



INCREASING TRUST
WITH **EID** FOR
DEVELOPING BUSINESS

eID Industry Monitoring Group

End of Project Report Out

GRIDS consortium

10-12-2021



Agreement number: INEA/CEF/ICT/A2019/1926018
Action No: 2019-EU-IA-0044

AGENDA

1. Welcome & Introductions
2. Progress Update & Milestones Achieved
3. Market Context: GRIDS Advantages & Benefits
4. GRIDS Platform High Level Overview
5. GRIDS Demo
6. eIDAS Context & Future Evolution
7. GRIDS Next Steps
8. Open Forum/Q&A



1

Welcome & Introduction

Paul Foster - KOMPANY



Atos



UNIVERSITY OF THE AEGEAN



Agreement number: INEA/CEF/ICT/A2019/1926018
Action No: 2019-EU-IA-0044

GRIDS Industry Monitoring Group



Stéphane MOUY
Independent
Consultant



Arne TAUBER
EGIZ



Clare ROWLEY
GLEIF



Ivan MARIN
GLEIF



Ravenio PARRINI
Banca d'Italia



Sigurður MÁSSON
Advania



Nikolaos SOUMELIDIS
QMSCERT



Eric WAGNER
Raiffeisen Bank Intl



Wil JANSSEN
InnoValor



Torbjörn ULL
Swedish Companies
Registration Office



Kalev PIHL
SK ID Solutions

eKYC & Identity Assurance Working Group



- Serves as a public trust organization
- Represents a global community of independent developers, industry leaders and users
- Steward of the OpenID intellectual property and brand marks
- Leader in global adoption of open internet identity standards



- eKYC and Identity Assurance (eKYC & IDA) WG
- Developing extensions to OpenID Connect
- Standardise the communication of assured identity information
- Verify claims and information about how the verification was done and how the respective claims are maintained

What is GRIDS?

Increasing trust with eID for developing business.

- Part of the European Commission's *Connecting Europe Facility* programme
- Makes it easier for businesses to operate across the EU
- Facilitates cross-border acceptance of e-identification & remote know-your-customer processes
- Enables both regulated & unregulated entities to identify consumers digitally
- Fully complies with anti-money laundering & data protection regulations
- Making full use of the electronic identification & authentication tools provided by eIDAS.





