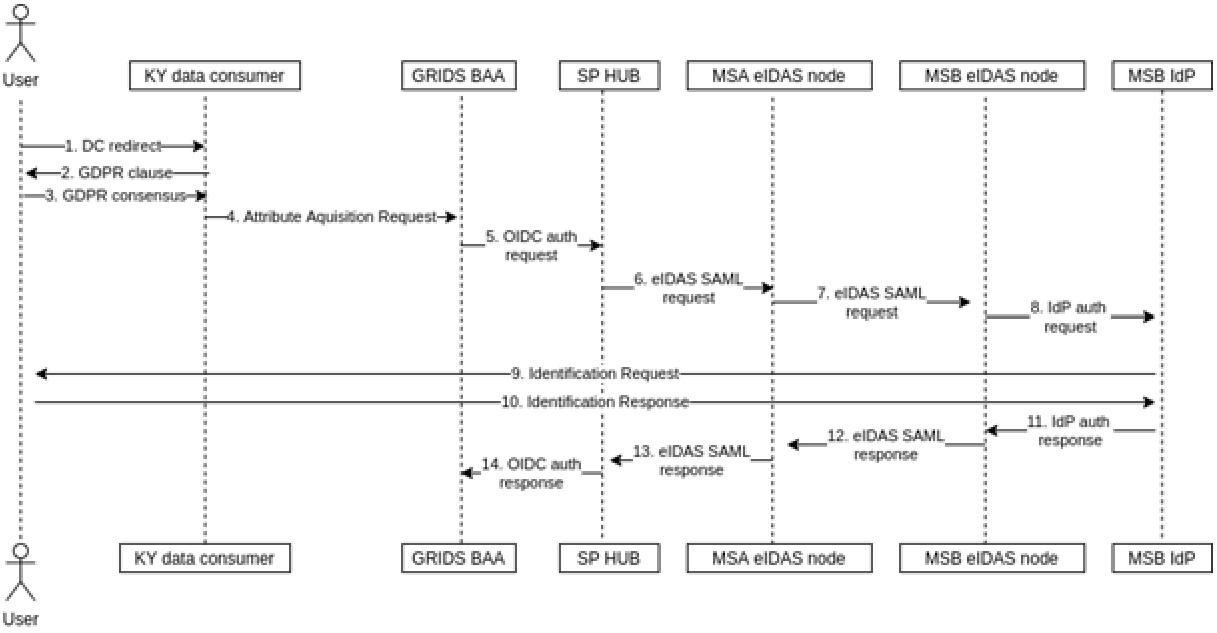


Figure 7: GRIDS network

Specifically, the user accesses a Data Consumer (DC) service, where they are requested to first authenticate. Authentication takes place over eIDAS/eID as follows:

1. The DC contacts the GRIDS BAA service it is connected to, by transmitting an appropriate Identification and KYC attribute acquisition request (steps 1 to 4). This request contains the eIDAS attributes required by the DC according to its business logic. In the simplest of cases these attributes might be limited to the eIDAS Minimum Data Set (MDS), but GRIDS will provide support for all available eIDAS attributes for both Legal and Natural Persons. Of course, the availability of the requested attributes depends on the connected IdPs by each MS.
2. The GRIDS BAA service contacts the SP Hub microservice, which acts as a connector to the eIDAS network, and propagates the DC identification request. The interaction between GRIDS BAA and the SP Hub takes place over the OpenId Connect protocol (OIDC) and the required user attributes are encoded as OIDC client scopes (step 5).
3. The SP Hub receives the request and generates and sends to its connected eIDAS node an appropriate eIDAS SAML authentication request (step 6).
4. The user is redirected to their national eIDAS node and from there to their national IdP where they authenticate using their eID credentials. The response follows the reverse path and is finally received by the SP Hub microservice (steps 7 to 13).
5. The SP Hub microservice validates the response and generates an appropriate OIDC response (encoded as a JWT) and propagates it back to the GRIDS BAA service (step 14).

In the end of the presented flow, for the current DC session the GRIDS BAA service is in possession of the user identification information as those were retrieved from the eIDAS network.

3.3 Parties involved and their actions in points

GRIDS is a business network formed for the needs of managing KYC information. It connects due diligence DPs providing KYC claims for consumption by DCs, as regards their clients or User DSs. GRIDS partners share Users' eIDAS eID information obtained through a single User authentication point, i.e. an SP hub acting as Relying Party for the eIDAS Network.

We can identify six main actors of which the main actions are described below: End User, KYC Data Consumer, Data Providers, Business Attribute Aggregator, Service Provider Hub, eIDAS Network and related nodes.

- **End user or Data Subject ('DS'):** is a natural person, including natural person that represents a legal entity, and a legal entity that is seeking a service (e.g. a citizen):
- clicks on Data Consumer website
- reads the Privacy policy and gives its consent for the treatment of personal data
- provides all information, including personal data, required for the chosen service
- authenticates itself, and possibly the legal person identity that he/she represents if supported over eIDAS (only available in Netherlands at present), through authentication eIDAS node entering its credentials
- receives the outcome of the process
- proceeds with the purchase of the choose service
- **Data Consumer ('DC'):** is a legal entity that offers a service to Data Subject (e.g. a Bank):
- receives the DS's request of service
- requests for and receives DS's information, including personal data
- provides the DS terms and conditions of the chosen service and the related privacy policy
- sends to the BAA the request of a service catalogue applicable to the chosen service
- selects the KYC and eIDAS authentication node that meet its needs (depending whether natural or legal persons)
- sends the request for a KYC information and checks
- sends the request for eIDAS authentication
- redirects the DS to the BAA for the eIDAS authentication
- receives all requested information through a token
- using the token and included information requests for a check to the appropriate DP
- informs the DS about the outcome of the KYC and eIDAS authentication
- if a positive result, provides the DS with the chosen service
- **BAA – GRIDS Player:** is the Business Attribute Aggregator and facilitate the gathering of KYC and eIDAS information:
- receives the DC's request of service catalogue of information
- sends the matching entries in the product catalogue to the DC
- receives the DC's request for KYC information and eIDAS authentication
- redirects the DS to the applicable Service Provider HUB for the eIDAS authentication, connecting into the GRIDS network through the SPhub, to authenticate the End User and generate an authentication token
- redirects the request to each DPs as appropriate, with required information from the authentication token

- receives DP's results to pass back to the DC
- aggregates the KYC and eIDAS authentication in a token
- sends the token to the DC

- **Data Provider:** is the entity or system that provides with KYC information (e.g. companies / commercial / transparency registers, a third party provider like 360kompany AG having direct access to these primary sources)

- receives the DC and BAA request of information
- provides the requested KYC information to the DC and BAA
- validates the token and responds

- **Service Provider HUB:** is the entity the provides eIDAS authentication tool

- Receives the BAA's authentication request
- Sends the authentication request to the eIDAS network

- **eIDAS Network/node:** is the eIDAS system that allows interoperability through the applicable national eIDAS node (notified as per eIDAS Regulation); the latter allows DS authentication:

- receives the authentication request from the SPHub
- forwards the requests to the DS's domestic eIDAS Node
- the domestic End User's eIDAS Node requests to the DS for Privacy data processing consent and requests for DS's credentials
- authenticates the DS
- sends the results back to the SPHub and BAA

3.4 Description of the process

The process flows are more fully defined in the appropriate architecture diagrams in the dedicated chapters. However, here are described the high-level steps in the GRIDS framework. A typical GRIDS flow would progress along these lines:

Login of End User: the User will register / login to the DC's systems as per however they require them to do so. This will vary depending on the DC and the service that the DC provides.

Registration/On boarding: the End user will be expected to provide information that the DC will need to be able to meet both their internal systems and business requirements and the requirements under appropriate legislation. In this context, the user will also be expected to authenticate themselves using GRIDS and therefore to permit their data to be passed onto one or more DPs as per GDPR.

GDPR control and consent: the End user will grant permission and provide appropriate information for themselves to be authenticated via GRIDS. Furthermore, the End user will allow the information, or a subset of such, to be passed to DPs to meet the legal and business needs of the DC.

BAA intermediation: the BAA is the interface point for DC's. It will act as a proxy for authentication token requests to the SPHub and GRIDS infrastructure and also for KYC checks towards the DP's.

