increasinG tRust with eId for Developing buSiness

D4.1 Business Use Case Definition

Document Identification			
Status	Final	**Due Date**	30/11/2020
Version	1.0	**Submission Date**	30/11/2020

Related Activity	Act 4	**Document Reference**	D4.1
Related Deliverable(s)	-		
Lead Participant	ICERT KOMPANY	**Lead Author**	Cristina Andreoli (ICERT) Dominik Tiefenbacher (KOMPANY)
Contributors	ICERT ATOS KOMPANY ADACOM UAEGEAN	**Reviewers**	1st reviewer - Petros Kavassalis, UAEGEAN 2nd reviewer - Konstantinos Noussias, ADACOM

Keywords
eIDAS, AML, KYC, KYB, GRIDS, Aggregate, BAA

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.

Document Information

List of Contributors	
Name	Partner
Cristina Andreoli	ICERT
Dominik Tiefenbacher	KOMPANY
Carina Wolf	KOMPANY

Document History			
Version	Date	Change editors	Changes
0.1	22/10/2020	Cristina Andreoli (ICERT)	Preparation of the document structure; First draft of the Table of Content.
0.2	26/10/2020	Carina Wolf	First contribution to assigned sections
0.3	02/11/2020	Carina Wolf	Completion of assigned sections
0.4	18/11/2020	Cristina Andreoli	Insertion of Introduction and Conclusions
0.5	24/11/2020	Petros Kavassalis	Reviewed and updated document
0.6	25/11/2020	Konstantinos Noussias	Reviewed and updated document
0.7	26/11/2020	Constantinos Pretenteris	Final review and add references section
0.8	26/11/2020	Cristina Andreoli	Last adjustments and drafting of clean version
1.0	30/11/2020	Carmen San Román	FINAL VERSION TO BE SUBMITTED

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Cristina Andreoli (ICERT)	20/11/2020
Peer reviewers	1st reviewer - Petros Kavassalis, UAEGEAN 2nd reviewer - Konstantinos Noussias, ADACOM	24/11/2020 25/11/2020
Quality Manager	Carmen San Román	29/11/2020

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AML	Anti Money Laundering
EC	European Commission
DC	Data Consumer
DP	Data Provider
DS	Data Subject
CDD	Customer due diligence
eIDAS	Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market
FIs	Financial Institutions
KYB	Know Your Business
KYC	Know Your Customer
LEI	Legal Entity Identifier
LOU	Local Unit Operator

Executive Summary

GRIDS identifies the importance of bundled services for worldwide commerce, business and financial sectors that require you to "Know Your Customer" and therefore identify the latter through an international accepted eIDAS eID system. For this reason, part of the project focuses on the following, existing services, whose addressable market is really large and will have a significant growth, especially due to the Covid pandemic period.

With the ultimate goal of demonstrating the applicability and benefits of the GRIDS architecture for obtaining KYC information in conjunction with cross-border eIDAS eID services in processes of private companies in different countries, the following three use cases and related needs have been examined:

- Onboarding of business accounts by Banks / Financial Institutions (FIs): the banking sector is the most involved in due diligence and KYC processes since it has to comply with AML/KYC regulations and prevent any illicit use of their services from fraudulent actors like financing terrorist and money laundering. In order to be able to do so, banks and FIs need an efficient onboarding process capable of gathering and validating company details and reports, but also to identify and verify associated natural persons, especially directors and officers acting on behalf of the legal entity. All of the above can be achieved through GRIDS to help banks and FIs gain a competitive advantage in the market.
- KYC Data for Legal Entity Identifier Checks: the Legal Entity Identifier (LEI) is uniquely connected to key reference information of legal entities. Before issuing any alphanumeric code, the various Local Unit Operators (LOU) need to perform quick and exhaustive checks and validations not only regarding up-to-date company details, data and documents, but also with respect to the signing authority. Especially, with LEI Level 2, LOU are required to investigate the final and ultimate parent companies of LEI applicants as well.
- KYC Checks for Business Sectors other than Banking and Finance: other business sectors, such as lawyers, notaries, etc., are required by law or might even voluntarily perform an AML and Due Diligence check on their customers. In order to facilitate this process without compromising its credibility, it is important to have access to up to date and primary source data. The access to KYC information via GRIDS, based on eIDAS eID, is expected to significantly reduce the effort required and guarantee the quality of the service.

With the consultation of three external parties, Raiffeisen Bank International WM Datenservice as a LOU and the law firm Advokat, the partners involved in GRIDS project have highlighted several benefits resulting from the integration of eIDAS eID with KYC data providers. More specifically, the most important immediate gains identified from interfacing eIDAS-eID with KYC providers is the realization of a single digital market inside the EU (thus allowing individuals and companies all over the EU to access cross border financial services) and of course the reduction of costs and manual work needed to verify the information of legal and natural persons which is an integral part of such services.

Nevertheless, all such endeavours contain risks. Indeed, scepticism of those involved in the potential market might impact the adaptation of their systems to the new eID structures and international structure.

1 Introduction

1.1 Purpose of the document

This document refers to the Activity 4 – End User APIs for Business Users of GRIDS Services, and more specifically to task 4.1 dedicated to 'Defining business use cases in depth (Banking, e-Commerce, Supporting Services)'.

Within this document, three use cases are defined for immediate use of bundled KYC and eIDAS based identity verification services. The following chapters will demonstrate the capacity and maturity of GRIDS offerings.

1.2 Reference to other project work

This document is strictly connected to the Activity 2.1 Business Service Definition. While the latter presents a general definition and overview of GRIDS regarding legal and compliance aspects, within this document the analysis has been focused on the most significant use cases only.