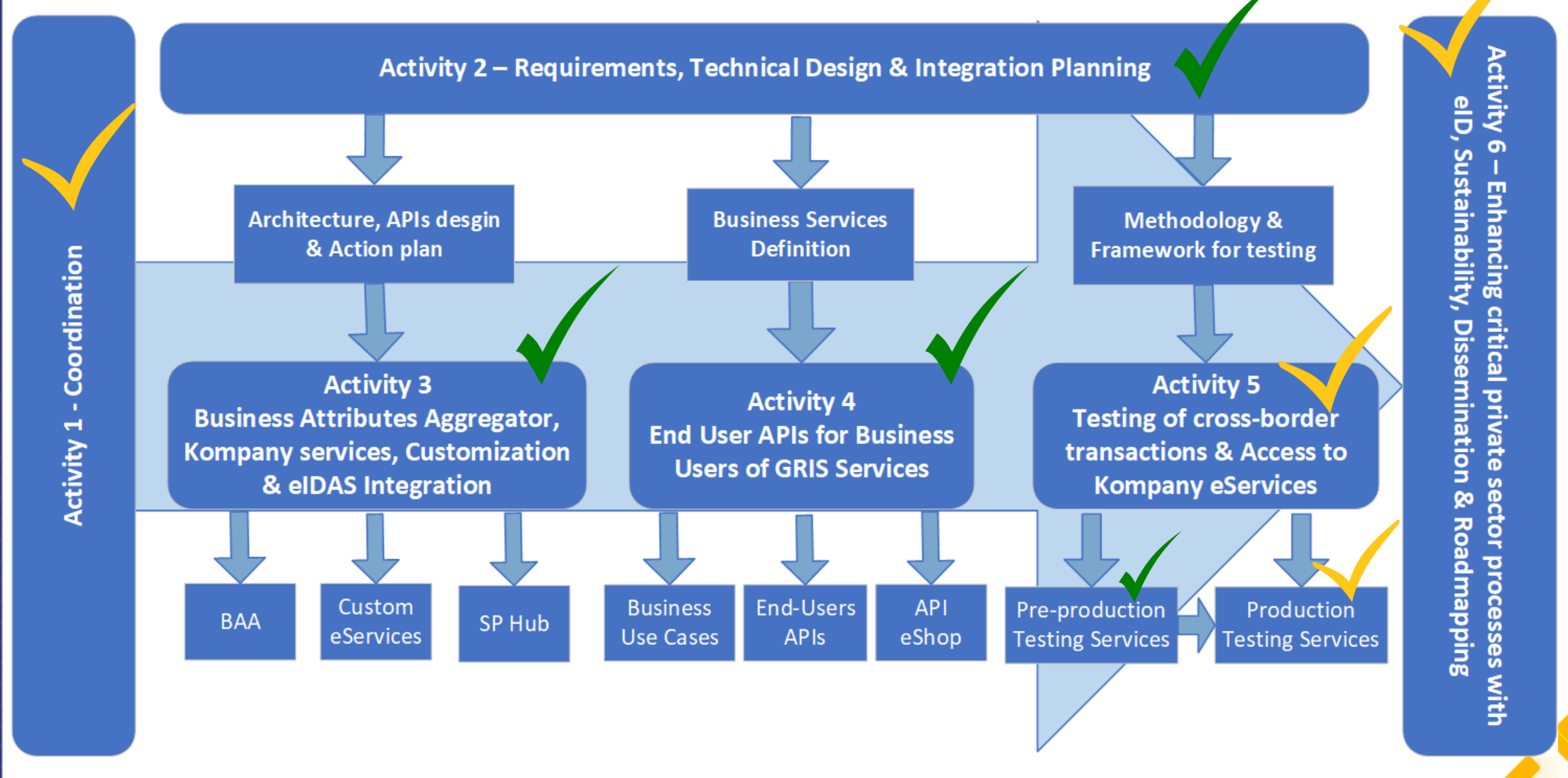
2

GRIDS Progress Overview & Milestones Achieved

Juan Carlos Perez Baun - ATOS



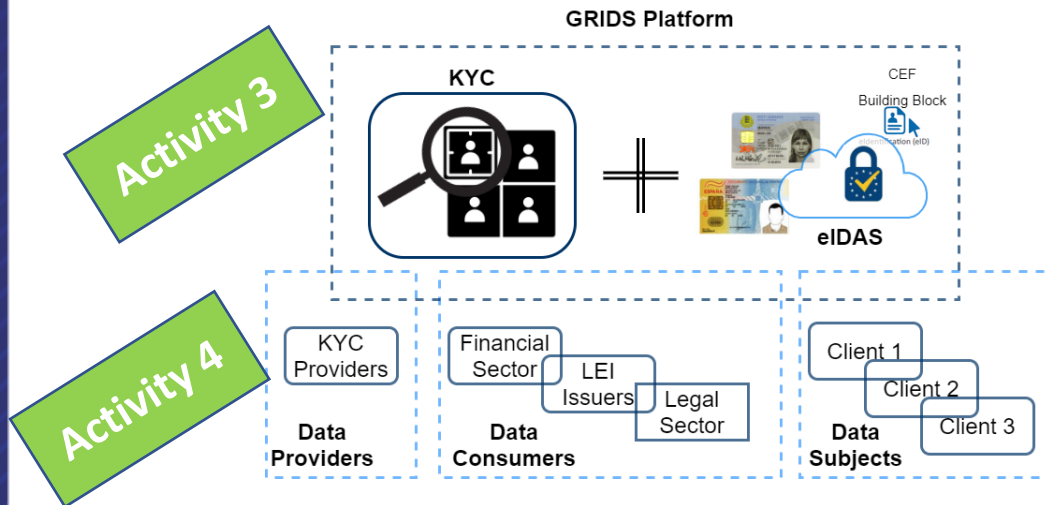
Activities & Dependencies



Objectives & Achievements

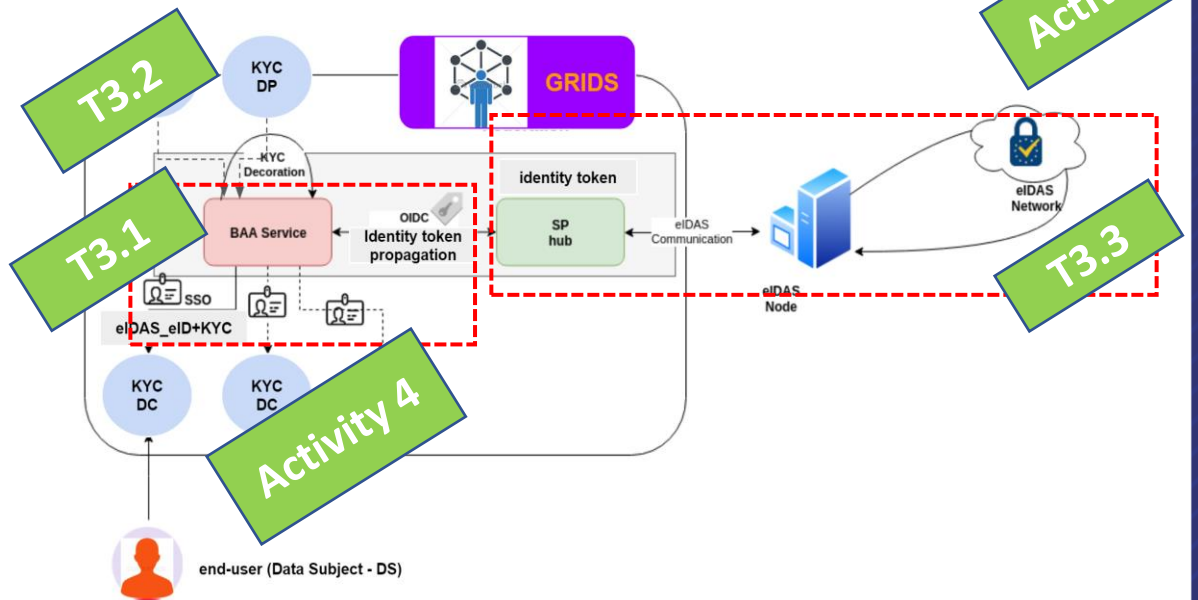
Initial Objectives

Bundle together KYC data with the eIDAS identification process, achieving enhanced KYC due diligence operations in multiple business scenarios.



Achievements

Business Services Definition and technical architecture



Created **SP HUB** to provide eIDAS authentication functionality & **BAA**, which will enrich data from KYC sources resulting in a token “eIDAS eID + KYC data to be shared with KYC data consumer

Created **SDK** for SSO-based integration of end-users to connect with “eIDAS enabled, KYC-as-a-service” project standard offerings

Created **e-shop** for the provision of these APIs, proving a single access point to the relevant documentation

Build a platform that **re-uses and extends** the functionality of the **eID DSI**. Propagate the identity information and the eIDAS authentication token.



Create a business network between KYC providers (DPs), customers from financial, LEI issuing and Legal sector (DCs) and the clients of these industries (Data subjects).



Objectives & Achievements

Initial Objectives

Demonstrate the applicability of eIDAS eID DSI in the onboarding processes of the private companies in different countries and to illustrate the potential of using cross-border eID services in conjunction with KYC information dissemination.

Assess specific benefits of CEF eID for private sector stakeholders to maximize trustworthiness of critical processes (remote onboarding, KYC/AML compliance, etc.) and adoption of cross-border identification and authentication services.
Also look into the sustainability of the action's results and ensure its dissemination.

Achievements

Developed 3 services:

- Onboarding of business accounts
- KYC data for LEI checks
- KYC checks for businesses beyond finance

Activity 4

- Perform automated test
- Services tested by 5 live testers from different EU countries: Greece, Spain, Italy, Estonia, Belgium and Czech Republic

Activity 5

Working on the sustainability and road mapping:

- Market analysis
- Recommendations for long-term sustainability
- Dissemination

Activity 6

3

Market Context: GRIDS Advantages and Benefits

Matteo Marinelli- INFOCERT

Digital transformation is now a key requirement

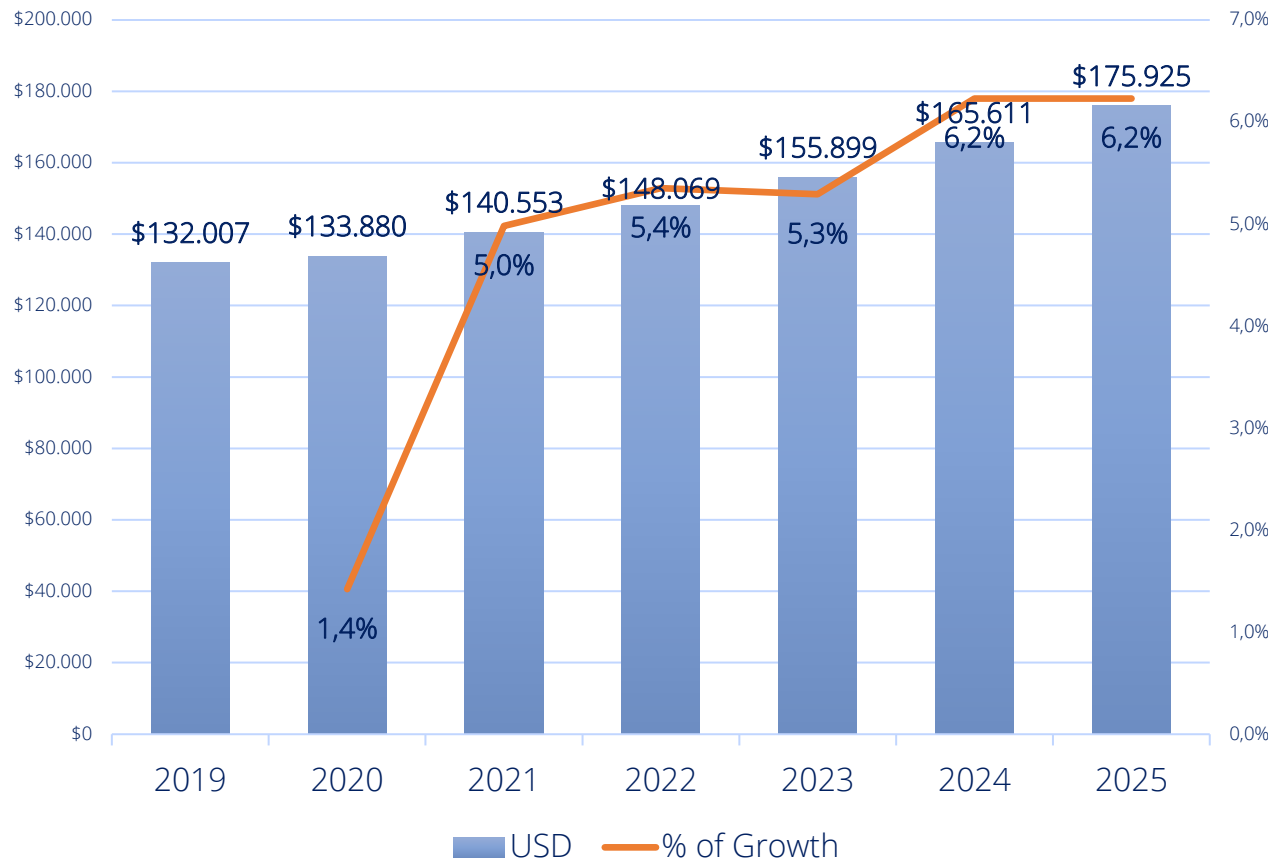
- Digital transformation has been accelerated by the COVID-19 pandemic
- Renewed focus on the digital onboarding process as a critical requirement for doing business.
- The pandemic turned the online identity proofing from a competitive advantage into a core requirement for businesses.

New Needs for businesses:

- Gaining confidence in end-user identities through remote interactions
- Improve User Experience to attract and retain customers



IT spending forecast in banking and investment services



Europe enterprise IT spending in the banking and investment services market is forecast to **grow by 5.0% in 2021** to \$140 billion in constant U.S. dollars, up from \$133 billion in 2020.

Spending is expected to see a five-year compound annual growth rate of 6.2% to reach an estimated **\$176 billion by 2025**.

Market trends in banking & FI



Identity

IDENTITY

The need to corroborate identity through remote interactions continues to grow.



Security

SECURITY

Data security continues to be a primary consideration for the financial services industry



Fraud prevention

FRAUD PREVENTION

By 2023, more than 25% of fraud detection teams will have become cross-functional, leading to a greater alignment with organizational goals and customer experience.



UX

USER EXPERIENCE

All FIs focus on the client. Interactions between financial services and customers have moved to digital environments. A user interface design's significance increases.



Functional capabilities

FUNCTIONAL CAPABILITIES

need to be integrated in the area which will link technology and digital business strategy, in order to continue the digitalization route.

Banking & FI market challenges

Prejudice in identity-proofing processes

Traditional approaches to Identity and Access Management are linked to in-person interactions. The need is to drive customer-facing interactions to digital channels.

Process automation

Is not only a means by which processes can be automated, but it is also a tactic to reduce the cost of delivery of services.