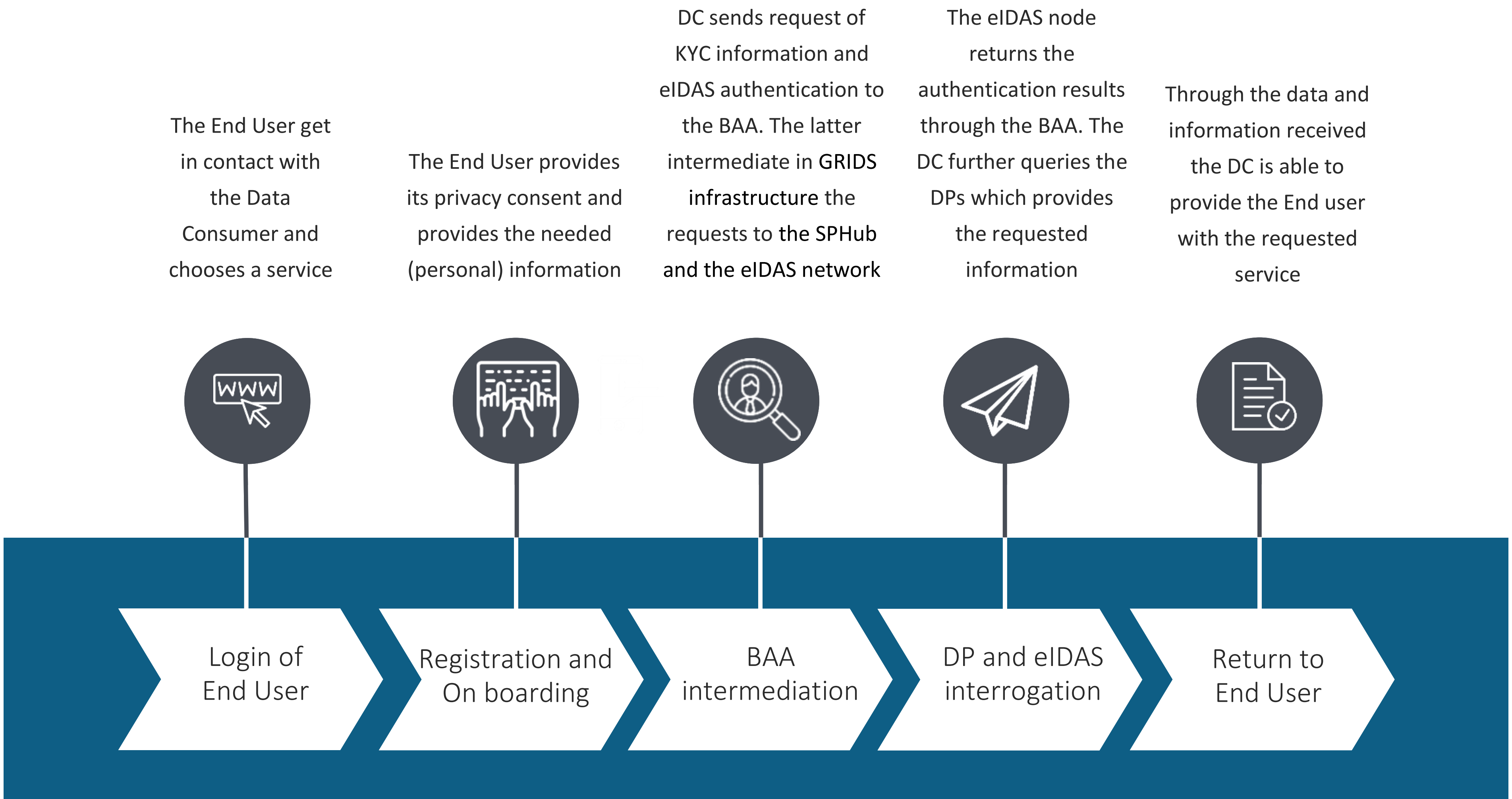
eIDAS interrogation: the BAA will forward eID identification request to the eIDAS network and the latter will interrogate the relevant eIDAS node; the node returns the identification data to the BAA which will pass back to the DC the authentication information/token.

Return to End user: t the DC queries the DPs and in this way the DC will be able to provide the service to the End User.

3.5 Diagram of the flow

The main steps of the GRID process are explained in the below diagram.

Figure 8: Diagram of the flow



The End User get in contact with the Data Consumer and chooses a service

The End User provides its privacy consent and provides the needed (personal) information

DC sends request of KYC information and eIDAS authentication to the BAA. The latter intermediate in GRIDS infrastructure the requests to the SPHub and the eIDAS network

The eIDAS node returns the authentication results through the BAA. The DC further queries the DPs which provides the requested information

Through the data and information received the DC is able to provide the End user with the requested service

4 Technical Architecture

The purpose of this section is to detail the GRIDS Business Attribute Aggregator (BAA) high level design. The BAA enables the authentication of natural and legal persons over eIDAS and uses this assured identity data in the further collection of Know Your Customer (KYC) & Know Your Business (KYB) claims from Data Providers, that are connected over the GRIDS BAA.

4.1 KYC

Customer diligence or KYC (Know Your Customer) is a critical procedure for financial institutions so to reliably identify customers and to assess their financial risk. In addition, it is a legal obligation at global and European level in order to fight against money laundering, terrorism financing (LCB-FT) and financial fraud.

4.1.1 General Criteria

In order to assess the risk of money laundering and financing terrorism recipients consider the general criteria under the anti-money laundering decree[55], which refer to the characteristics of the customer, his conduct and the specifics of the operation or ongoing relationship.

In identifying the risk factors inherent to a client (data subject), the recipients (corporations or financial institutions also data consumer) also consider the actual holder and, where relevant, the executor. Recipients assess the scope of activity and characteristics of the client, the actual holder and, where relevant, the performer, as well as the country or geographical area in which they have their headquarters or residence or domicile or from which the funds come; they also note the location of the activity carried out and the countries with which the actual client or owner and, where relevant, the executor have significant links. The importance of risk factors related to the country or geographical area varies in relation to the type of ongoing or transaction relationship.

Recipients consider the behaviour of the customer or performer when opening continuous reports or performing operations.

In the case of a client other than a physical person, the recipients consider the purpose of its constitution, the purposes it pursues, the way it works to achieve them, as well as the legal form adopted, especially if it contains particular elements of complexity or opacity.

Recipients check whether the client and the actual owner are included in the "lists" of persons and entities associated with terrorist financing activities adopted by the European Commission.

Recipients also use, as aid tools, the anomaly indicators and communications on the prevention of terrorism financing published by the AML directive.

4.1.2 Information sources useful for risk assessment and customer profiling

Recipients draw information for the identification of the risk profile of customers from every source and useful documents, including: the report adopted by the European Commission under Article 6[55] of the Anti-Money Laundering Directive (aka. Supranational Risk Assessment Report); the report adopted by the Financial Security Committee under Article 14[55] of the Anti-Money Laundering Decree containing the 'National Risk Analysis'.

Recipients define the risk profile attributable to each customer, based on the overall assessment elements and risk factors, that are weighted on the basis of their relative importance. As a result of profiling, each customer is included in one of the predefined risk classes by the recipients.

Risk profile processing is based, as far as possible, on computer algorithms and procedures. Recipients ensure that the risk class automatically proposed by computer systems is consistent with their customer knowledge, applying, where appropriate, higher risk classes.

If the computer system is provided by external parties, the recipients are adequately aware of the operation of the system and the criteria that determine the attribution of the risk class.

For recipients belonging to a group, when the customer's profiling is not centralized, it is also carried out by the individual companies on the basis of the information used by the other companies in the group. Each company assumes, for the same customer, the highest risk profile among those assigned by all companies in the group. When a company varies, a customer's risk class the company communicates it to the other companies concerned.

For each risk class, the recipients associate a consistent level of depth and extent of the measures taken in the different areas of the appropriate verification.

In relation to ongoing reports, recipients define the frequency of updating the customer's profiling in line with its level of risk. Recipients check the appropriateness of the risk class assigned to the use of events or circumstances that are likely to change the risk profile.

4.1.3 Information sources useful for risk assessment and customer profiling

4.1.3.1 Requirements

- Written and formalized procedure
- Encrypted communication channels
- Colour images
- Clear display of the interlocutor in terms of brightness, sharpness, contrast, fluidity of images
- Clearly audible audio
- Environments without special noise elements
- Electronic recording and retention of data, images, and metadata

4.1.3.2 Process Step

1. It acquires consent to video recording and informs that it will be stored in protected mode
2. Declares its generalities
3. Communicate your identification data
4. Confirm date and time and willingness to establish the relationship
5. Confirms the data entered online during pre-registration
6. Confirm mobile phone number and email address
7. Send a text message and an email to the customer, with a link to a URL for verification
8. It shows a valid ID on the front, equipped with a photograph and an autograph signature
9. Exhibits the health card on which the tax code is listed
10. Send electronic copy of ID
11. Performs random actions to strengthen the authenticity of the request
12. Summarizes the customer's will and collects his confirmation

There are also enhanced[10] ways of verifying acquired identification data, with a first verification of captured data plus a further verification of that data. In details, in the first step there is a receipt of

[10] KYC enhanced due diligence signifies the execution of complex operations to verify the identity of a client, and collect detailed and rigorous information and data, in order to make sure that the clients of a company are not involved with money-laundering or other types of financial crime. This information enables banks, financial institutions and other organizations

identification data (including the tax code) by taking -by fax, mail, electronically or in similar ways, copying a valid ID; on the other hand, the further verification consists of:

- Telephone contact on fixed user (welcome call),
- Sending communications to a physical home with a return receipt,
- Request to submit countersigned documentation,
- Verification of residence, domicile, activity carried out, through requests for information to the relevant offices or through on-site meetings, carried out using their own or third-party staff,
- Transfer from a banking intermediary in an EU country,
- Use of other feedback mechanisms based on reliable innovative technological solutions (such as those involving forms of biometric recognition), provided they are assisted by robust security guards.

4.2 eIDAS

4.2.1 eIDAS Regulation

As better specified in the chapter 2.1 of this document, eIDAS Regulation No 90/2014 of the European Parliament and of the Council of 23 July 2014 addresses electronic identification and trust services for electronic transactions in the internal market, so as to boost confidence and trust towards digital world by adopting the following principles among others:

- mutual acceptance of national e-ID
- common framework for secure interaction between citizens, companies and public administration
- interoperability solutions reduce fragmentation of digital market
- technological neutrality is required in order to avoid security requirements to be restricted to specific technological solutions
- interoperability of digital signatures is necessary to increase trust in business online transactions
- the level of trust in national electronic identity can be defined by a certain e-ID quality level;
- each member state must define one or more supervision organisations in order to verify the adoption of the Regulation and to interact with the European Commission
- supervision organisations should interact with authorities for data privacy, so as to avoid abuses and misuse of personal data

The eIDAS Regulation Implementing Act of 8 September 2015[6] has laid down requirements on the implementation of the regulation in European member states.