A further analysis regarding GRIDS benefits and market/marketing studies will be performed for the Activity 6 during Milestone 11 – Market Analysis and GRIDS Benefits.

1.3 Structure of the document

This document is structured in 4 major chapters.

Chapter 3 presents a general workflow diagram applicable to the 3 use cases analysed.

Chapter 4 presents the first Use Case: "Onboarding of business accounts by Banks / Financial Institutions (FIs)". This Use Case highlights the benefits of integrating KYC services and eIDAS eID to simplify onboarding processes of business accounts and minimize risk of fraud and time spent for the required identification processes.

Chapter 5 presents the second Use Case: "KYC Data for Legal Entity Identifier (LEI) Checks". This Use Case highlights the way that the integration of the existing Legal Entity Identifier (LEI) check mechanisms and eIDAS based eID services support a faster and potentially more secure data verification framework for legal entities and related legal representatives for Local Unit Operator (LOU) issuing LEIs in all EU countries.

Chapter 6 presents the third Use Case: "KYC Checks for Business Sectors other than Banking and Finance". This Use Case demonstrates the way to accelerate the business transactions in the context of paneuropean eTrade system while retaining trust in the system via the provision of comprehensive KYC information together with eIDAS eID based access.

2 Use Cases General Introduction

The steady growth of the online market and the necessity of fintech businesses and e-commerce platforms to broaden the base of clients, requires the use of Know Your Customer (KYC) services for onboarding processes and cross-border business with other clients. In this context trust is crucial for private sector businesses development, as well as fulfilling with the regulatory framework avoiding fraud.

GRIDS will create a KYC-business value network and new generation of "KYC as a Service" offerings to enable key private players in different sectors across Europe to effectively and simultaneously access and process KYC Intelligence and eIDAS identity information, generating very high cost and time savings in due diligence procedures e.g. for online customer onboarding or LEI checks.

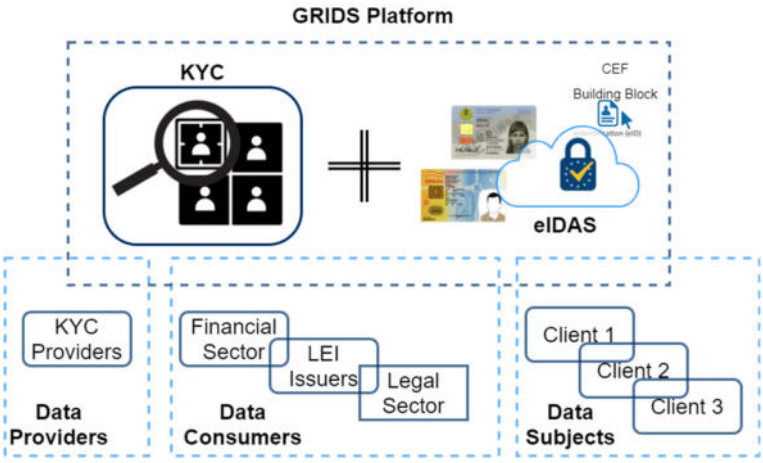


Figure 1: GRIDS Platform

The main objectives GRIDS will achieve, especially in the presented Use Cases, are:

- Showcase how digital KYC providers can use eIDAS identity verification to create and maintain a consistent single view of their customers
- Perform effective and accurate screening of customers
- Preventing and recognizing financial crimes
- Increasing the operational efficiency of anti-money laundering, counter-terrorist financing and more

In order to develop this ecosystem, GRIDS will:

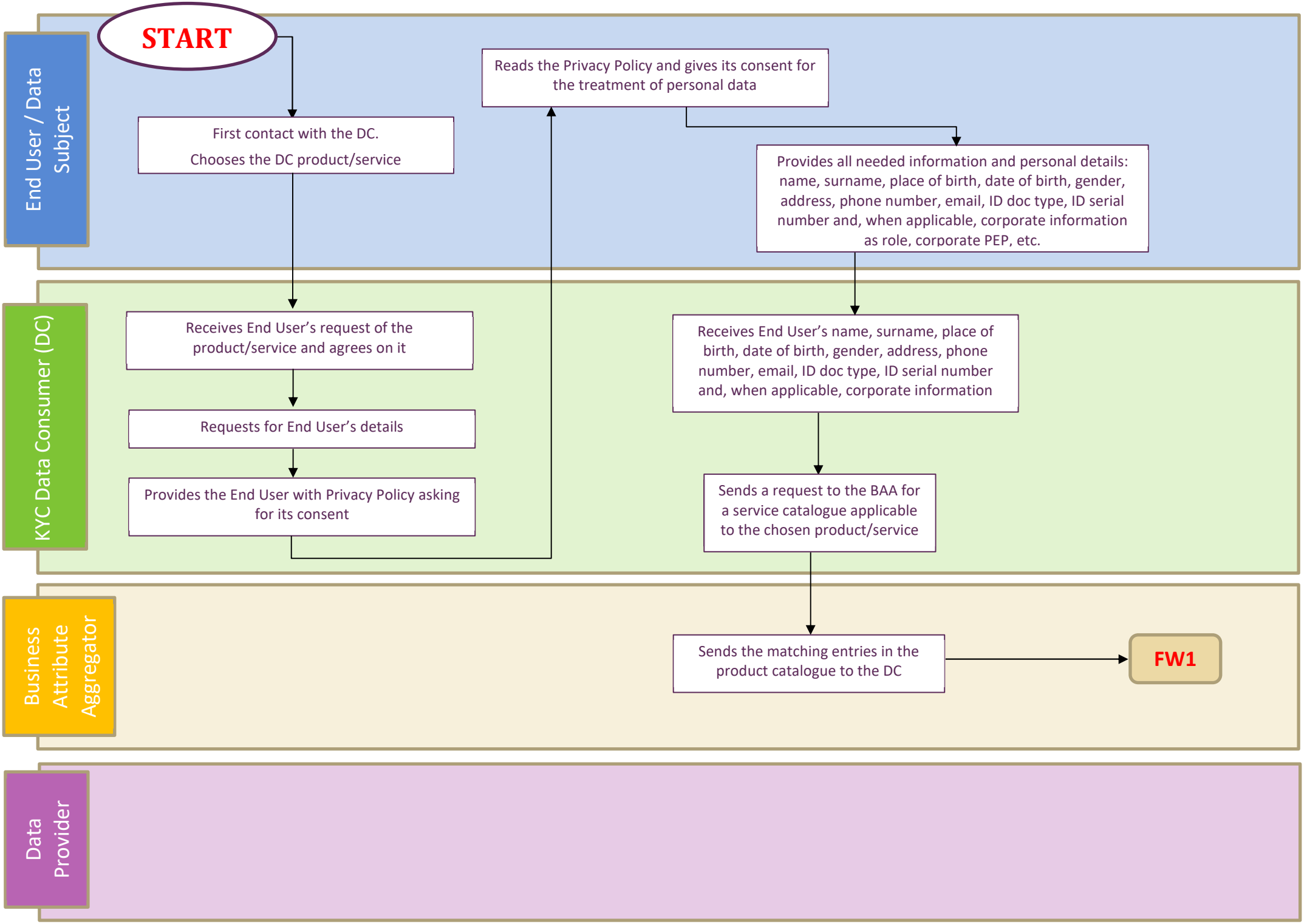
- Leverage the eIDAS interoperability of eID with a high Level of Assurance, which will increase the trust in business and facilitate to satisfy the regulatory requirements.
- Allow cross-border interoperability across Europe.
- Create a business infrastructure by establishing a business network between KYC providers, customers and end-users