API architecture strategy

is a key part of the strategy for Financial Institutions as they seek to build out ecosystems to drive new revenue streams and differentiated offerings to digital customers.

Fintech banks vs traditional banks

The unstoppable growth of the Fintech phenomenon with its way of providing services to customers is affecting the banking system.

Regulatory Compliance

Has become one of the most significant banking industry challenges as a result of the intense increase in regulatory fees. Technology is a critical component in creating this culture of compliance.

Security Breaches

A security incident can have consequences on the day-to-day operations. Security is one of the leading banking industry challenges. Financial institutions must invest in security technology.

Fincrime Market Map
400+ RegTech Products

END TO END AML
ALTERGAIA, Vneuron, actico, NAPIER, ESSENCE INTELLIGENCE, WorkFusion, frankieone, quantexa

CDD AND KYC
ACCUTY, SIMPLEKYC, NorthRow, KYC-CHAIN, RiskMS, EastNets, AMLYZE, trunarrative, targens, encompass, DivDoc, norbloc, actico, Socure, TOKEN IQ, KYCQ, SCANTEK, Acuris, ANTIOPEA, RiskScreen KYC, SPIDER, BUREAU VAN DIJK, smartKYC, SwiftDil, KYC3, Kyckr, Know Your Customer, SILO, finform, 4STOP, BLOCKPASS, CLIENT SCOPE, KYC Manager, VERIPHY, NEOTAS, Beaufort, flinks, GRC WATCH, Datarama, kompany

ONBOARDING AND CLM
muinmos, komgo, WEALTH DYNAMIX, fenergo, ihub, [IMTF], SNAPSWAP, SPHONIC, iMETA, agreement, thirdfort, alessa, pathlock, MINERVA INTELLIGENCE, RegSmart, Fraugster, AI, XPERT, telindus, thync, 34FINANCE, WEB SHIELD, PEGA, BlackSwan, PassPort, QUEENAY, ARCTIC, ACUMINOR

FINANCIAL CRIME RISK ASSESSMENT
alessa, pathlock, MINERVA INTELLIGENCE, RegSmart, Fraugster, ARCTIC, ACUMINOR

FRAUD DETECTION AND PREVENTION
SEON, riskified, Ravelin, AMLT, Brighterion, shieldpay, simility, FRAUDLABS, cybertonica, fiserv, FORTER, FICO, Amberoon, COINFORM, DATAVISOR, Ocrolos, QUANTIPLY, FEEDZAI, FIS, Jewel Paymentech, Heliocor, sif, buguroo, NICE-ACTIMIZE, Fraud.net, LexisNexis, ACI, UNIVERSAL PAYMENTS, TransUnion, features+analytics, PRECOGNITIVE, Bottomline, NetGuardians

FEATURE SPACE
Jewel Paymentech, LexisNexis, NetGuardians

THIRD PARTY RISK MANAGEMENT
ethixbase, Kount, enigma, venminder, VERAfin, EXIGER, Integrity Next, Rights, VADOS, Prevalent, Confinty, ARAVO, Steele, IN-FRONT COMPLIANCE, Ever, ProcessUnity

TRANSACTION MONITORING
Chainalysis, LUCINITY, Intelomate, Paradigm, FNA, Fuzzy Logic, CONFInALE, nsknox, ComplianceWise, Identitii, Toolitaki, SOLINK, Osprey, Rippleshot, SAS, Merkle Science, AYASDI, GBG, Global Vision Systems, Hawk AI, Nota Bene, Consensus

SCREENING AND EDD
Kompli-Global, Acuris, RIPJAR, DATACTICS, SILENT EIGHT, NameScan, SmartSearch, EYES CLEAR, Smart Oversight, Merlon.ai, POLE STAR, Diligencia, Pliance, Argos Risk, docfox, KYC2020, Comply Advantage, infoGnosis, KHARON, GIANT OAK, upLexus, AML Partners, INTELLIGO, Transparrant, Info4c, Compiladata, First AML, Risk Ident

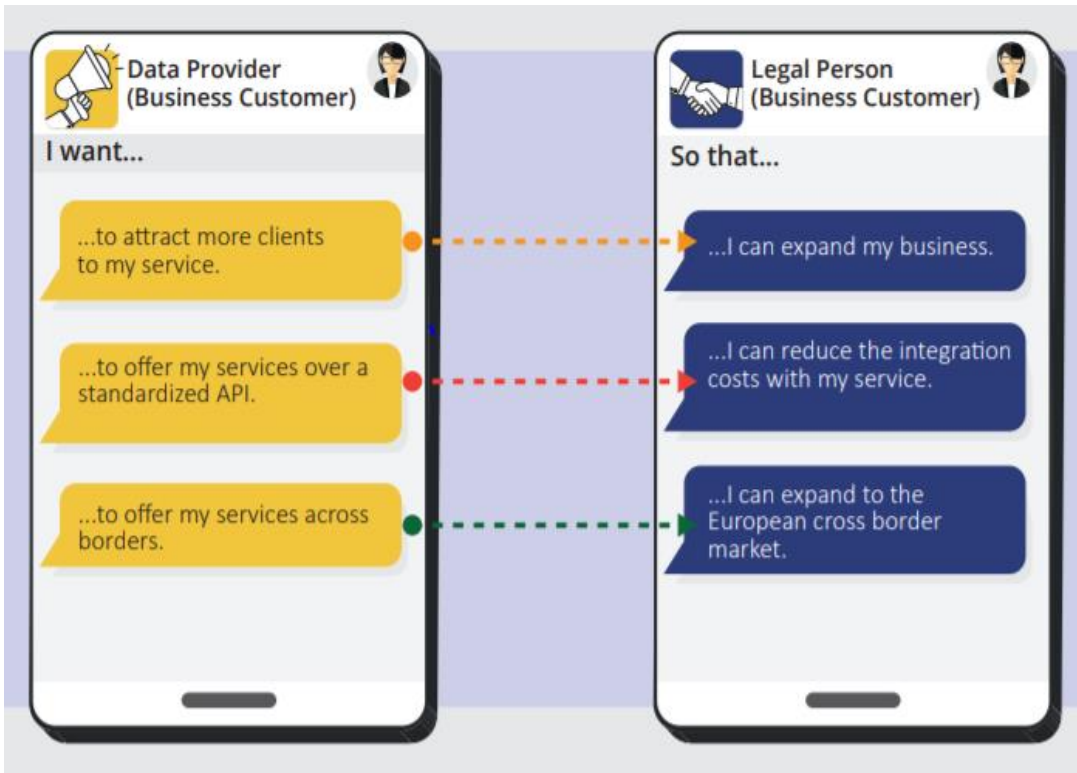
RISK IDENT
RISK IDENT

Most of the KYC identity solutions in the market today are based on technologies that allow automation of the onboarding process and not on leveraging on eIDAS solutions across different member states.

Key Market Features

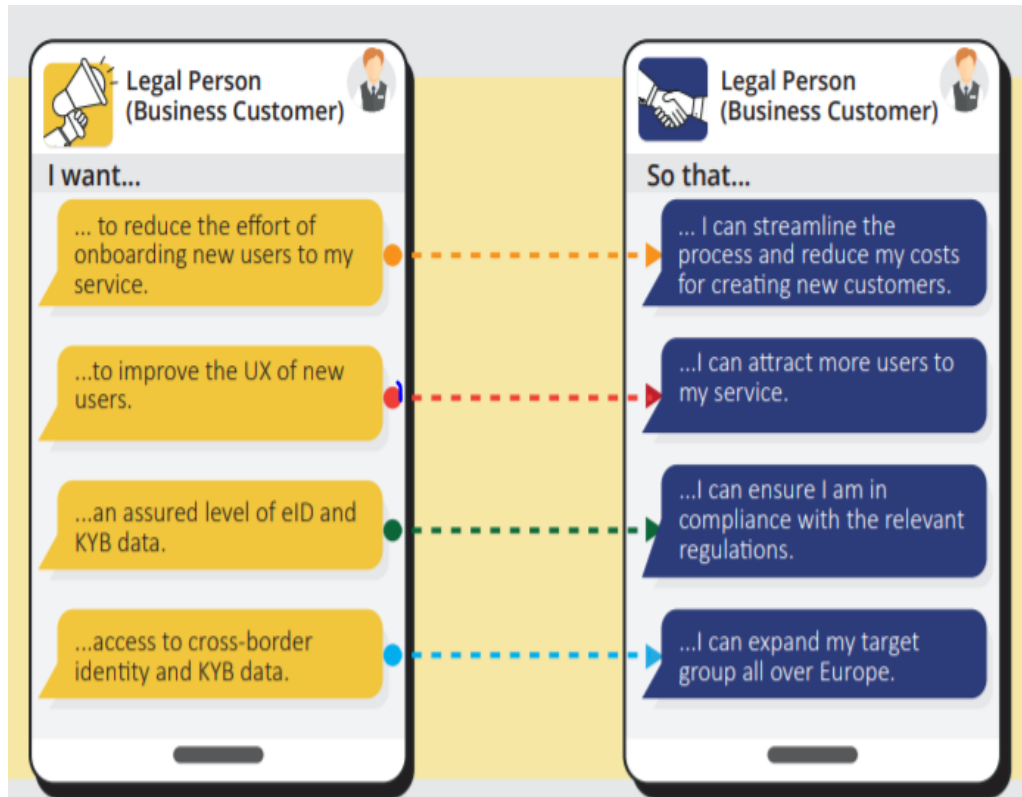
- A high level of fragmentation of onboarding practices and differences in the way they are implemented within the EU financial sector
- Fragmentation is driven by differences in approaches with regard to the deployment of digital ID solutions within national markets and significant discrepancies between national KYC requirements
- This results in banking groups focusing primarily on their own domestic markets and less emphasis on the acquisition of cross-border customers so acting as a barrier to the development of competitive panEuropean KYC services by commercial solutions providers
 -
- At regulatory level there is tension between a 'single market' elements (e.g., banking passport etc.) and minimum harmonization rules set out by the AML Directive