4.2.2 Security requirements of eIDAS component

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.

that are critical for the global stability of the economy, to make informed judgments about whether or not to provide – or continue to provide – services to particular customers.

The eIDAS-SP requires authenticity and integrity of the received person attributes, in order to assure their validity. It also needs confidentiality of the received identification data, so as to fulfil his data protection legal obligations.

The citizen requires confidentiality too, so as to be sure that his own 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.

These security requirements result in the following specifications for the components, which 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.

4.2.3 eIDAS Attributes

We can identify two different set of attributes for eIDAS regulation, one for natural person and one for legal person as specified in the previous section 2.4.2.

As not all countries support the legal entity registration functionality, the solution to this problem is to allow that the DC obtains the identity of the legal person or the identity of the entity along with its nationality, directly from the user in order to include it in the KYC request to the BAA.

If the user belongs to a country that supports the registers of legal persons companies eIDAS, this can first be requested and provided in the request.

4.3 Design of an interconnection architecture between eIDAS and KYC domains

4.3.1 Business Use Case

The high level business use case below introduces the stakeholder actors and needed use case functionality for providing Data Consumers with eIDAS identity authentication with KYC Services from Data Providers.

GRIDS will show how digital KYC providers can use eIDAS identity verification to create and maintain a consistent single view of their customers and perform effective and accurate screening, thereby increasing the operational efficiency of anti-money laundering, terrorist financing and, more generally, prevention and recognition of financial crimes. Essentially, GRIDS will support and simplify the online onboarding of individuals and businesses, including SMEs, thereby saving significant time and effort for companies implementing digital onboarding processes. It will provide the operational framework that will allow KYC data providers to group KYC information with eIDAS authentication data, thus creating a new generation of "KYC as a Service" offerings. Indeed, GRIDS will manage an enterprise infrastructure that facilitates and reduces the cost of KYC operations by establishing a corporate network, in the form of a federated Single Sign-On (SSO), between KYC providers (data providers), their customers from the industry. financial and beyond (data consumers) and customers in these sectors (end customers or stakeholders). This network will propagate the identity information and the eIDAS authentication token obtained to a node in the network and will group the KYC data with the identity data of the end customers (Data Subjects).

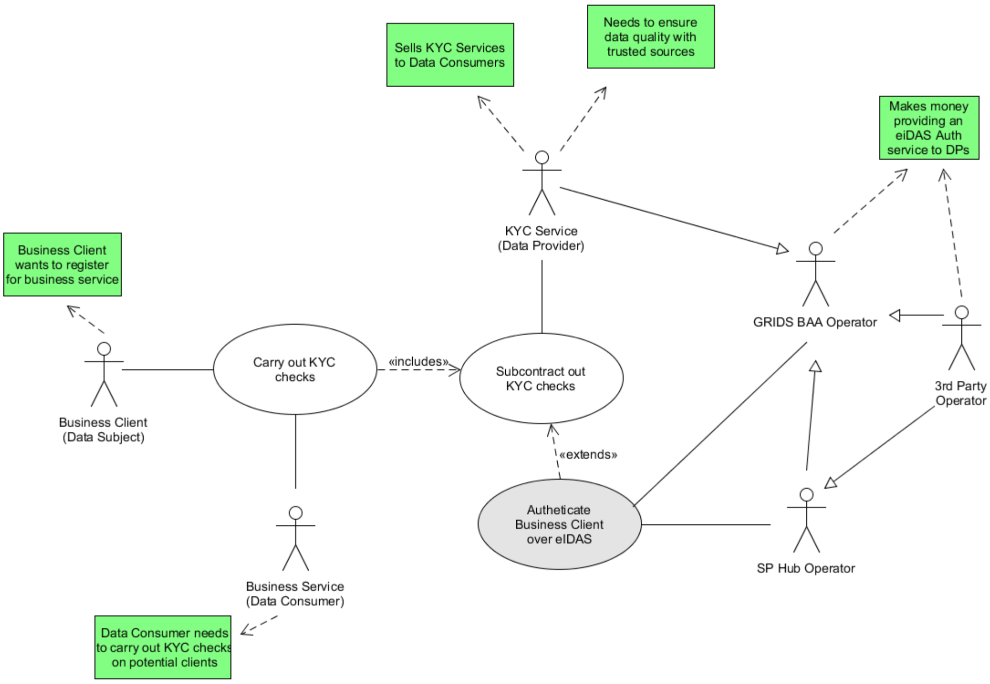

Sells KYC Services to Data Consumers
Needs to ensure data quality with trusted sources
Makes money providing an eIDAS Auth service to DPs
KYC Service (Data Provider)
Business Client wants to register for business service
GRIDS BAA Operator
3rd Party Operator
Business Client (Data Subject)
Carry out KYC checks
«includes»
Subcontract out KYC checks
«extends»
Autheticate Business Client over eIDAS
SP Hub Operator
Business Service (Data Consumer)
Data Consumer needs to carry out KYC checks on potential clients

Figure 9 Business Use Case

Table 10: Business Use Case Actor

Actor	
KYC/KYB Providers	The BAA enables the authentication of natural and legal persons over eIDAS and uses this assured identity data in the further collection of Know Your Customer (KYC) & Know Your Business (KYB) claims from Data Providers. The purpose is delivering verified identity and business data and screening: a) based on a single, comprehensive view of their customers, b) using the eIDAS Network-enabled authentication process in order to verify customers' identity (natural or legal person) and create the foundation for such a single customer view.
End-customers	End-customer referred to a natural or legal person. For these, remote digital onboarding of business customers is supported, including a mix of large companies and SMEs, a reliable digital mechanism for verifying the identity of the company's legal representative.
KYC Consumers or Data Consumer as referred in D3.1	Provide financial institutions and other business beyond the banking and financial sector: a) with a standardized, faster and less expensive identity verification and validation process that can be purchased "as-a-service", b) the possibility to create and promote complementary services, such as eiDAS eID-based authorization for the digital signature of business contracts, integration of eIDAS eID-based

	authentication to the existing Legal Entity Identifier (LEI) check mechanisms, KYC-based verification for the partners of an e-invoicing network, also initiated through an eIDAS eID-based authentication process etc. They correspond to the legal persons that are customers of company.

Table 11: High level Use Case

HIGH LEVEL USE CASE	
Use case name	Onboarding of Business Accounts by Banks / Financial Institutions (FIs)
Actor	▶ KYC Providers ▶ End-customers ▶ KYC Consumers
Description	It is highly essential for corporate banks and FIs to have a seamless and convenient business onboarding process to maintain an effective and profitable customer relationship with their corporate clients. A well-designed online onboarding process helps banks and FIs to gain a competitive advantage in the market. Banks and FIs also need to adhere to AML/KYC regulations and prevent fraudulent actors to use their institution for illicit activities like money laundering, terrorist financing, sanctions circumvention, etc. In order to be able to do so, banks and FIs need not only to gather and challenge company vitals (such as name, address, legal form, etc.) and company documents (such es register extracts, annual reports, etc.) but also to identify and verify associated natural persons, meaning especially directors and officers acting for the legal entity. So far identification and verification is performed either face to face by showing and comparing a passport manually or electronically by using some video identification method. While both possibilities bear certain risks of fraud or human errors the first mechanism is also very time consuming in comparison. With eIDAS-based eID checks both, risks of fraud as well as time spent for longsome identification processes are reduced significantly. The interoperability of company KYC checks and eID services will result in fundamental changes for the onboarding processes of business accounts. Not only will banks and FIs be able to retrieve governmentally approved eID data but it would also be possible to reduce onboarding time from about 6-8 weeks to same day. For example, kompany is providing KYC information (including real time business verification, check of company vitals as well as retrieval of authoritative and audit-proof company filings) for Raiffeisen Bank International28, a bank with a broad subsidiary network in the CEE region (10+ countries), which is increasingly using kompany's services and for which the integration of eIDAS based eID services could result in significant improvements with regards to their cross border activities.

4.3.2 Proposed GRIDS Architecture

The figure below shows the distributed claims approach of the GRIDS Business Attribute Aggregator (BAA).

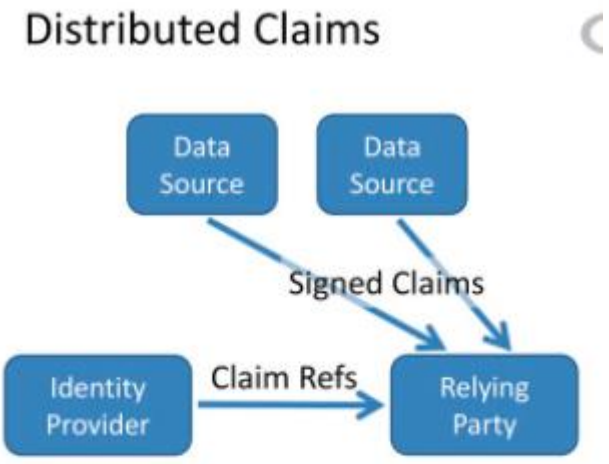


Figure 10 Distributed claim approach

Grids implements the **"OpenID connect for Identity Assurance (aka "IDA")[62]",** a specification that defines an extension of OIDC for providing Relying Parties with verified Claims about End-Users.

Two different approach for verified claims delivery:

- Aggregated claim
- Distributed claim

The **distributed claim** approach is the base approach used in GRIDS (even if the aggregate claim approach is supported) that allows to:

- Issue the claim directly from DC
- Use a BAA as OIDC OP
- define a clear separation of interests between commercial agreements (DC / DP) and level of trust

The main components are:

- The Service Provider hub: provides eIDAS authentication functionality and generate an identification token containing:
  - eIDAS attributes received
  - End-user/DS consent to transfer the received attributes to the end-users

  The Service Provider SP hub provides eIDAS authentication functionality (i.e. Relying Party for the eIDAS Network). It is the direct consumer of an eIDAS Network-enabled authentication process for GRIDS end-users natural persons representing a business entity.