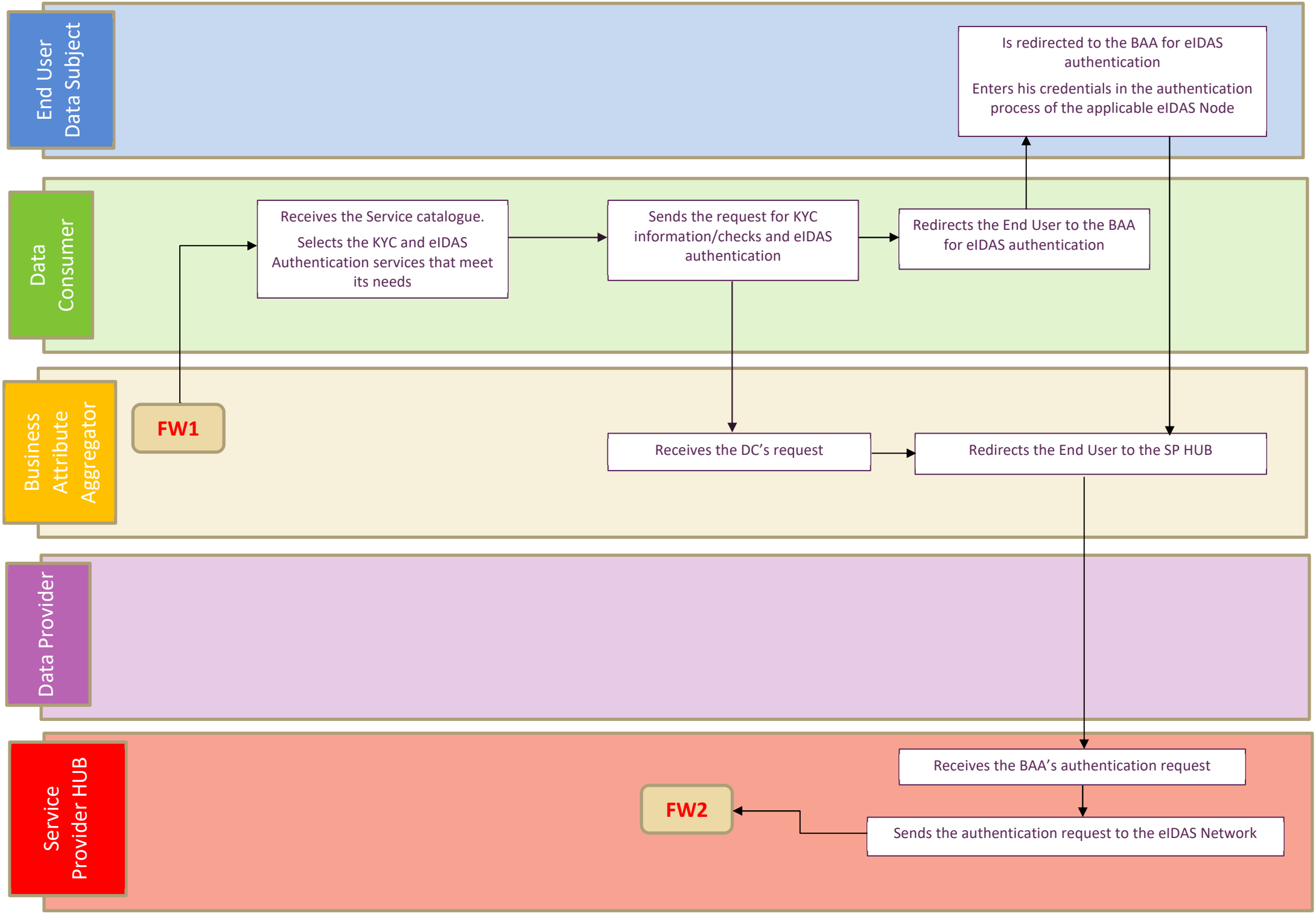
3 Workflow of Use Cases

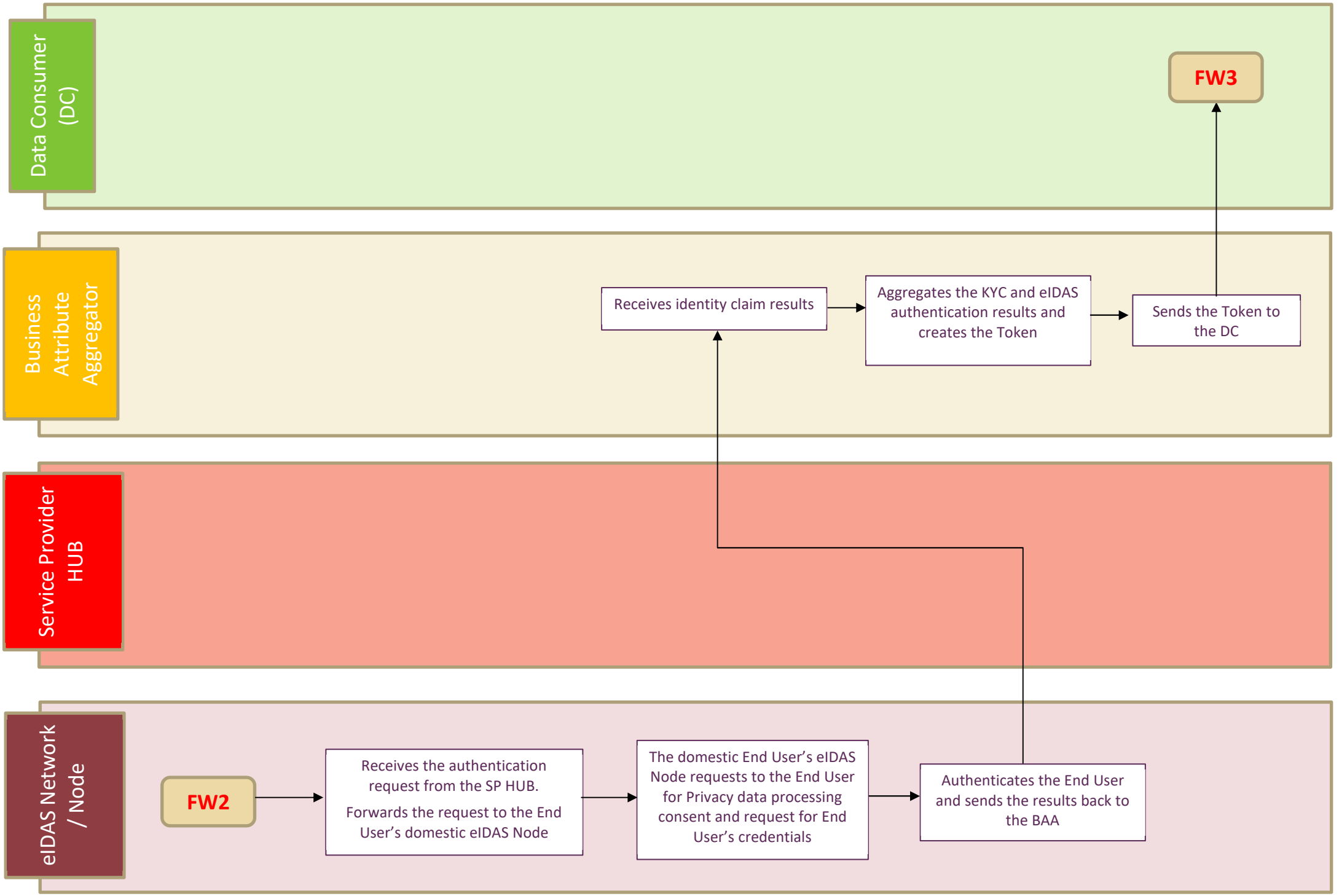
To better understand the GRIDS process applicable in all Use Cases, within this chapter you will find a workflow where each action of all parties involved are step by step represented and connected.