Data Providers' needs



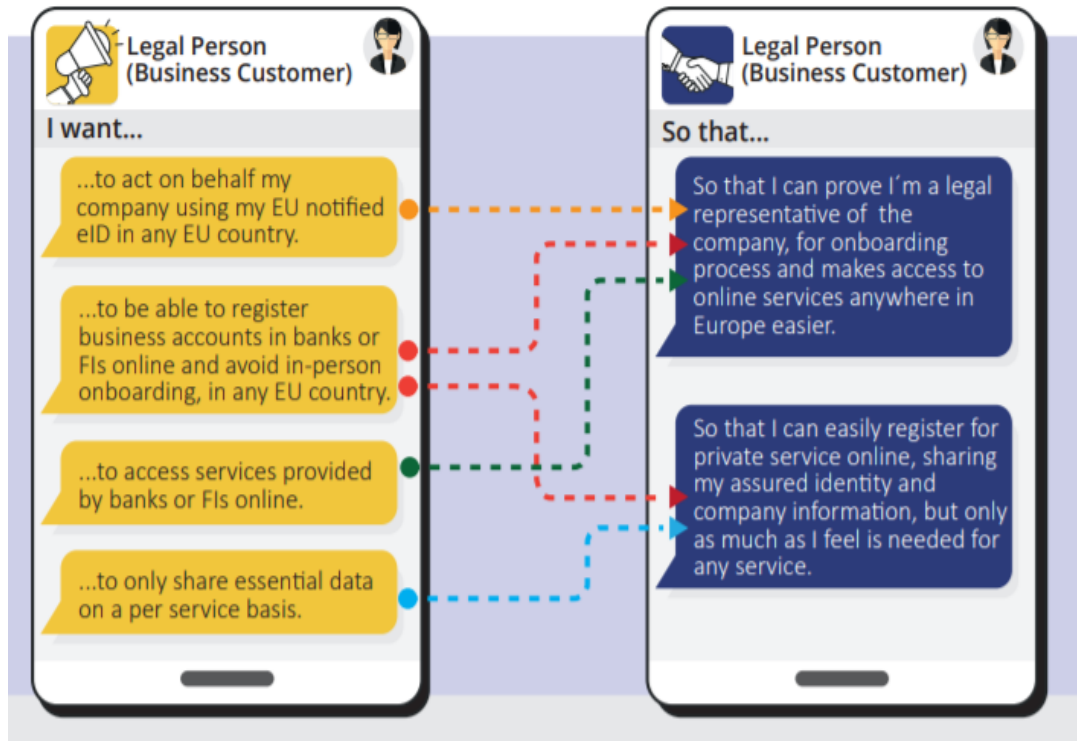
- Need to integrate with their customers (Data Consumers) in a standardized environment, become more competitive and pursue more growth opportunities
- Need to extend their reach, across borders through a framework that allows both individual and business verification services for more potential customers

Data Consumers' needs



- Need the provision of automated, digital KYC/KYB services, with access to different Data Providers from different countries, to save time and cost
- Need integration with eIDAS-based authentication and authorization for more straight-forward identification, verification and onboarding processes that increase customer satisfaction
- Need cross-border services for existing and potential new customers in new geographical markets

Data Subjects' needs



- Need increased trustworthiness in services associated with individual data privacy
- Need more choices to interact with and seek services from financial and legal institutions, across European borders.
- Need simplified processes such as digital onboarding and digital identification that saves time, money and increases trust in European institutions and businesses

GRIDS benefits

STRENGTHS

- GRIDS reduces the effort for digital onboarding services in EU, addressing the gap of cross-border acceptance of e-identification and remote KYC/KYB processes.
- DC, DP and DS can benefit from GRIDS business network, perform cross-border transactions and rely on the concept of a European eIDAS network.
- GRIDS developed a Service Provider (KYB Custodian), enabling the generated portable KYB profile to be accepted across jurisdictions
- GRIDS focuses on Business Verification for regulated entities' which for AML purposes require both verification of the private individual and businesses.
- GRIDS can provide a robust KYB solution ensuring to Data Consumers a qualitative data (always up to date, time stamped, and audit-proof) to satisfy the stringent AML regulations which are placing increasing emphasis on data quality.

OPPORTUNITIES

- AML directives throughout the EU member states created the need of a solution for regulated entities to avoid reputational damage and to comply with the law.
- The increasing rate of digitization in the compliance function of companies is being driven by a huge growth in the RegTech sector.
- GRIDS could fill the gap in KYC/B and AML services by providing a cross-border, standardized process for Data Subjects' identification and verification.
- In the future, a new AML/KYC Regulation will harmonize and standardize the requirements for digital onboarding



GRIDS Platform: High level overview

Dimitrios Bakas – ADACOM
Ross Little Armitt – ATOS



Design Objectives

- **Create a GRIDS platform** to enable Data Consumers (Relying Parties) to :
 - authenticate natural & legal persons over eIDAS
 - bundle KYC data from Data Providers with verified eIDAS identities
- **Create a trusted ecosystem** where:
 - Data Consumers register to GRIDS platform
 - Data Providers are registered to GRIDS and publish the identity and KYC claims they support
 - GRIDS publish all identity & KYC claims that are supported over its platform by eIDAS and all connected Data Providers with up-to-date information
- **Easy Integration:**
 - Reduce integration effort by providing a GRIDS SDK for Data Consumers to integrate & query for identity & KYC data over GRIDS APIs

Design Principles

- **Make use of commonly deployed standards where possible:**
 - OIDC interface with Data Consumers for requesting Identity and KYC Claims
 - OIDC Identity Assurance Specification (OIDC IDA) V1.0 builds on OIDC to provide trusted a trusted level of assurance with verified claims
 - https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html
- **Privacy and Security by Design**
 - Data Subject is informed of whole process and OIDC IDA includes in its design the purpose for which each individual claims are being requested
 - GRIDS supports encrypted and signed eID+KYC requests / responses
- **Scalable solution:**
 - OIDC Distributed Claims approach implemented so that the GRIDS platform returns self describing access token(s) to be used by the Data Consumers to request the KYC data directly from the Data Provider(s) without traversing the GRIDS platform