  - The SP hub is operated by ADACOM, a Greek Service Provider authorized to provide eIDAS Network connectivity to its customers in Greece and abroad.
- The Business Attribute Aggregator is responsible of:
  - Aggregate eIDAS + KYC request
  - Routing KYC request

- DP KYC service catalogue queries to GRIDS registry
- BAA network map of local and remote DP KYC service
- Connection with external provider

BAA is operated by 360kompany AG (therefore Kompany), an Austrian KYC provide, offering real-time access to official and audit-proof commercial register information, including company filings (Kompany covers more than 100 million companies in 150+ jurisdictions).

4.3.3 GRIDS Infrastructure Building Blocks

The GRIDS Platform is a Business Network, in the form of a Single-Sign-On (SSO) federation, between KYC providers (Data Providers), their customers (Data Consumers) and the clients for these customers (Data Subjects).

4.3.3.1 Service Provider Hub (SP Hub)

The SP hub is operated by ADACOM, a Greek Service Provider authorized to provide eIDAS Network connectivity to its customers in Greece and abroad.

The Service Provider (SP) hub will provide eIDAS authentication functionality. It will be the direct consumer of an eIDAS Network-enabled authentication process for GRIDS end-users natural and legal persons (Data Subjects) representing a business entity. The SP Hub will generate an identification token containing eIDAS received attributes and end-user/DS consent to transfer the receive attributes to the Data Consumers. The identification token generated by the SP Hub will be transmitted to the Business Attributes Aggregator (BAA).

To be compliant with the GDPR legislation, the backward sharing of authentication data in response SAML, in the registration phase, the GDPR clauses will also include this agreement.

The SP Hub design is centred on the goal of minimising eIDAS interoperability costs for service providers in order to boost adoption and thus boost end user usage. SP Hub will act as a central point of trust for Natural and Legal Persons between Data Consumers (DC) and Service Providers (SP) and to provide all the available by SPs Natural and Legal Person eIDAS attributes, such as:

- Uniqueness Identifier
- Current Family Name(s) (mandatory)
- Current First Name(s) (mandatory)
- Legal Name
- Legal Person Identifier
- Lei
- Date of Birth
- First name(s) and family name(s) at birth
- Place of Birth
- Current Address
- Gender

To initiate a user authentication, the BAA interface (implementing OIDC) creates an identification request and forwards it to the SP hub in the form of a message containing the following data:

- Scope: the scope defines the requested attributes (claims) needed
- OIDC parameters

  - response_type: the OIDC flow used (in this case this value will always be equal to "code")
  - client_id: the client ID that the BAA service has registered with the SP Hub
  - redirect_url: the url that the authorization code will be returned to
  - state: the BAA session identifier

The BAA interface (OIDC) will receive from the SP hub a (Signed) JSON containing:

- The eIDAS retrieved identification attributes
- TimeStamp
- The eIDAS node SAML response (signed by the eIDAS node, and encrypted with the SP hub private key - this information is returned as evidence)
- Consent statement
- SP hub signature
- Additional info contained within the token (eIDAS node issued time-of-use-slot and "extended" time of use slot)
  - Not Before - Not After
  - eIDAS node "Issued At"
  - eIDAS node "Expiration"

The SP Hub will be developed containing the following components:

- SP interface: Establishes interaction with the BAA services. Contains a single endpoint which receives the authentication request from the BAA;
- eIDAS interface: Connects to the country eIDAS node, Comprises two endpoints:
  - Metadadata endpoint: Provides SP metadata;
  - ReturnPage endpoint: Receives the SAML response from the country eIDAS node.
- UI module: Interacts with the end user;
- Manager service: Orchestrate the authentication process inside the SP Hub;
- Protocol Translation service: Translates in both ways from the BAA to eIDAS node:
  - The authentication request from the BAA to a SAML request;
  - The SAML response from eIDAS node to an authentication response to BAA;
- Mapping service: Maps the BAA attribute names to SAML eIDAS attribute names, doing the semantic translation;
- SAML Engine: Manages the SAML request and response, encrypting/decrypting and signing.
- Metadata service: Creates BAA metadata;

4.3.3.2 Business Attribute Aggregator

The interface with the DC and the BAA (acting as OIDC OP) is based on OpenID Connect for Identity Assurance 1.0 (aka "IDA").

The GRIDS architecture can support both the IDA Aggregated and Distributed Claims approaches. However, it is decided that for GRIDS, it is only needed for the BAA to support the Distributed Claims approach due to its more desirable characteristics, as follows:

- the KYC claims are not proxied over the BAA to DPs or indeed over remote BAAs where other DPs have their trust relationship
- no proprietary GRIDS KYC query interface needs to be implemented for requesting KYC claims from the BAA to the DPs

- the BAA only provides the trust relationship between the DC and DPs without the need for the DCs to have any previous relationship with the DPs.
  - Trust established with signed OIDC Access Token as per Distributed Claims approach
  - BAA provides the subject's eIDAS identity in the Access Token claims
- Follows a similar approach as exists today between Data Consumers and KYC Data Providers where the DC will request directly to the DPs the KYC attributes directly via APIs. The difference now being that this will be a standardized interface as per the IDA spec to retrieve the verified claims at an OIDC Userinfo endpoint offered by the DPs.
- Provides the capability for the DC to include charging information in the userinfo request to the DP KYC Source to enable the DP to charge the DC without previously having any relationship.
  - The charging information options that can be provided will be explored more in the project with consultation with Data Consumers and Data Providers. For example, it could include Credit Card or Bank Account information or a customer account key and registration point.

The BAA will establish trusting relationships with the data providers, who will provide the DP entity ID, public key, KYC declarations, and IDA verified metadata. The BAA exposes a DC Introspection endpoint so that the DP can query information about the DC from which it received a KYC request and with which it has no relationship. In addition, the BAA regularly queries the OIDC configuration address of the well-known DP to check availability as well as to keep KYC claim support information up to date.

Note: In this design it is the Data Consumer is the Data Controller that is responsible for making sure that it obtains the user's consent for any collection, processing and sharing of the user's personal data, and that the GRIDS platform only facilitates this process acting as a Data Processor on behalf of the Data Consumer. To make sure that the DC respects EU privacy laws concerning consent in the GDPR, the DC should at all times make it clear to the user the personal data that is being requested, why, with whom and what personal data it will share with the DPs as part of this process.

4.3.3.3 eIDAS Greek Node

Greece supports the eIDAS network in both production and pre-production environments. Specifically, in Greece two eIDAS nodes are deployed (one for each environment) running eIDAS version 1.4.3[24].

The existing governance policy for the eIDAS nodes allows both public and private Service Providers (SPs) to connect to the Greek eIDAS nodes, enabling them to seamlessly authenticate cross-border users from any of the connected Member States (MS).

However, since Greece does not have a notified eID scheme yet, connectivity at a production level, with other member state eIDAS nodes, is limited. Additionally, the lack of a notified eID scheme in Greece results in the situation that although citizens from any third party MS connected to the Greek node can authenticate to any SP service connected to it, Greek citizens are unable to authenticate to SP service connected to other MS´s eIDAS nodes (at a production level).

However, the Greek eIDAS strategy is being revisited as part of the creation on a national eID scheme (this is also an immediate result of the fact that the custody of the Greek eIDAS nodes has been passed over to the Greek Ministry of Digital Governance[25]). Thus, it is expected that in the near future the connectivity of the Greek eIDAS node will improve significantly.

4.3.3.4 KYC Data Consumer (DC)

KYC Data Consumer are responsible to carry out a ***Due Diligence Check***, in the sense that they take data from KYC Data Providers and check the user identity and financial activities to determine any risk that is taken on or not. Potentially this information could be returned to the End User (Data Subject) but that is entirely within the scope of the DC and does not affect eIDAS or GRIDS in any way.

As regards, the information that the data consumer collects on the data subject, through the data providers, it is needed the following set of attributes:

- Relationship to given company (e.g. director)
- Full name
- Address
- Birthdate (+ possibly country of birth)
- ID verification results (passport/ID card number)
- Corporate information (such as Legal Person Identifier, Legal Name, LEI)
- Personal and/or corporate PEP/Sanction check results

4.3.3.5 KYC Data Provider (DP)

After successful user authentication, the DC can request KYC/KYB claims to DP thought a ***Transparent Model***, that is based on two scenarios:

- DC requests specific services from specific Data Providers, all of which are available in a service catalogue
- DC does not specify the service from catalogue, and all DPs that support certain requested claim return this info to DC and then will be the DC to choose which one to use.

5 High Level IDentity Assurance Interwork Flows

The interface with the DC and the BAA (acting as OIDC OP) is based on OpenID Connect for Identity Assurance 1.0 (aka "IDA"), [63].