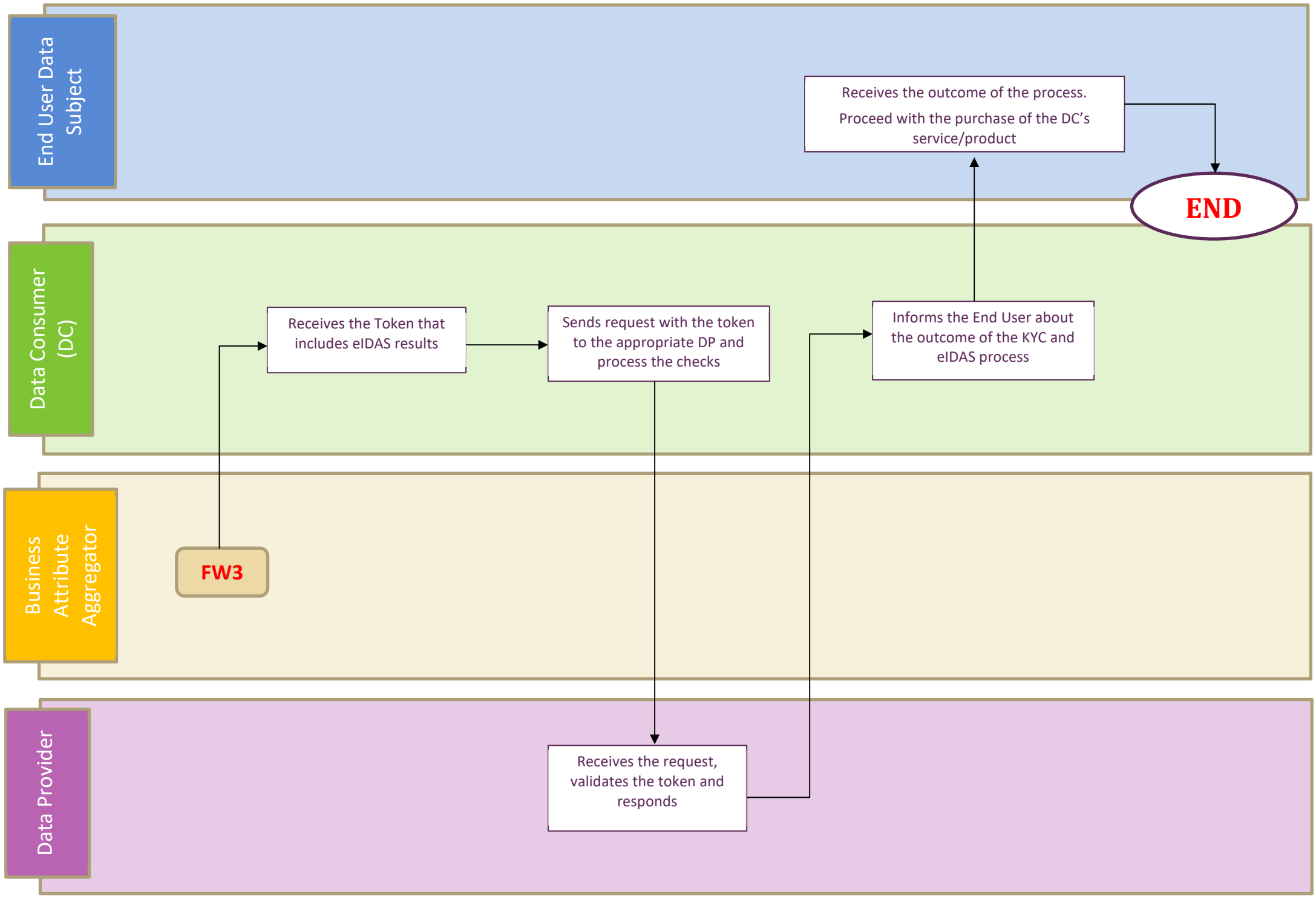
The coloured rows represent each stakeholder involved, starting from the End User/Data Subject (blue) who comes into contact with the Data Consumer (green) for the purchase of a specific product, including but not limited to the opening of a bank account, financial service, LEI code, consultation, etc.

The Data Consumer sends a request to the BAA (yellow) and the latter redirects the Data Consumer to the relevant Data Provider (purple), Service Provider HUB (red) and eIDAS network/node (dark red). The BAA delivers eIDAS results back to the Data Consumer and provides an access token which is used by the Data Consumer to access the Data Providers to complete the checks necessary for the Data Provider to perform their due diligence and KYC.


START
End User / Data Subject
First contact with the DC.
Chooses the DC product/service
Reads the Privacy Policy and gives its consent for the treatment of personal data
Provides all needed information and personal details: name, surname, place of birth, date of birth, gender, address, phone number, email, ID doc type, ID serial number and, when applicable, corporate information as role, corporate PEP, etc.
KYC Data Consumer (DC)
Receives End User's request of the product/service and agrees on it
Requests for End User's details
Provides the End User with Privacy Policy asking for its consent
Receives End User's name, surname, place of birth, date of birth, gender, address, phone number, email, ID doc type, ID serial number and, when applicable, corporate information
Sends a request to the BAA for a service catalogue applicable to the chosen product/service
Business Attribute Aggregator
Sends the matching entries in the product catalogue to the DC
FW1
Data Provider


End User
Data Subject
Is redirected to the BAA for eIDAS authentication
Enters his credentials in the authentication process of the applicable eIDAS Node
Data Consumer
Receives the Service catalogue.
Selects the KYC and eIDAS Authentication services that meet its needs
Sends the request for KYC information/checks and eIDAS authentication
Redirects the End User to the BAA for eIDAS authentication
Business Attribute Aggregator
FW1
Receives the DC's request
Redirects the End User to the SP HUB
Data Provider
Service Provider HUB
Receives the BAA's authentication request
FW2
Sends the authentication request to the eIDAS Network


Data Consumer (DC)
FW3
Business Attribute Aggregator
Receives identity claim results
Aggregates the KYC and eIDAS authentication results and creates the Token
Sends the Token to the DC
Service Provider HUB
eIDAS Network / Node
FW2
Receives the authentication request from the SP HUB.
Forwards the request to the End User's domestic eIDAS Node
The domestic End User's eIDAS Node requests to the End User for Privacy data processing consent and request for End User's credentials
Authenticates the End User and sends the results back to the BAA


End User Data Subject
Receives the outcome of the process.
Proceed with the purchase of the DC's service/product
END
Data Consumer (DC)
Receives the Token that includes eIDAS results
Sends request with the token to the appropriate DP and process the checks
Informs the End User about the outcome of the KYC and eIDAS process
Business Attribute Aggregator
FW3
Data Provider
Receives the request, validates the token and responds

4 Use Case n° 1 – Onboarding of Business Accounts by Banks / Financial institutions

4.1 High level description

There are currently two trends in the financial industry with regards to Anti-Money Laundering following the EU's AMLD4 and AMLD5 regulation.