GRIDS Platform High level overview

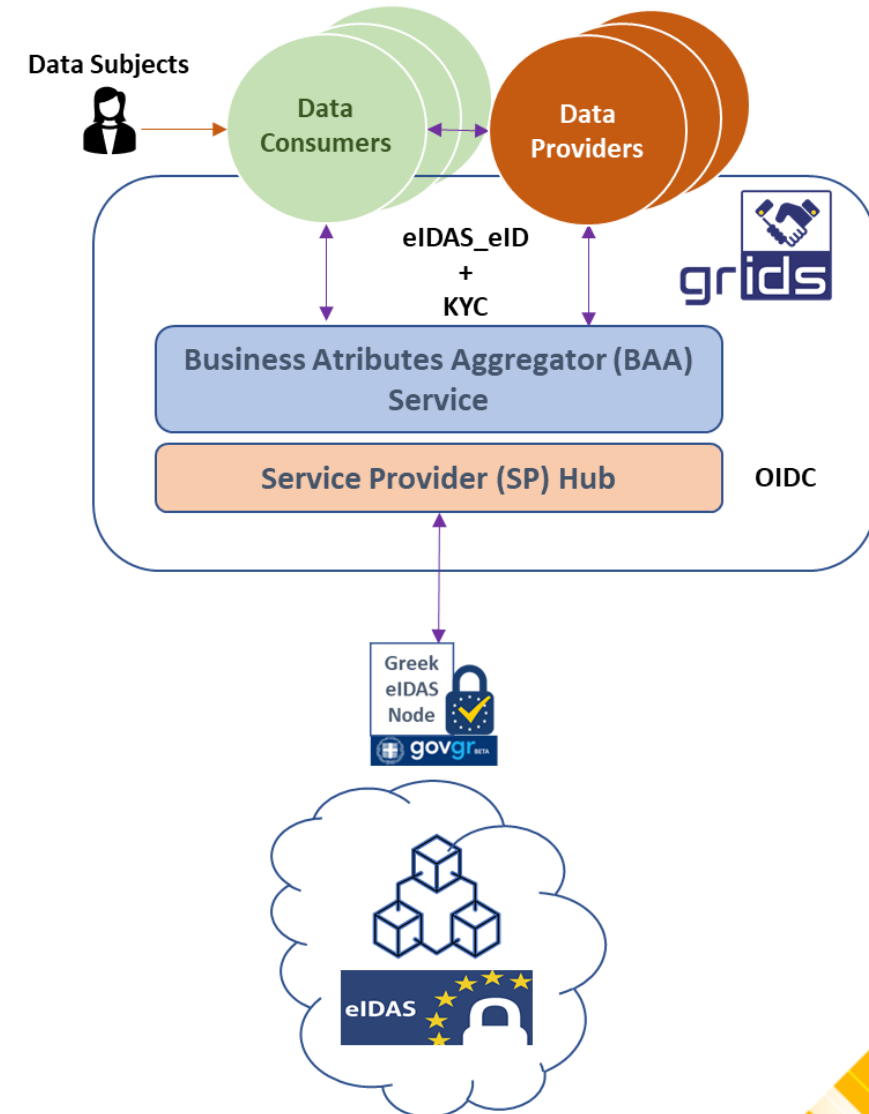


GRIDS platform operates as a **business network** in the form of a Single-Sign-On (SSO) federation between:

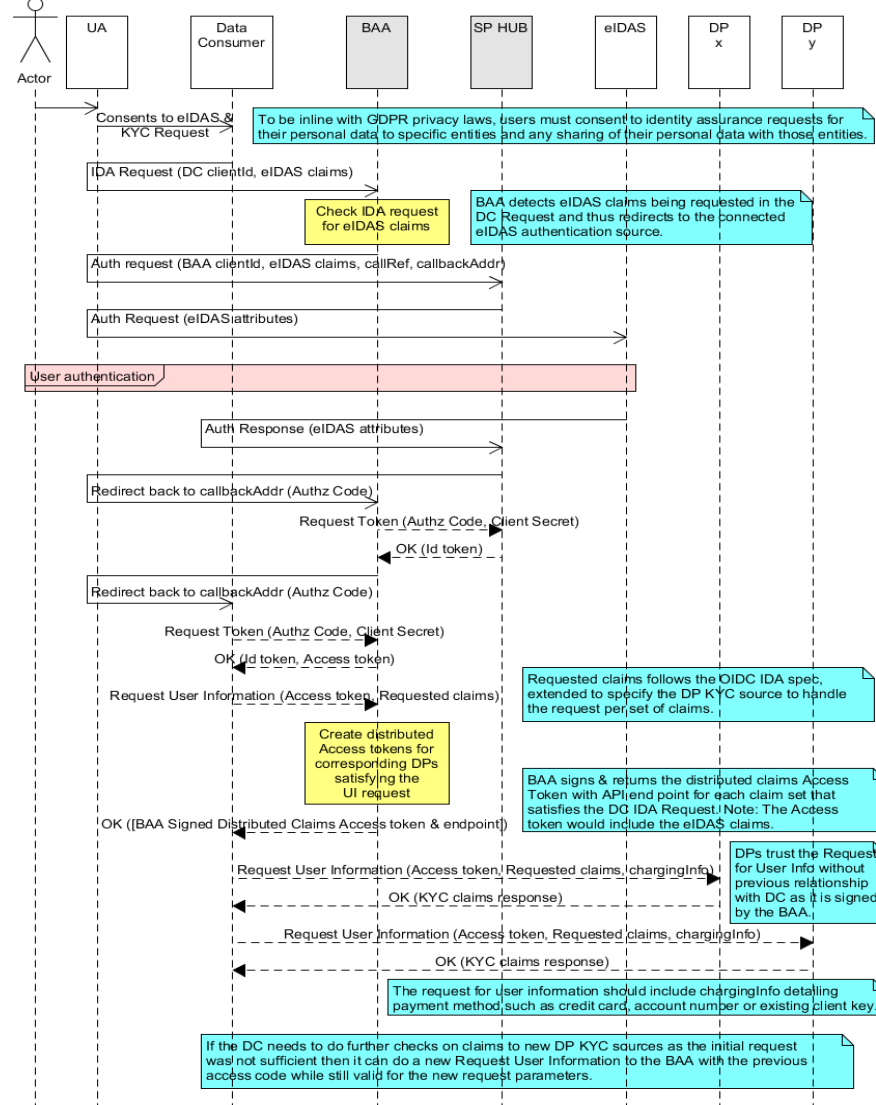
- KYC providers (Data Providers)
- Their customers from the financial, LEI issuing and legal sector (Data Consumers)
- The clients of these industries (Data Subjects)

The platform includes:

- The **Service Provider Hub (SP HUB)** to provide eIDAS authentication functionality
- The **Business Attributes Aggregator (BAA)** to enrich the data obtained from additional sources, such as KYC information resulting in the bundled token (“eIDAS eID + KYC” data facility), which is further shared with the KYC Data Consumer (KYC DC).
- An **SDK** (software development kit) developed to enable the seamless and SSO-based integration of end-users with KYC services and enhance the efficiency and accuracy of the diligence process.



GRIDS eID+KYC



OIDC IDA Trust Framework & KYC/KYB Claims

```
{
  issuer: "https://dp.kompany.com:8050/",
  userinfo_endpoint: "https://dp.kompany.com:8050/userinfo",
  jwks_uri: "https://dp.kompany.com:8050/.well-known/jwks.json",
  scopes_supported: [
    "openid"
  ],
  response_types_supported: [
    "code",
    "token",
    "code token",
    "code id_token",
    "id_token",
    "token id_token",
    "code token id_token",
    "none"
  ],
  subject_types_supported: [
    "public"
  ],
  userinfo_signing_alg_values_supported: [
    "RS256"
  ],
  userinfo_encryption_alg_values_supported: [
    "RS256"
  ],
  claim_types_supported: [
    "distributed"
  ],
  claims_supported: [
    "aud",
    "exp",
    "iat",
    "iss",
    "sub",
    "txn"
  ],
  claims_parameter_supported: true,
  service_documentation: "http://DataProvider.example1.com/connect/service_documentation.html",
  ui_locales_supported: [ ],
  verified_claims_supported: true,
  trust_frameworks_supported: [
    "grids_kyb"
  ],
  evidence_supported: [
    "company_register"
  ],
  company_register_document_SKU_supported: [
    "REX",
    "AA",
    "AOA",
    "SL"
  ],
  claims_in_verified_claims_supported: [
    "legal_name",
    "legal_person_identifier",
    "lei",
    "vat_registration",
    "address",
    "sic",
    "business_role",
    "sub_jurisdiction",
    "trading_status",
    "family_name",
    "given_name",
    "birthdate",
    "person_identifier"
  ],
  company_register_registry_country_supported: [
    "ES",
    "UK",
    "FR",
    "NL"
  ]
}
```