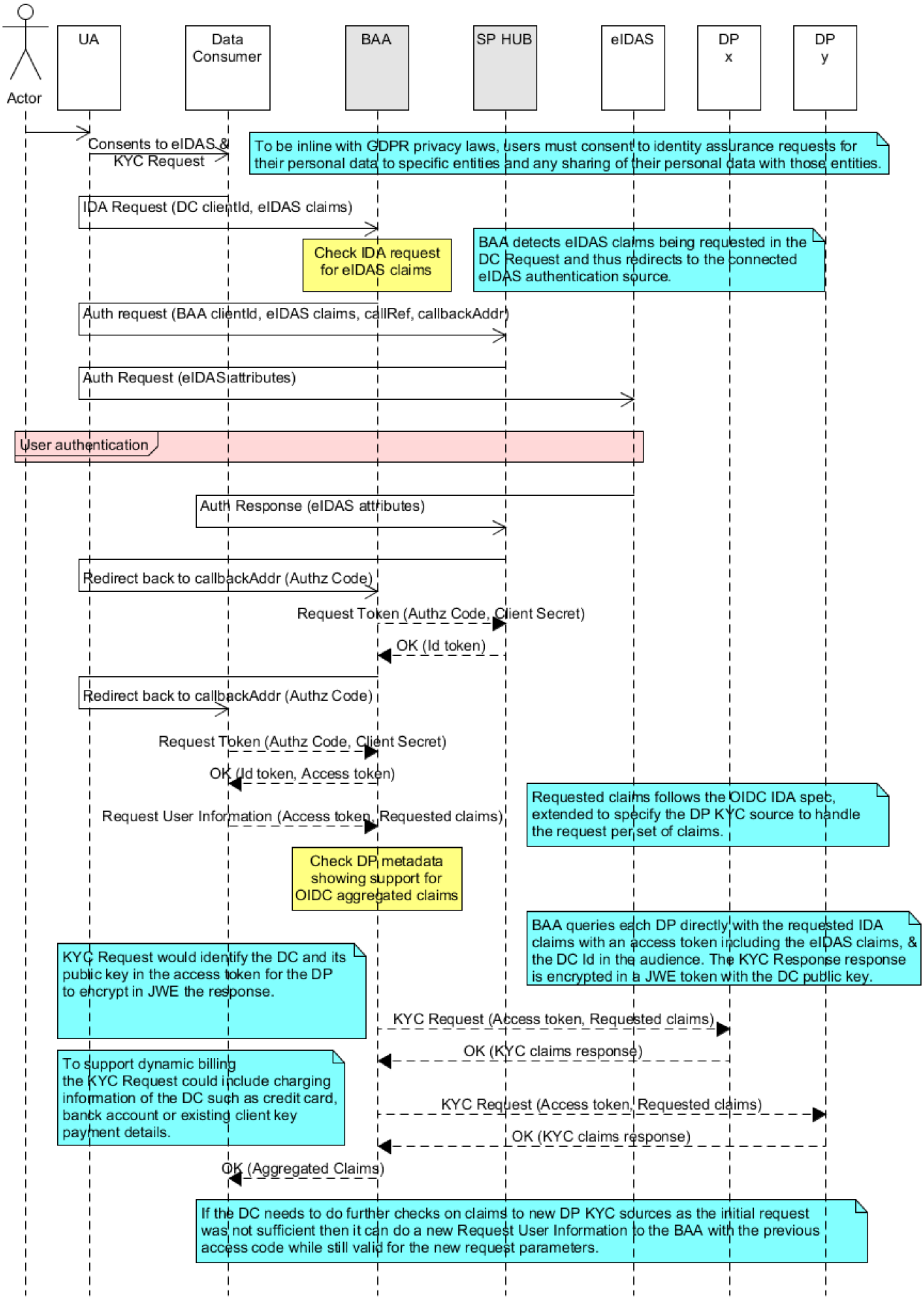
The GRIDS architecture can support both the IDA Aggregated and Distributed Claims approaches. However, it is decided that for GRIDS, it is only needed for the BAA to support the Distributed Claims approach due to its more desirable characteristics, as follows:

- the KYC claims are not proxied over the BAA to DPs or indeed over remote BAAs where other DPs have their trust relationship
- no proprietary GRIDS KYC query interface needs to be implemented for requesting KYC claims from the BAA to the DPs
- the BAA only provides the trust relationship between the DC and DPs without the need for the DCs to have any previous relationship with the DPs.
  - Trust established with signed OIDC Access Token as per Distributed Claims approach
  - BAA provides the subject's eIDAS identity in the Access Token claims
- Follows a similar approach as exists today between Data Consumers and KYC Data Providers where the DC will request directly to the DPs the KYC attributes directly via APIs. The difference now being that this will be a standardized interface as per the IDA spec to retrieve the verified claims at an OIDC Userinfo endpoint offered by the DPs.
- Provides the capability for the DC to include charging information in the userinfo request to the DP KYC Source to enable the DP to charge the DC without previously having any relationship.
  - The charging information options that can be provided will be explored more in the project with consultation with Data Consumers and Data Providers. For example, it could include Credit Card or Bank Account information or a customer account key and registration point.

Each BAA is part of a network of BAAs, where each BAA will establish trust relationships with Data Providers, which provision the DP's entityID, public key, KYC claims and IDA verified metadata. The only software interface the DP will optionally have with the BAA is a health-check API so that the BAA can provide this information to the Data Consumers.

Note: In this design it is the Data Consumer is the Data Controller that is responsible for making sure that it obtains the user's consent for any collection, processing and sharing of the user's personal data, and that the GRIDS platform only facilitates this process acting as a Data Processor on behalf of the Data Consumer. To make sure that the DC respects EU privacy laws concerning consent in the GDPR, the DC should at all times make it clear to the user the personal data that is being requested, why, with whom and what personal data it will share with the DPs as part of this process.

5.1 Aggregated Claims


Actor
UA
Data Consumer
BAA
SP HUB
eIDAS
DP x
DP y
Consents to eIDAS & KYC Request
IDA Request (DC clientId, eIDAS claims)
Check IDA request for eIDAS claims
Auth request (BAA clientId, eIDAS claims, callRef, callbackAddr)
Auth Request (eIDAS attributes)
User authentication
Auth Response (eIDAS attributes)
Redirect back to callbackAddr (Authz Code)
Request Token (Authz Code, Client Secret)
OK (Id token)
Redirect back to callbackAddr (Authz Code)
Request Token (Authz Code, Client Secret)
OK (Id token, Access token)
Request User Information (Access token, Requested claims)
Check DP metadata showing support for OIDC aggregated claims
KYC Request (Access token, Requested claims)
OK (KYC claims response)
KYC Request (Access token, Requested claims)
OK (KYC claims response)
OK (Aggregated Claims)

To be inline with GDPR privacy laws, users must consent to identity assurance requests for their personal data to specific entities and any sharing of their personal data with those entities.

BAA detects eIDAS claims being requested in the DC Request and thus redirects to the connected eIDAS authentication source.

Requested claims follows the OIDC IDA spec, extended to specify the DP KYC source to handle the request per set of claims.

BAA queries each DP directly with the requested IDA claims with an access token including the eIDAS claims, & the DC Id in the audience. The KYC Response response is encrypted in a JWE token with the DC public key.

KYC Request would identify the DC and its public key in the access token for the DP to encrypt in JWE the response.

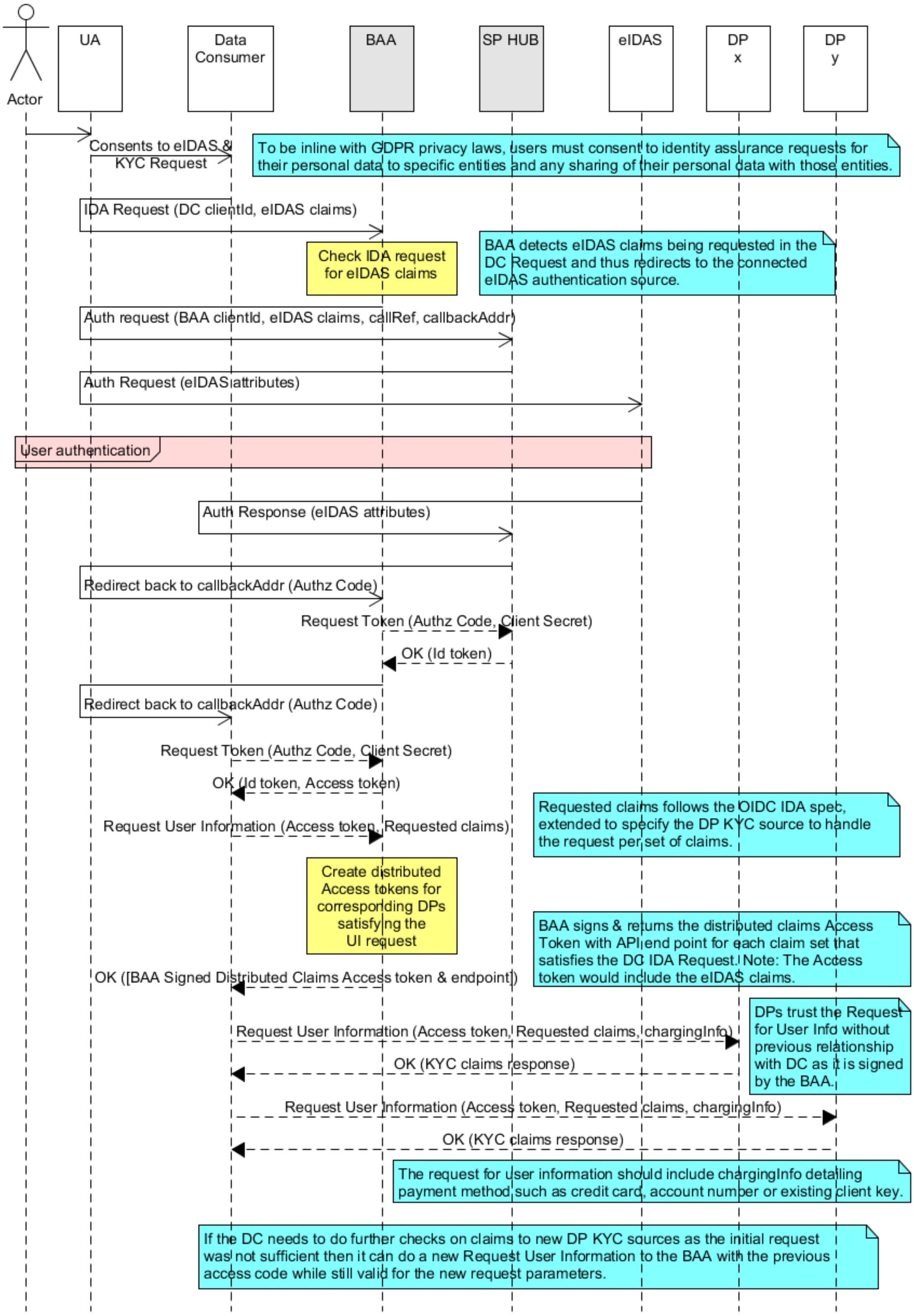
To support dynamic billing the KYC Request could include charging information of the DC such as credit card, banck account or existing client key payment details.