The first is the need to automate B2B clients on-boarding and continuously monitor to reduce a) the on-boarding costs and b) the on-boarding duration.

The second trend is the move from the use of static company information to real-time data, i.e. instead of secondary sources and company information retrieved from third-party static databases, such as credit reporting agencies, start using real-time primary source data.

Automated B2B onboarding provides cost reduction by at least 50% (examples: from EUR 500 to EUR 250 or even less) and a duration reduction from weeks to only a few days, or even instant. The main three gaps in B2B onboarding automation today are:

- identification of the legal representation of the entity,
- legal representatives signing and
- (EU) cross-border acceptance.

Even if a financial institution offers digital B2B on-boarding, the contract itself is usually still required to be signed on paper or a signed contract is provided as a scan and send to the counterparties (e.g. via email). eIDAS will play a crucial role in providing the entity and the directors or authorized representative verification while also the option to electronically sign all account opening contracts.

Table 1: Use Case no. 1 Data

Who is the user of the service?	Who is the provider of the service? (KYC Data Consumer)	Identification target	Use KY data for?	GRIDS also provides	Reference business - Partner (KYC Data Consumer - raw2)
Any type of business -- including SMEs	Banks and Financial Institutions (FIs) -- including PSD2 Payments Institutions	Natural persons (Company's Legal Representative, managers, directors, etc.) Legal persons (in the future)	Company check -- authoritative and audit-proof company filings etc.	Authorization management for account administration and contract signing	Raiffeisen Bank International - AT (subsidiaries in 10+ CEE countries)

4.1.1 Involved parties and their role

- Data Consumer (DC): Financial institutions and all addressees of the AMLD regime (so-called "obliged entities")
- Data Subject (DS): DC's business customer
- Data Provider (DP): data provider will be the eIDAS system when it comes to identification phase of the data subject and the national company registries for authentication of the information provided by the data subject

4.2 Benefits and Risks

4.2.1 Benefits for involved parties

The advantages of implementing the aforementioned use case via GRIDS architecture are described below, separated for each entity involved:

- Data Consumer (DC):
  - Chance to gain access to new market and - hence - new potential customers which will result in customer base & revenue increase;
  - Faster and automated onboarding process which leads to a decrease in costs (this can be considered a significant advantage of integrating with GRIDS as compliance costs are considered an important resource constraint for all financial institutions);
  - DC are able to use a one stop shop solution, instead of lengthy and costly physical ID check
  - Replace of video ID checks (for which DC usually pays a third-party provider). Video ID check is a quick and efficient mean of onboarding clients, but highly susceptible to corruption;
  - Competitive advantage compared to "traditional" AML processes (because of all reasons outlined above);
  - eID information about directors/ officers / trustees / other persons with signatory rights and if needed also for other persons, such as shareholders, by utilizing the eIDAS eID legal person identification features.
- Data Subject (DS):
  - Choose the "best" offer within EU and not only one jurisdiction, namely their home country;
  - Reduce barriers for DS in terms of borders (by accepting an identification process with one official "EU ID" = eID)
  - Quicker on-boarding process which results in better customer journey
- Data Provider (DP):
  - Reduce barriers that hold back the growth of the EU Digital Single Market (DSM);
  - Consolidation of the eIDAS / eID ecosystem and an attractive eID use case;
  - Implementing improved AML & CTF precautions and an EU-wide compliance standard;
  - Implementing a best-standard practice for compliance procedures;
  - Participation and collaboration in EU wide project.

4.2.2 Risks and changes for involved parties

Nevertheless, alongside benefits there are some unavoidable prerequisites to implementing the Use Case and additionally, risks to be considered. These risks (presented below) will be evaluated during the project.

- Prerequisites:
  - DS should acquire eID from its governmental issuing authorities and start using it;
  - DC should accept and - hence - implement eID identification checks and/or GRIDS process. Such acceptance is possible only if enough DS use eID;
  - Requirements of an EU wide, safe and trustworthy AML compliance standards and therefore a chance to implement a best practice model.

- Risks:
  - DS are not willing to get another official ID document (in addition to driver license, passport, standard ID card);
  - DC does not see enough market potential and - hence - no Use Case (profit vs costs).

4.3 Legal aspects

This section contains a brief overview of the Regulations that are applicable to this use case.

Table 2: Use Case no. 1 Legal Aspects

Regulation	GRIDS Compliance
eIDAS	eIDAS regulation introduces a safe and trustworthy system to identify natural persons and entities EU-wide. As entities are usually represented by natural persons appointed to act as management for such entity, eID can include such information. This means that eID includes information on the natural person while also on the natural person's power of representation regarding entities. GRIDS foresees that a DS has to identify itself via eID in accordance with eIDAS regulation. Such identification via eID is the precondition to use GRIDS and does not only meet the AML requirements for customer identification but also provides a mean of an efficient way to identify the authorized representatives of an entity.
GDPR	GRIDS processes inter alia personal data by automated means. Hence, the EU-wide applicable GDPR regime needs to be considered. In order to meet the GDPR requirements, a DS has to accept the GRIDS privacy policy prior any further use of the GRIDS services. However, a DC has prevailing interest when it comes to information for its CDD. Same applies for DP when it comes to information for compliance purposes. As a result, GRIDS and the DC can also base their use of personal data on "prevailing interests" (legal and compliance requirements) in accordance with Article 6 (c) and (f) of GDPR.
AML	The EU AMLD regime states obligation in order to prevent AML and CTF. One core principle of the regime is that a prospect customer of a DC has to be identified and verified prior any commence of business relations (so-called customer due diligence = CDD). The AMLD regime requires a CDD including a safe and trustworthy identification of the DS and verification of DS's information. GRIDS foresees the use of eID for the identification of a DS. This identification process complies with AMLD requirements. Furthermore, the data and information provided by DP origin from primary sources in real-time and audit proof form, satisfies the CDD requirement in terms of verification. Consequently, GRIDS provides an AML-compliant service for the CDD of DC.