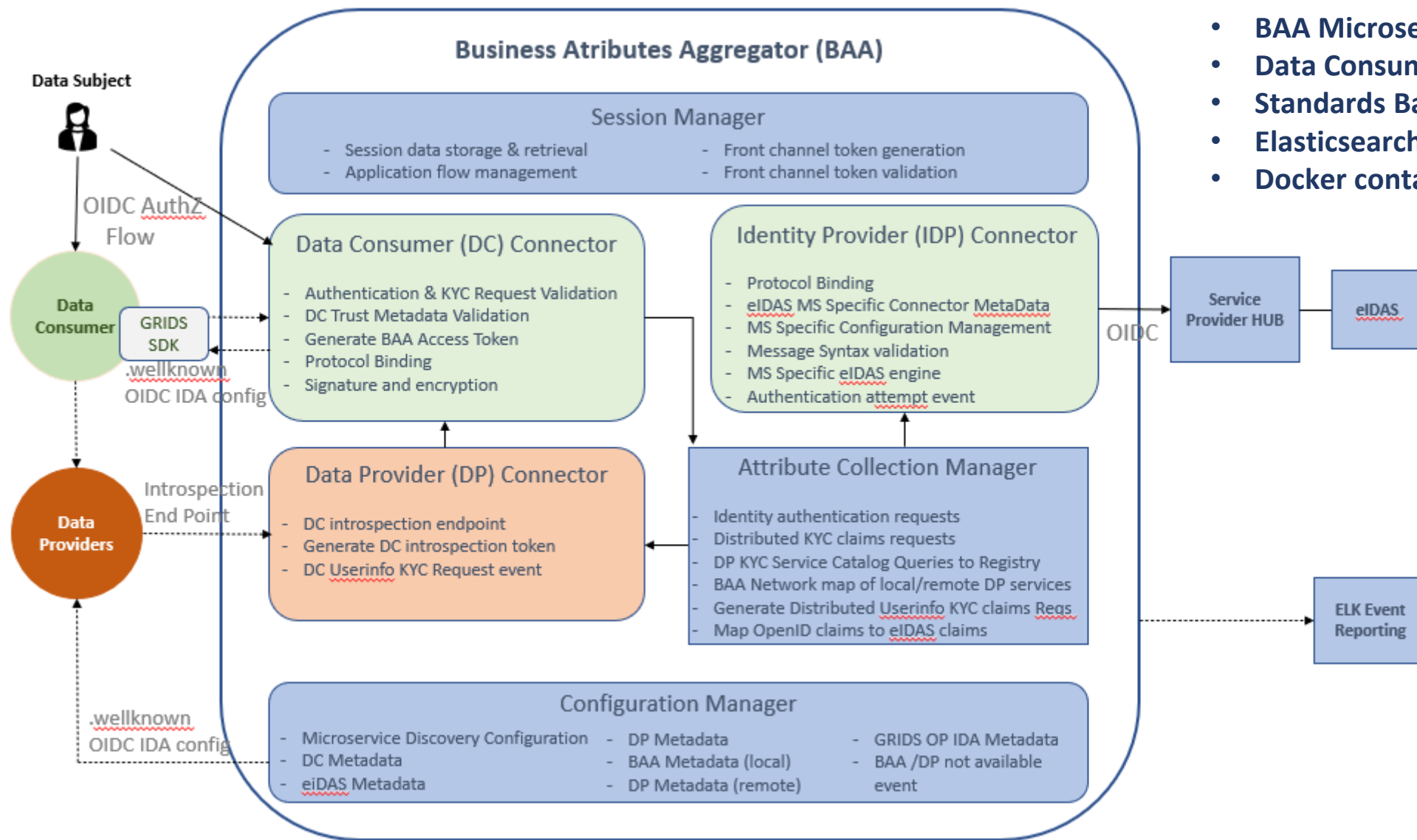


```
verified_claims_supported: true,
trust_frameworks_supported: [
  "grids_kyb"
],
evidence_supported: [
  "company_register"
],
company_register_document_SKU_supported: [
  "REX",
  "AA",
  "AOA",
  "SL"
],
claims_in_verified_claims_supported: [
  "legal_name",
  "legal_person_identifier",
  "lei",
  "vat_registration",
  "address",
  "sic",
  "business_role",
  "sub_jurisdiction",
  "trading_status",
  "family_name",
  "given_name",
  "birthdate",
  "person_identifier"
],
company_register_registry_country_supported: [
  "ES",
  "UK",
  "FR",
  "NL"
]
```


UserInfo Request example (received at Data Provider)

```
{
  "iss": "https://BAA.1.example.com",
  "sub": "X731Z219A",
  "aud": "https://DP.anotherexample.com",
  "scope": "openid",
  "exp": "1311281970",
  "iat": "1311280970",
  "jti": "knm34145j1451",
  "txn": "12347565411142194650508795011123",
  "client_id": "https://DC.example.com",
  "client_introspection_uri": "https://GRIDS.BAA1234.com/clients?id=https://DC",
  "client_introspection_access_token": "78y98yy98hyubui989y98yh8y7",
  "legal_person_identifier": "375714X",
  "legal_name": "Acme Corporation",
  "verified_claims": {
    "verification": {
      "trust_framework": "eidas",
      "identity_assurance_level": "substantial",
      "time": "2012-04-22T11:30Z"
    },
    "claims": {
      "given_name": "John",
      "family_name": "Smith",
      "birthdate": "1971-04-17",
      "person_identifier": "X731Z219A",
      "address": {
        "country": null,
        "street_address": "George Street 123",
        "locality": "Glasgow",
        "postal_code": "G1 1QD"
      }
    }
  },
  "claims": {
    "userinfo": {
      "verified_claims": {
        "verification": {
          "trust_framework": {
            "value": "grids_kyb"
          },
          "evidence": [
            {
              "type": {
                "value": "company_register"
              }
            }
          ]
        }
      }
    }
  },
  "registry": {
    "organisation": {
      "essential": false,
      "purpose": "string"
    },
    "country": {
      "essential": true,
      "value": "ES"
    }
  },
  "time": {
    "max_age": 0,
    "essential": true
  },
  "document": {
    "SKU": {
      "value": "REX"
    }
  }
},
"claims": {
  "given_name": null,
  "family_name": null,
  "birthdate": null,
  "legal_name": null,
  "legal_person_identifier": null,
  "lei": null,
  "vat_registration": null,
  "address": null,
  "tax_reference": null,
  "sic": null,
  "business_role": null,
  "sub_jurisdiction": null,
  "trading_status": null
}
}
```

GRIDS Platform



- BAA Microservices architecture
- Data Consumer SDK
- Standards Based Interfaces
- Elasticsearch Kibana event logs
- Docker containers

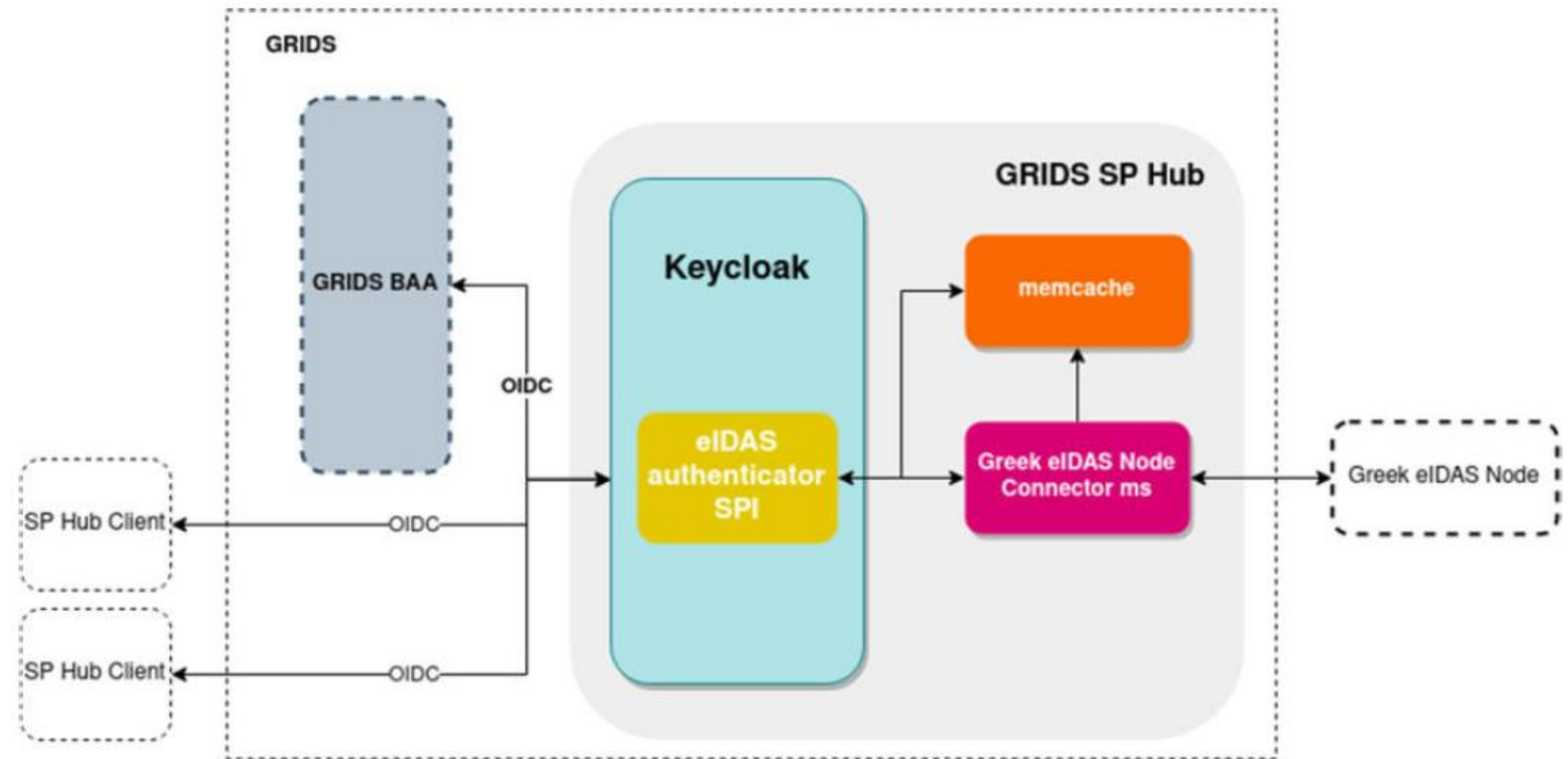
Service Provider (SP) Hub

SP Hub Is realised via an **OpenIdConnect (OIDC) Server** (Keycloak) complemented by a Memcached instance for GRIDS (via the Greek eIDAS Node Connector ms)