If the DC needs to do further checks on claims to new DP KYC sources as the initial request was not sufficient then it can do a new Request User Information to the BAA with the previous access code while still valid for the new request parameters.

Figure 11 Aggregated Claims approach

This figure is shown for information only and is not supported in this version of the BAA, due to the reasons given previously in this section. However, it must be noted the architecture design also supports this aggregated approach, and thus could be supported in a later development if there are new DP and DC stakeholders that favour to connect with GRIDS using this approach.

5.2 Distributed Claims


Actor
UA
Data Consumer
BAA
SP HUB
eIDAS
DP x
DP y
Consents to eIDAS & KYC Request
IDA Request (DC clientId, eIDAS claims)
Check IDA request for eIDAS claims
Auth request (BAA clientId, eIDAS claims, callRef, callbackAddr)
Auth Request (eIDAS attributes)
User authentication
Auth Response (eIDAS attributes)
Redirect back to callbackAddr (Authz Code)
Request Token (Authz Code, Client Secret)
OK (Id token)
Redirect back to callbackAddr (Authz Code)
Request Token (Authz Code, Client Secret)
OK (Id token, Access token)
Request User Information (Access token, Requested claims)
Create distributed Access tokens for corresponding DPs satisfying the UI request
OK ([BAA Signed Distributed Claims Access token & endpoint])
Request User Information (Access token, Requested claims, chargingInfo)
OK (KYC claims response)
Request User Information (Access token, Requested claims, chargingInfo)
OK (KYC claims response)

To be inline with GDPR privacy laws, users must consent to identity assurance requests for their personal data to specific entities and any sharing of their personal data with those entities.

BAA detects eIDAS claims being requested in the DC Request and thus redirects to the connected eIDAS authentication source.

Requested claims follows the OIDC IDA spec, extended to specify the DP KYC source to handle the request per set of claims.

BAA signs & returns the distributed claims Access Token with API end point for each claim set that satisfies the DC IDA Request. Note: The Access token would include the eIDAS claims.

DPs trust the Request for User Info without previous relationship with DC as it is signed by the BAA.

The request for user information should include chargingInfo detailing payment method such as credit card, account number or existing client key.

If the DC needs to do further checks on claims to new DP KYC sources as the initial request was not sufficient then it can do a new Request User Information to the BAA with the previous access code while still valid for the new request parameters.

Figure 12 Distributed Claims approach

5.2.1 BAA External Interfaces

The BAA supports the following external interfaces:

5.2.1.1 OpenID Configuration Endpoint

The configuration of any GRIDS Endpoint: BAA or Data Provider can be retrieved via OpenID Configuration published by the respective Issuer. OpenID Providers supporting Discovery MUST make a JSON document available at the path formed by concatenating the string /.well-known/openid-configuration to the Issuer [64].

5.2.1.2 Client Registration Endpoint

The Client Registration Endpoint is an OAuth 2.0 Protected Resource through which a new Client registration can be requested. The OpenID Provider MAY require an Initial Access Token that is provisioned out-of-band (in a manner that is out of scope for this specification) to restrict registration requests to only authorized Clients or developers [65].

5.2.1.3 Authorization Endpoint

The Authorisation Endpoint supports an OAuth 2.0 Authorization Request that requests that the End-User be authenticated by the Authorization Server [66].

5.2.1.4 Token Endpoint

To obtain an Access Token, an ID Token, and optionally a Refresh Token, the RP (Client) sends a Token Request to the Token Endpoint to obtain a Token Response, when using the Authorization Code Flow [66].

5.2.1.5 Userinfo Endpoint

The UserInfo Endpoint is an OAuth 2.0 Protected Resource that returns Claims about the authenticated End-User. To obtain the requested Claims about the End-User, the Client makes a request to the UserInfo Endpoint using an Access Token obtained through OpenID Connect Authentication [66].

In this implementation the Userinfo Endpoint will return the userinfo response with distributed claim requests towards remote Userinfo Endpoints supported by GRIDS Data Providers to request Identity Assured claims as specified in the OIDC IDA 1.0 specification [67].

5.2.1.6 Client Introspection Endpoint

The client introspection endpoint is an OAuth 2.0 endpoint, used by the Data Providers, that queries a client introspection token and returns a JSON document representing the metadata for the Data Consumer client [68].

The client introspection endpoint and client introspection token are made available to the DP in the distributed claims Userinfo request.

5.2.2 High Level Architecture Decision

The most important architectural choices made, which concern the following areas, are shown below:

- Centralized approach vs distributed approach
- Commercial Considerations
- Billing observation
- Maintenance and Support
- Service Discovery
- API consistency

- Governance

5.2.2.1 Centralized vs Distributed

In line with general best practice approaches for maintenance, throughput, and scalability, a centralized approach is discarded. Such an approach would put an unnecessary burden on both DCs and DPs and would lead to a single point of (commercial) failure, and a lack of transparency to the operation of the network. Given the distributed nature of the eIDAS system, the BAA solution should also be distributable.

Having determined the type of approach, another important consideration concerns the mapping between BAAs and DPs.

The choice fell on these two options:

- simple, 1 to 1 mapping (1 BAA per DP), model (middleware model)
- n:m, fully distributed model

This decision is also based on the factors described above, but also has to take into account the ease of participation in the network. Given the goal of the project is to facilitate operations for the end user, this implies that the ease of integration for the Data Consumer should be maximized, and also the ease of integration for the Data Provider – but with a preference given to the consumer.

The **OpenID connect for Identity Assurance (aka “IDA”):** Specification that defines an extension of OIDC for providing Relying Parties with verified Claims about End-Users.

This specification provides two different approach for verified claims delivery:

- Aggregate claim
- Distributed claim

The distributed claim approach allows to:

- Issue the claim directly from DC
- Use a BAA as OIDC OP
- Define a clear separation of interests between commercial agreements (DC / DP) and level of trust

5.2.2.2 Commercial considerations

Given that the provision of service by a DP to a DC is a commercial operation, there needs to be a mechanism for these costs to be paid, accounted, and reconciled. The selected architecture must be able to meet this requirement without forcing extra costs or creating a barrier to entry into the network for either DCs or DPs.

The simplest working assumption for charging was that there would be an existing relationship between the DP and the DC(s), and that charging and billing would take place between them irrespective of the BAA or any other eIDAS/ GRIDS components. In this scenario, the BAA would be acting as a proxy for whatever authentication is needed from the DC to the DP, and also for any response from the DP to the DC. This allows for complete flexibility of charging models (one off / monthly / per call / combinations) to be offered, as well as multiple payment options (cc, invoice, sepa, etc), and response types (pure data, URL, callbacks, etc). There is a massive amount of combinations possible, and is not the case to getting into that area. Also, if the BAA is aware of the content of communications between the DP and the DC, this may have legal implications as well, and at a minimum would not be liked by the DC’s as they would be concerned with the data flow and ensuring data security within the BAA.

This does not preclude the BAA from becoming involved in an introductory manner of course, and it might well be the case that some services do not require pre-registration or payment. There isn't the need for the BAA to be aware of payload, as the DP response will be simply wrapped, and again having a 3rd party with knowledge of the request and response is unwanted, if not illegal.

In any case, the BAA should be logging the request and response metadata as a minimum – this would allow the BAA to act as a 3rd source of reconciliation if there arises a dispute between a DC and a DP over usage. If the BAA is to log payloads, this must only be logged in an encrypted fashion such that only the DP and the DC can see the content.

Regarding the approach to be used for sharing data between DP and DC, using a download token is the best approach, it places a slightly higher burden for entry on DPs but simplifies BAA management and payload demarcation.

5.2.2.3 Billing observation

The thinking here was for request/response log access. Assuming the BAA is logging the metadata (and potentially encrypted payload) of requests and responses, then an API must be provided to DPs and DCs to access these logs for items relevant to them. Also, they can be used to determine the health state of DPs. A tool like elastic search can be used to index the logs to provide these details, but it could also be done using a database of some form. The functionality is important, not the mechanism.

5.2.2.4 Maintenance and Support

It is assumed to be vital that:

- the chosen architecture allows for secure logging of request and response metadata
- the BAA code components are stored and developed in a controlled environment
- the BAA code components can be updated in a timely fashion without undue downtime

in a fully distributed model, the network can withstand extra-request node failures (Failures occurring outside the timing scope of a single request).

5.2.2.5 Service Discovery

For a range of DPs to offer a range of services to a range of DCs, it is proposed that a Service Discovery/Catalogue function is included, whereby DCs can choose from available services in a consistent fashion. The architecture should allow this to happen in a manner which maximizes the options available to the DCs.

The BAA service catalogue should show all available DP API's.

An introduction mechanism, in case of a DC joins up and ask to provision the Dps that it wishes to use, will be provided and could be as simple as a signup url.