5 Use Case n° 2 – KYC Data for LEI Checks

5.1 High level description

At the G20 Summit that was held in Cannes back in 2011, the members requested that the Financial Stability Board should establish a global framework for a Legal Entity Identifier (LEI). These LEIs are issued by LOUs, who in turn are required to fully KYB legal entities, funds, foundations, public companies, etc. applying for or renewing a LEI. Until recently, this process was manually performed, but digital and automated on-boarding has become the norm for most of the top 5 LEI-issuers.

With the new LEI regulation (Level2, so called 'full validation'), full identification of the legal entity will be required. The identification of legal entity through eIDAS will allow for the continuation of a fully automated KYB for the issuance of the LEI.

- LEI is the acronym of Legal Entity Identifier. It is a 20-character, alpha-numeric unique EU wide company ID thanks to which, Legal Entity can be easily identified. It connects to key reference information that enables clear and unique identification of legal entities participating in any business or financial transactions[1].
- LEI issuance is performed by a Local Operating Unit (LOU)
- The company WM Datenservice that will participate in GRIDS project is a LOU
- LOU needs to perform KYC checks similar to banks (see Use Case no. 1 at chapter 4) before LEI issuance
- Benefit: Integration of eIDAS to existing LEI check mechanisms
- Major time saving factor and (signing authority) data verification for LOU

Table 3: Use Case no. 2 Data

Who is the user of the service?	Who is the provider of the service? (KYC Data Consumer)	Identification target	Use KYC data for?	GRIDS also provides	Reference business (KYC Data Consumer - raw2)
Financial Institutions (FIs), funds and others require to obtain or renew a LEI	Legal Entity Identifier (LEI) issuers -- also referred as Local Operating Units (LOUs)	Natural persons (Company's Legal Representative) Legal persons (in the future)	Exhaustive checks of company vitals and documents before issuing a LEI	Authorization of managers/directors for signing organizational charts in notarized manner	WM Datenservice - DE (serving 10+ EU countries)

[1] Into LEI subject, important role is played by the Global Legal Entity Identifier Foundation (GLEIF), a supra-national not-for-profit organization which support and manage the implementation and use of the Legal Entity Identifier (LEI); please visit GLEIF website for further information https://www.gleif.org/en/

5.1.1 Involved parties and their role

- Data Consumer (DC): LOU
- Data Subject (DS): All entities required by law to obtain a LEI code (e.g. entities involved in trading financial instruments, issuers of financial instruments, entities participating in over-the-counter or exchange-based derivatives trading, listed companies)
- Data Provider (DP): Data provider will be the eIDAS system when it comes to identification phase of the data subject and the national company registries for authentication of the information provided by the data subject

5.2 Benefits and Risks

5.2.1 Benefits for the involved parties

As per the previous Use Case, within this analysis different advantages have been identified too. Below these are defined for each party involved in the use case:

- Data Consumer (DC):
  - faster onboarding process which also means cost reduction
  - potential replacement of lengthy and costly physical ID check
  - potential replacement of video ID check (see above use case No 1)
  - competitive advantage compared to “traditional” AML processes
  - eIDAS-eID based trusted information about directors/ officers / trustees / other persons with signatory rights
- Data Subject (DS):
  - reduce existing barriers in terms of borders (identification process with on official “EU ID” = eID)
  - quicker onboarding process which leads to a better customer journey
  - reduce time and costs in the sphere of the DS
- Data Provider (DP):
  - reduce barriers that hold back the EU Digital Single Market (DSM) growth
  - eIDAS / eID ecosystem consolidation
  - AML & CTF precautions and EU-wide compliance standard
  - Implementing a best-standard practice
  - EU wide project participation and collaboration

5.2.2 Risks and changes for involved parties

For KYC data checks for LEI issuance the same prerequisites and risks as per Use Case No 1 have been identified.

5.3 Legal aspects

This section contains a brief overview of the Regulations that are applicable to this use case.

Table 4: Use Case no. 2 Legal Aspects

Regulation	GRIDS Compliance
eIDAS	Same pursuant to Use Case No 1 (see above)
GDPR	Same pursuant to Use Case No 1 (see above)
AML	The regime implemented by G-20 Summit foresees for LOUs obligation to identify and verify their customers prior issuing a respective LEI code. GRIDS foresees the use of eID for the identification of a DS. This identification process complies with the obligations of LOUs. Furthermore, the data and information provided by DP origin from primary sources in real-time and audit proof form, satisfies CDD requirements in terms of verification. Consequently, GRIDS provides a G20 regime-compliant service for the CDD of DC.

6 Use Case n° 3 – KYC Checks for Business Sectors other than Banking & Finance

6.1 High level description

LegalTech companies, such as Advokat[2], offer cloud services for lawyers and law firms. The features that such companies usually offer include client management, invoicing and billing, case file management, document management and digital court filings. The KYC (natural persons) and KYB (legal entities and representatives) is still conducted manually by passport viewing and verifying a commercial register extract's content while validating the contents as a trusted third party. Additionally, for commercial transactions or transactions falling under commercial law, often a notary has to verify and identify a legal entity. EU cross-border transactions always require an apostilled commercial register extract, and apostilled passport copy of the legal representative. This manual verification and identification process are time-consuming and costly for business. By integrating eIDAS natively into their systems LegalTech companies and law firms could automate the onboarding of business clients and could also alleviate the need for apostilled documents (cross-border) or even notaries for local transactions. The costs could be reduced by EUR 35 – 250 per onboarding and the onboarding cycle could be reduced from a week down to same day or even instant.