The SP HUB OIDC Server is a lightweight, production ready, stable and scalable implementation

By employing a composable microservice architecture the SP Hub can be easily expanded to integrate with additional eIDAS Nodes

This integration is possible with no modification of the core OIDC server (and as a result with no down time)



GRIDS Architecture implementation benefits

The GRIDS architecture supports a **distributed claims** approach with following benefits:

- BAA provides the trust relationship so that no previous relationship between the DC and DP is needed.
- BAA provides the trust relationship between DCs and DPs
 - BAA signs and encrypts OIDC self-describing access token which includes the Data Subject's eIDAS identity claims & requested KYC claims
- Claims issued directly from DP to DC in distributed claims approach (userinfo end point)
- Clear separation of interests between commercial agreements (DC / DP)
- DC able to include charging information in request for the KYC claims to the DP

GRIDS Platform - Features



The GRIDS platform showcases in practice how the eIDAS network can work together with private sector stakeholders, both large and SMEs, to address issues of trust in modern digital services

The eIDAS network remains the body, comprised of the national authorities, responsible in the event of liability issues about the eID and the eIDAS network

- The identity of an individual or an entity is of high value and only official authorities remain responsible for the issuance of identification documents.

GRIDS provides a straightforward route to enter a contract with the Data Provider ensuring the required data flow follows existing contractual law principles and the agreed governing law.

Specific benefits of CEF eID for private sector stakeholders are addressed to maximize trustworthiness of critical processes

- Remote onboarding,
- KYC/AML compliance
- Adoption of cross-border identification and authentication services
- Contributing to sustainable growth of financial and legal sectors, adding value in their operations



GRIDS DEMO:

Martynas Mazutis – KOMPANY

Peter Bainbridge-Clayton – KOMPANY

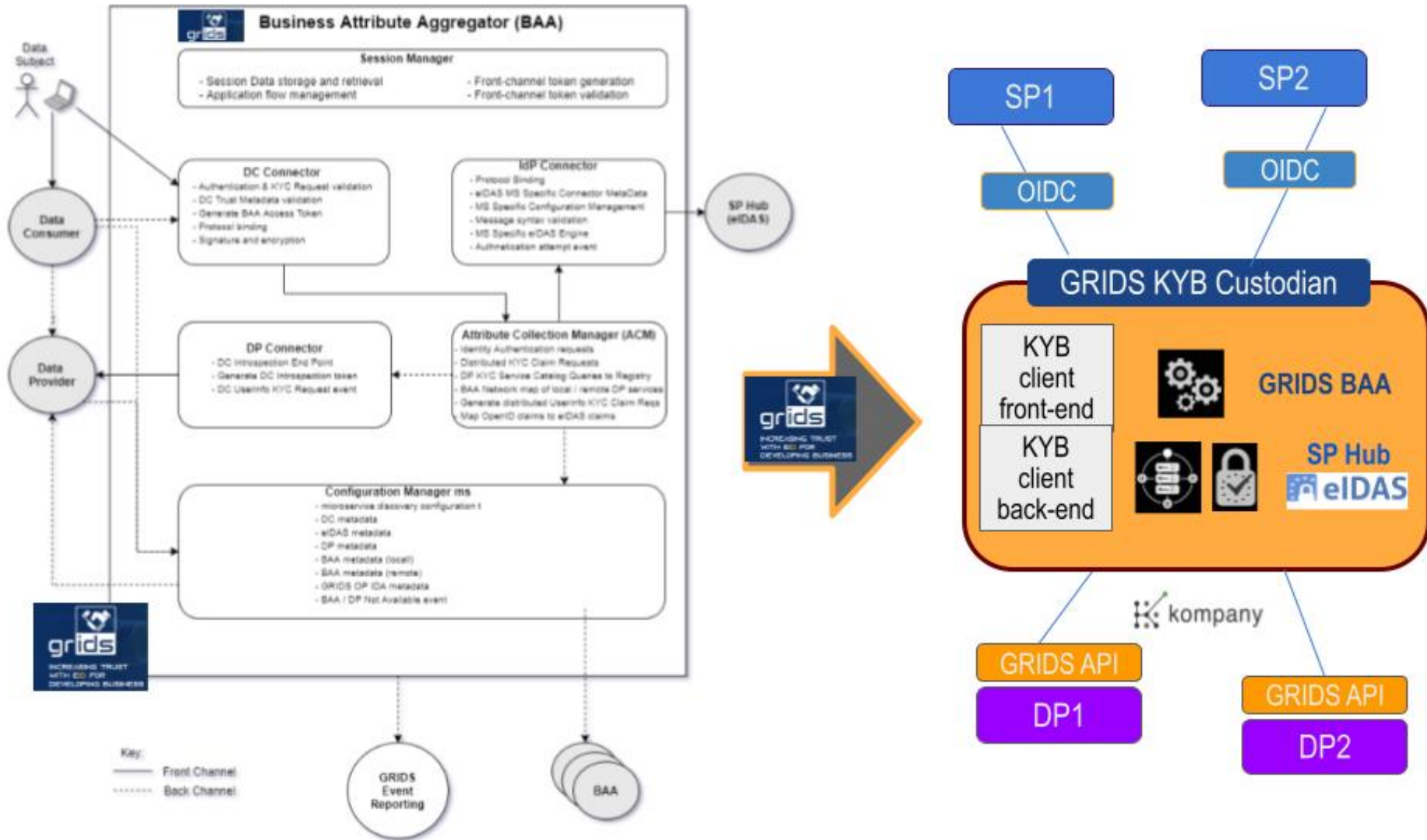
Szabolcs Lefkanics - KOMPANY

eIDAS Context: Future needs & Evolution

Petros Kavassalis – University of the UEGEAN



GRIDS service pack



motivation (a)



Search



Home



My Network



Jobs



Messaging



Notifications



Me



Work

1

GRIDS-eIB Workshop on "Identity Attributes and KYC: the transition to eIDAS 2.0 and AMLR"

Published on November 25, 2021

[Edit article](#)



Identity Attributes and KYC: the Transition to eIDAS 2.0 and AMLR era

6 followers

✓ Following

The **GRIDS** and **eIB** projects organized the **GRIDS-eIB Workshop on "Identity Attributes and KYC: the transition to eIDAS 2.0 and AMLR"** which took place virtually on **Thursday 16 September 2021** from 2:00-5:00 pm CET.

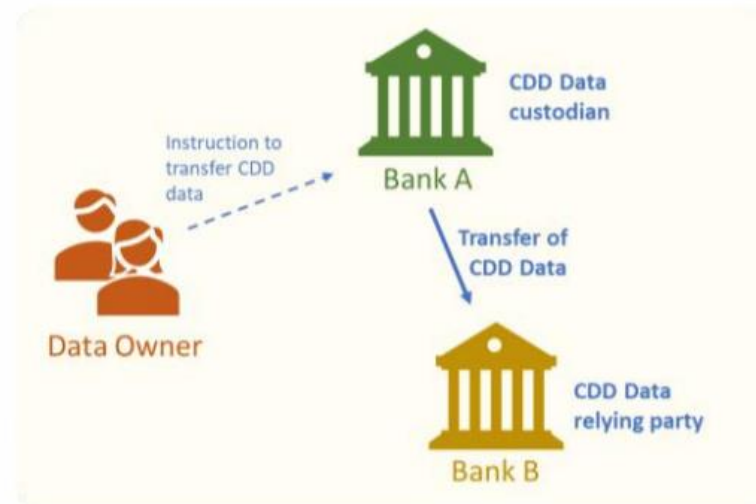
motivation (b)