Alternatively, if the DC tries to use a DP but does not have an account at that DP an error message is given back to the user.

5.2.2.6 API Consistency

To facilitate ease of use for DCs, the services offered by DPs should be in as consistent a format as possible, ideally on both the inbound (calling) end, and also on the outbound (response).

5.2.2.7 Governance

Any choice of architecture will have governance issues associated with it. The selected architecture should minimize the burdens of governance and strike a balance between security, governance and flexibility.

5.2.2.8 Centralized Event Logging & Reporting

GRIDS will implement a centralized logging and event reporting capability so GRIDS benefits from the following features:

1. that all microservice modules will be able to report any alarms e.g. heartbeat failure
2. exception events
3. successful and unsuccessful eIDAS authentications with cross-border country captured
4. successful and unsuccessful KYC Request searches for the actual service and DP it was requested to

This event reporting capability will help operations and maintenance monitor the platform and identify potential issues and help to resolve any issues between the Data Consumers and Data Providers.

Additionally, it can provide statistical reports that could be used for quantity-based charging tariffs towards the DPs.

The following figure demonstrates a possible implementation architecture based on the popular OSS event reporting solution Elasticsearch, Logstash, Kibana (ELK).

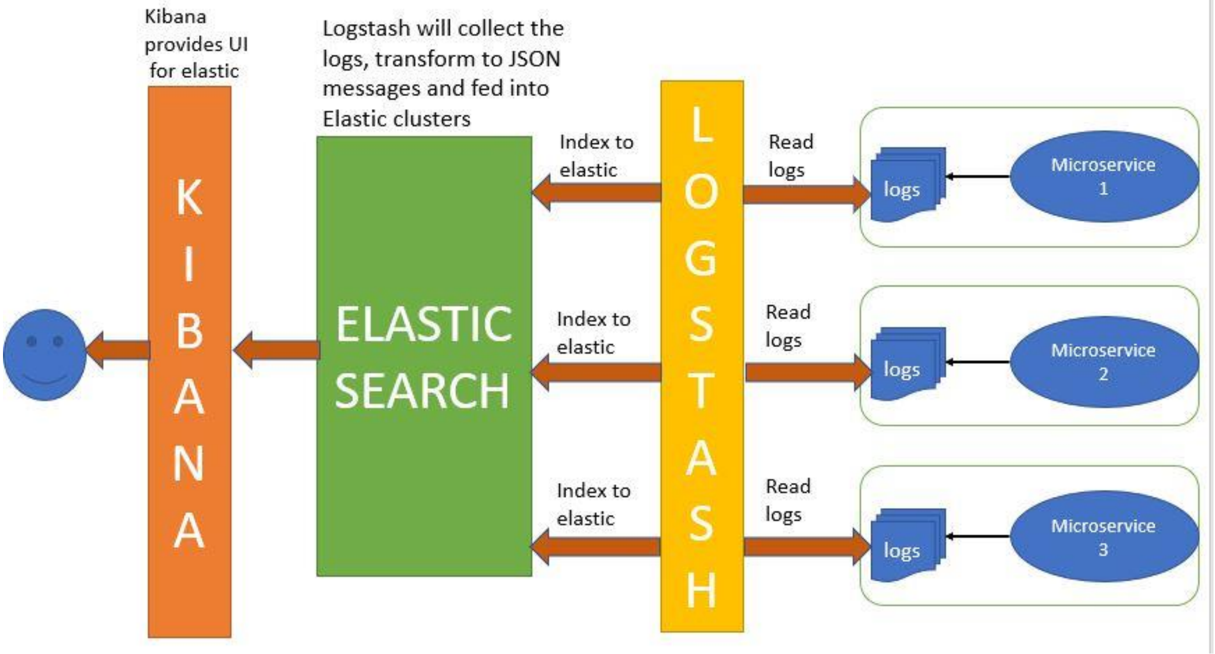


Figure 13 Microservice ELK Event Reporting Solution

5.3 Testing Frameworks

The Testing Framework of GRIDS is designed to implement an end-to-end test solution that serves as:

1. means of verification of the correct functionality of the GRIDS platform in both production and pre-production
2. a monitoring solution the platforms status
3. a user evaluation tool

This framework will be based on eCATS v2.0 (eIDAS Connectivity Automated Testing Suite 2.0), that was developed during the ESMO project[58], which will be further expanded to facilitate the specific needs and use cases of GRIDS.

In more details, apart from the typical CI/CD testing tasks (unit tests, integration tests etc., that will be undertaken during the development of the GRIDS platform and its deployment on the production and pre-production servers) the GRIDS Testing framework primarily consist of the execution and result evaluation of a series of:

- automated test cases, in the case of the pre-production environment, authenticating users with test credentials
- in-vivo test cases, in the case the production environment conducted by real test users with real eIDAS credentials

The focus of each such test case is to verify the successful cross border authentication (over eIDAS network) of the users and also to verify the satisfaction of the various GRIDS use case specific requirements. After each execution of a test round, the outcomes will be evaluated and based on the results a new round of development might be triggered.

The execution of the automated test cases will be based on the use of Katalon Studio[57], a freemium test automated application (built on top of the state of the art, testing automation open-sources frameworks, Selenium and Appium). Katalon Studio allows users to automate test scripts and run them across different browsers and operating systems while providing a specialized IDE interface for API, Web and Mobile testing. In more details, Katalon Studio (the essential components of eCATS v2.0) acts as a general-purpose tool to perform the automatic testing of web applications and web-based composite services, even if they span multiple pages and use complex interactions like pop-up windows and modular messages. It is completely user-interaction free. Used in the case of testing the integration of an Online Service with the GRIDS platform, eCATS v2.0 provides the following core functionalities:

- Automated execution of the Data Consumer eIDAS + KYC request to the GRIDS platform
- Automated execution of the entire eIDAS authentication process
- Automated selection of suitable KYC providers and the automated submission of additional data required to execute the KYC attribute acquisition request
- Automated logging of events/errors/failures
- Multiple tests in a single run
- Automated reporting

Essentially, eCATS v2.0 enables the design and construction of scripts which simulate the user's actions during the execution of an eIDAS authentication and KYC request (including the testing of a pre-defined authentication failure case). These steps are executed in an automated fashion, which in turn reports the result of each execution ("Success" / "Failure"). A Success is detected only when the tool reaches a test specific designated URL whose content indicates the correct retrieval of both eIDAS and KYC attributes of a test user.

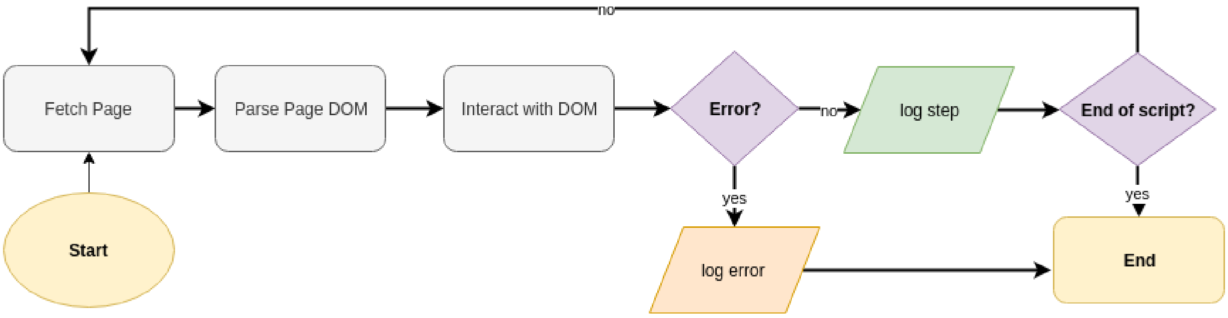


Figure 14: eCATS v2.0 Operational Flow

For each test, the service tester generates a test script file using a GUI provided by the Katalon Studio IDE. This test script defines the various interactions of an actual user with all of the components of the system (the DC interfaces, the eIDAS Node interfaces, the KYC provider selection and so on). Test scripts can be bundled together in test suites which can be run automatically and, most important, periodically to verify the integration of a Service with the GRIDS platform and the eIDAS Network.

At the end of the execution of a test suite an email is sent to the tester with the test summary report. Also, two reporting files (one in html format and one in pdf format) are generated. These files, contain a detailed description of execution of the test case; if the result was a success or a failure and various details about the test execution process (like time of execution of each command, url, the DOM object that was interacted etc.) and in the case they were requested by the test script screenshots of various steps of the process. These files also contain the specific test commands that produced an error and the reason for which the error occurred (if of course an error occurred that caused the test case to fail).

Apart from the automated testing, real test users will be recruited, such that they are in possession of real eIDAS cross border credentials. These test users will be organised into test groups and each test group will be instructed on the conduction of targetted tests cases of the GRIDS platform requiring eIDAS + KYC attributes from the connected KYC providers. After the conclusion of the tests the users will be asked to submit evaluation reports, interviews, regarding the usability of the platform and their over all experience and their answers will be used to further evaluate and improve the impact of GRIDS.

6 Conclusions

Business Constraint

- Interaction DP/DC is a commercial operation
- Needs for accountability and reconciliation mechanism
- BAA should be independent from business relations
- BAA act as a proxy to guarantee a level of trust

which provides the following benefits: flexibility and separation of interests.

Distributed claim approach

OpenID connect for Identity Assurance (aka "IDA"): Specification that defines an extension of OIDC for providing Relying Parties with verified Claims about End-Users.

Two different approach for verified claims delivery:

- Aggregated claim
- Distributed claim

Although the aggregate claim approach is supported, the best approach to use is the distributed claim approach.