- AML/KYC regulations are not only applicable to banks / financial institutions, but to many more sectors (like Professionals as lawyers and notaries, Real Estate, Virtual Assets, etc.)
- Requirements are very similar to Use Case 1 (RBI/Financial Industry)

Table 5: Use Case no. 3 Data

Who is the user of the service?	Who is the provider of the service? (KYC Data Consumer)	Identification target	Use KYC data for?	GRIDS also provides	Reference business (KYC Data Consumer - raw2)
Any type of business -- including SMEs	Legaltech services & platforms, Supply Management Platforms, Domain Name Registrars	Natural persons (Company's Legal Representative, managers, directors, authorized persons etc.) Legal persons (in the future)	Supply Chain Network verification Due diligence checks on applicants, especially of the authorized representatives	Verify directors and authorize them for signature	Advokat - AT (specialized on serving AT market customers)

6.1.1 Involved parties and their role

- Data Consumer (DC): legal industry and all other industries obliged to comply with AML/CTF obligations (in accordance with national law requirements)
- Data Subject (DS): DC's customers
- Data Provider (DP): data provider will be the eIDAS system when it comes to identification phase of the data subject and the national company registries for authentication of the information provided by the data subject

[2] Advokat is a provider of software solutions for lawyers (customer database, case management, time recording, courts communication, file evidence, etc).

6.2 Benefits and Risks

6.2.1 Benefits for the parties involved

The advantages of implementing this use case via GRIDS architecture, separated for each entity involved are the following:

- Data Consumer (DC):
  - Faster onboarding process which leads to cost reduction
  - Replacement for lengthy and costly physical ID check
  - Replacement for video ID check (see above use case No 1)
  - Provide a competitive advantage compared to “traditional” AML processes
  - Provides information via eID about directors/ officers / trustees / other persons with signatory rights
- Data Subject (DS):
  - Reduction of existing barriers in terms of borders (identification process with on official “EU ID”)
  - Quicker onboarding process which results in a better customer journey
  - Faster way of customer onboarding process and cost reduction in in the sphere of the DS. Additionally, potential reduction in extra fees from the use of such services
- Data Provider (DP):
  - Reduction of barriers that hold back the Digital Single Market (DSM) growth
  - eIDAS / eID ecosystem consolidation
  - AML & CTF precautions and EU-wide compliance standard
  - Implementing a best-standard practice
  - EU wide project participation and collaboration

6.2.2 Risks and changes for involved parties

For KYC data checks in Business Sectors other than Banking & Finance the same modifications and risks as per Use Case No 1 and 2 have been identified.

6.3 Legal aspects

This section contains a brief overview of the Regulations that are applicable to this use case.

Table 6: Use Case no. 3 Legal Aspects

Regulation	GRIDS Compliance
eIDAS	Same pursuant to Use Case No 1
GDPR	Same pursuant to Use Case No 1
AML	The EU AMLD regime states obligation in order to prevent AML and CTF. With AMLD4 the requirements for the legal sector where aligned with the AML obligations of FIs which means that AMLD4 stated for the legal sector similar AML/CTF-obligations. Hence, the legal sector has - based on national law in accordance with the AMLD 4 - to identify and verify its customers prior any commence of business relations. GRIDS foresees the use of eID for the identification of a DS. This identification process complies with AMLD requirements for the legal industry. Furthermore, the data and information provided by DP origin from primary sources in real-time and audit proof form, satisfies the CDD requirement in terms of verification. Consequently, GRIDS provides an AML-compliant service for the CDD of DC.

7 Conclusions

This document described the benefits of adopting the GRIDS architectures in the main Use Cases that are supported by the project. These Use Cases were designed with the collaboration of third parties that were interested in integrating with the GRIDS system. From the conducted analysis it has been made clear that GRIDS can complement and improve services that do not strictly fall in the financial sector but are still subject to anti money laundering checks and have constant KYC needs.

Moreover, some challenges have to be identified. GRIDS may encounter difficulties in terms of market acceptance and the success of GRIDS requires a high acceptance rate from Data Subjects as this will make sure that the Data Consumers will deem it relevant from a commercial point of view to implement it in their compliance systems.

Nevertheless, partners and consulted industry experts strongly believe that there are significant benefits in integrating with GRIDS that overshadowed the potential risks. In particular, the Data Consumers integrated with the platform will be in possession of an AML tool providing a safer, more trustworthy, less time-consuming and money-saving way to identify and verify their customers (Data Subjects). Furthermore, these DCs will be capable of expanding their business to other markets and potential customers for their products and services. The analysis of this report can be the base for further marketing actions as will be exposed in the Activity 6 of the GRIDS project.

Furthermore, the analysis of the three Use Cases will be also developed during activity 5 of the GRIDS project. A testing phase of cross border transactions in financial sector, LEI issuance and professional field will be performed from April 2021 thanks to the collaboration with Raiffeisen Bank International, WM Datenservice and Advokat. Several End Users will have the opportunity to get in contact with GRIDS services.

8 References

[1] Raiffeisen Bank International (www.rbinternational.com)

[2] Advokat (https://www.advokat.at/)

[3] WM Datenservice(www.wmdaten.de)

[4] GLEIF (www.gleif.org)