With distributed claim approach:

- the KYC claims are not proxied over the BAA to DPs
- no proprietary GRIDS KYC query interface needs to be implemented
- the BAA only provides the trust relationship between the DC and DPs
- define a clear separation of interests between commercial agreements (DC / DP) and level of trust

Audit mechanism

The BAA provide a log event transactions mechanism and exposes an API to access these logs.

7 References

[1] Agid, Le tappe del Regolamento eIDAS https://www.agid.gov.it/it/piattaforme/eidas/tappe-del-regolamento-eidas

[2] European Union law https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002

[3] Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[4] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of eIDAS Regulation trust https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002

[5] Guidance for the application of the levels of assurance which support the eIDAS Regulation https://ec.europa.eu/cefdigital/wiki/download/attachments/40044784/Guidance_on_Levels_of_Assurance.docx

[6] REGULATIONS 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://ec.europa.eu/futurium/en/system/files/ged/celex_32015r1501_en_txt.pdf

[7] COMMISSION IMPLEMENTING DECISION (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) 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://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1984_en_txt.pdf

[8] COMMISSION IMPLEMENTING DECISION (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) 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://ec.europa.eu/futurium/en/system/files/ged/celex_32015d0296_en_txt.pdf

[9] E. McCallister e R. Brackney, "ITU-T Recommendation X.1254 | International Standard ISO/IEC DIS 29115 --Information technology --Security techniques --Entity authentication assurance framework," November 2011, [online] https://www.oasis-open.org/committees/download.php/44751/285-17Attach1.pdf

[10] DECRETO LEGISLATIVO 7 marzo 2005, n. 82, Codice dell'amministrazione digitale

[11] Agid, Identificazione e Autenticazione elettroniche, https://www.agid.gov.it/it/piattaforme/eidas/identificazione-autenticazione-elettroniche

[12] Agid, Nodo eIDAS italiano, https://www.agid.gov.it/it/piattaforme/eidas/progetto-ficep

[13] Research projects STORK and STORK 2.0 – online STORK Consortium, "Secure idenTity acrOss boRders linKed,» [online] https://www.eid-stork.eu/ and STORK Consortium, "Secure idenTity acrOss boRders linKed 2.0 (STORK),» [online] https://www.eid-stork2.eu/

[14] Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electronica https://boe.es/buscar/act.php?id=BOE-A-2005-21163

[15] Pae, Sistema europeo de reconocimiento de identidades electrónicas – eIDAS https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Identidad_y_firmaelectronica/Nodo-eIDAS.html#.X2oE14vtZEY

[16] CUERPO NACIONAL DE POLICÍA, Diferencias DNIe y DNI 3.0 https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_038

[17] Pae, Spain deployed the first version of its eIDAS node, integrated with the DNI-e https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2016/Diciembre/Noticia-2016-12-21-Espana-despliega-la-primera-version-de-su-nodo-eIDAS--integrado-con-el-DNIe.html?idioma=en#.X2oE3YvtZEY

[18] Cl@ve Identificación, Conoce Cl@ve Identidad Electrónica para las Administraciones http://clave.gob.es/clave_Home/clave.html

[19] Cl@ve Identificación https://administracionelectronica.gob.es/ctt/clave#.X2oJeYvtZEY

[20] LEPS, Leveraging eID in the Private Sector http://www.leps-project.eu/

[21] INEA, Connecting Regional and Local Administrations to Spanish eIDAS Node (eID4Spain) https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2018-es-ia-0039

[22] INEA, eIDAS2Business: Making Private businesses benefit from eIDAS https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2016-eu-ia-0066

[23] INEA, Opening a bank account with an EU digital identity https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2016-eu-ia-0070

[24] European Commission, Copyright European Commission —DIGIT Unit D3eIDAS-Node Installation and Configuration Guide - Version 1.4.3 https://ec.europa.eu/cefdigital/wiki/download/attachments/82773765/eIDAS-Node%20Installation%20Manual%20v1.4.3.pdf?version=1&modificationDate=1536823008963&api=v2

[25] Greek Ministry of Digital Governance website https://mindigital.gr/

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/eli/reg/2016/679/oj

[27] New European Interoperability Framework https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf

[28] eIDAS Interoperability Architecture v.1.2 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile?preview=/82773108/148898845/eIDAS%20Interoperability%20Architecture%20v.1.2%20Final.pdf

[29] European Commission, The New European Interoperability Framework https://ec.europa.eu/isa2/eif_en

[30] INEA, CEF Telecom https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom

[31] CEF Digital, Connecting Europe, CEF Building Blocks presented at Releasing the Power of Procurement https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/05/07/CEF+Building+Blocks+presented+at+Releasing+the+Power+of+Procurement

[32] CEF Digital, Connecting Europe, eID Documentation. What is eID? https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+eID

[33] CEF Digital, Connection Europe, eID Documentation. Use case: Proxy to Proxy https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Proxy+to+proxy

[34] CEF Digital, Connecting Europe, eID Documentation, How does it work? https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773030

[35] ISO, https://www.iso.org/obp/ui/#iso:std:iso-iec:29115:ed-1:v1:en

[36] NIST Special Publication 800-63A, Digital Identity Guidelines https://pages.nist.gov/800-63-3/sp800-63a.html

[37] ICAO publication https://www.icao.int/publications/pages/publication.aspx?docnum=9303

[38] CEF Digital, Connecting Europe, eID Documentation. Proxy to Middleware https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Proxy+to+Middleware

[39] CEF Digital, Connecting Europe, eID Documentation. Use case: Middleware to Proxy https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Middleware+to+proxy

[40] CEF Digital, Connecting Europe, eID Documentation. Use case: Middleware to Middleware https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Middleware+to+Middleware

[41] De Maria, A – Ranise, S., Agenda Digitale, 2019, Cie 3.0, tutti gli usi digitali della nuova carta d'identità https://www.agendadigitale.eu/cittadinanza-digitale/cie-3-0-tutti-gli-usi-digitali-della-nuova-carta-didentita/

[42] Dragoni, G – Gastaldi, L – Portale, V, Agenda Digitale, 2021, SPID (Sistema Pubblico di Identità Digitale), cos'è, a cosa serve e come creare un account https://www.agendadigitale.eu/cittadinanza-digitale/a-che-punto-e-il-sistema-pubblico-dell-identita-digitale-e-a-che-serve/

[43] International Bank for Reconstruction and Development/The World Bank, 2018, Technology Landscape for Digital Identification https://thedocs.worldbank.org/en/doc/199411519691370495-0090022018/original/TechnologyLandscapeforDigitalIdentification.pdf

[44] European Commission, Electronic Identification https://digital-strategy.ec.europa.eu/en/policies/electronic-identification

[45] How to make your EU login account ready to log in using 2-factor authentication. Access to microdata application system https://ec.europa.eu/eurostat/documents/203647/771732/EU_Login_Tutorial/

[46] CEF eID SMO, Version 1.0, May 2020, Trends in electronic identification – Embracing mobile identification for eGovernment https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Embracing+mobile+identity+for+eGovernment?preview=/232688243/232688247/Trends%20report%20on%20electronic%20identification_Mobile_FINAL.pdf

[47] Torroglosa E., 2018, LEPS D3.1 Mobile ID App and its integration results with the Industrial Partners http://www.leps-project.eu/node/343

[48] CEF Digital, Connecting Europe, New notified eID schemes in 2020 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2020/12/17/New+notified+eID+schemes+in+2020

[49] Nem ID https://www.nemid.nu/dk-en/

[50] CUERPO NACIONAL DE POLICÍA, DNI y Pasaporte https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_035&id_menu=21[6]https://www.digid.nl/en/

[51] Autenticacao Government website https://www.autenticacao.gov.pt/web/guest/a-chave-movel-digital

[52] CUERPO NACIONAL DE POLICÍA , Descripción DNI 3.0 https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_103&id_menu=1

[53] CUERPO NACIONAL DE POLICÍA, Cuáles son https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_035&id_menu=21

[54] eIDAS Technical Sub-group, 28 October 2016, eIDAS SAML Attribute Profile v. 1.1

[55] AML Directive - DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L0849&from=EN#d1e40-73-1

[56] GitHub, Architecture and Common Datatypes, https://github.com/erasmus-without-paper/ewp-specs-architecture

[57] Katalon, An all-in-one test automation solution, https://www.katalon.com/?pk_abe=AB_testing_Homepage_11_2020&pk_abv=layout1

[58] ESMO project, GRANT AGREEMENT UNDER THE CONNECTING EUROPE FACILITY (CEF) - TELECOMMUNICATIONS SECTOR AGREEMENT No INEA/CEF/ICT/A2017/1451951) https://www.esmo-project.eu/

[59] Information Commissioner's office – ICO, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/#data_minimisation

[60] European Commission website, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/how-should-my-consent-be-requested_en

[61] A&L Goodbody - The GDPR: A Guide for Businesses, https://www.algoodbody.com/media/TheGDPR-AGuideforBusinesses1.pdf

[62] Workgroup: eKYC-IDA, openid-connect-4-identity-assurance-1_0-11, 6 July 2020, https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html

[63] Websites: https://www.javainuse.com/spring/springboot-microservice-elk , retrieved 2020-09-24

[64] Websites: https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html, retrieved 2020-10-19

[65] Websites: https://openid.net/specs/openid-connect-discovery-1_0.html, retrieved 2020-10-19

[66] Websites: https://openid.net/specs/openid-connect-registration-1_0.html#ClientRegistration, retrieved2020-10-19

[67] Websites: https://openid.net/specs/openid-connect-core-1_0.html, retrieved2020-10-19

[68] Websites: https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html, retrieved2020-10-19