FISMA/2020/023/B3/SE/LV CONTRACT

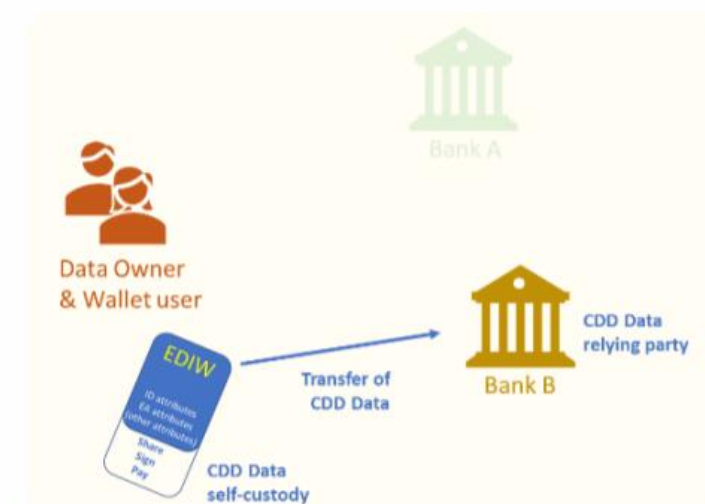
2

DEVELOPING A DIGITAL IDENTITY SOLUTION FOR USE BY THE FINANCIAL SECTOR BASED AROUND eIDAS TRUST SERVICES

FI-centric portability (Delegated custody)



User-centric portability (self-custody)

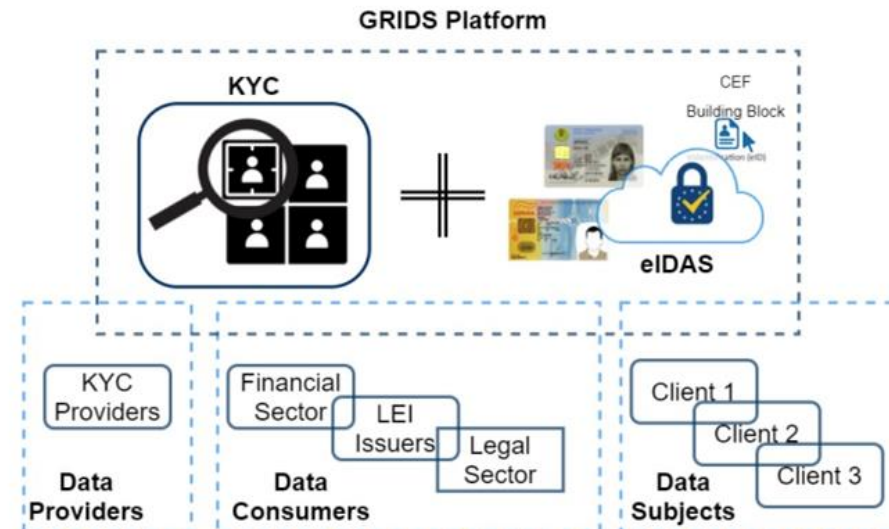


KYB as a Service



A bundled one-stop solution for KYC & KYB screening:

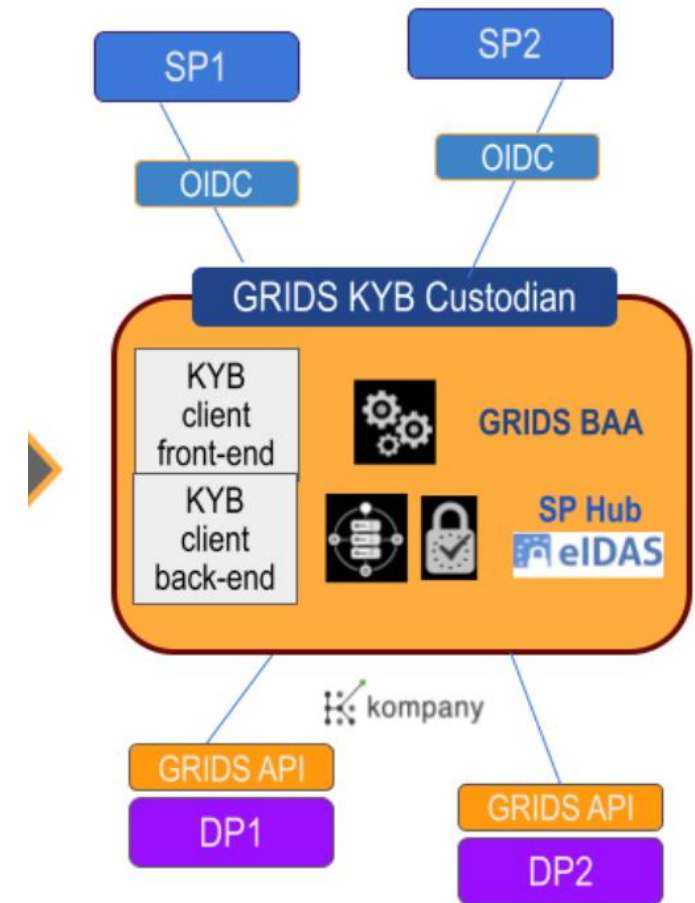
- Identifies legal and natural persons through access to the established pan-EU eIDAS core service platform
- Accesses company information and commercial documents directly from official primary sources around the world.



*Peter Bainbridge - Clayton,
Kompany, Austria*

GRIDS KYB Custodian Demo Case

- KYB Custodian:** The provider of a digital “KYB/KYC screening” service: We assume that this KYB Custodian primarily addresses the needs of the following user groups:
 - Financial Institutions, utility and e-commerce providers, and other Service Providers, qualified to query information about a company/organization, eventually in the context of a compliance due diligence process and beyond
 - Companies represented by an Individual (legal or any other authorized representative) which access directly the services of a Custodian KYB to issue a trustworthy “standard KYB identity” that can be credibly used to transact with Service Providers (for example, if they want to build a cryptocurrency portfolio)
- SP or DC: Service Provider or Data Consumer,** an entity providing FinTech services to corporate customers, which partners with the KYB Custodian to operate KYB/KYC checks in a compliant way with regulations in force
- Company or Corporate Customer (Data Subject):** A Legal Entity that accesses the service of an SP (DC) in partnership with a KYB Custodian
- Legal Representative:** A Natural Person representing a Legal Entity
- DP (Data Provider):** A Provider of corporation-related data giving access to their registries containing KYB information about Companies and Public Organizations



GRIDS KYB Custodian interacting with a demo SP (CryptoAegean) and kompany's Data Providers (DPs)



1 Registration / Verification — 2 Mandate Validation — 3 KYB Profile — 4 Register with us Optional

Company Information

Company Name	Company Registration Number
Country of Company Registration	

Company Representative Information

Name	Surname
e-mail	

BACK

NEXT



Welcome 1. Build your KYB profile

In order to initiate the generation of the KYB profile of your Company, you must first provide your personal details and the details of the company you represent below. Then click the "Next" button.



The GRIDS KYB Custodian Service has been co-financed by the [Connecting Europe Facility \(CEF\)](#) of the European Union | GRIDS Project: Grant Agreement No INEA/CEF/ICT/A2019/1926018

Developed by [UAegean i4m Lab](#), [Kompany](#) and [GRIDS Consortium](#)

Contact:  



A meta-registry issuing CDD data as VCs (add-on for invoice delivery & cryptopayments)



1. Query for Corporate Customer Data (KYB/KYC screening):
Implementing a delegated CDD process, on behalf of a partner SP.



Due diligence

2. Issue a KYB Verifiable Identity for a Company: Enabling a Company (DS) to generate Verifiable Identity Credentials (VCs), implementing a **portable KYB business identity** (i.e. , a standard KYB profile), and store them in the Identity Wallet of their Legal Representative (FDIW)



B-wallet (EDiW)

EBSI Wallet Conformance Testing



3. Verifiable KYB Public (meta) Registry: Storing a KYB profile (created through a SP or a DS request) in the form of Verifiable Data, thus enabling the instant retrieval of the KYB profile of an organization; this gives Companies a place to issue public verifiable business identities, and Regulation Supervision Authorities, government bodies and other qualified users, the possibility to receive proofs of verifiable KYB attributes, without requiring Companies to have their own wallets and the institutional users of Companies' identity proofs to run specific software agents for VC verification.





GRIDS Next Steps

Paul Foster – KOMPANY

Alberto Miranda Garcia - ATOS



Sustainability & Uptake: External Considerations

Government:

- Need to have eID schemes in place
- These need to be officially *notified* for cross-border acceptance
- Proactive effort to officially enable eIDAS for the private sector

Data Subjects:

- Need to be aware of eID schemes and ,beyond government‘ use cases
- Need to be convinced to subscribe (sufficient uptake levels)

Data Providers:

- Node interconnectivity in between the relevant countries

Data Consumers:

- Need to be convinced to adopt new AML methods (corporate inertia)

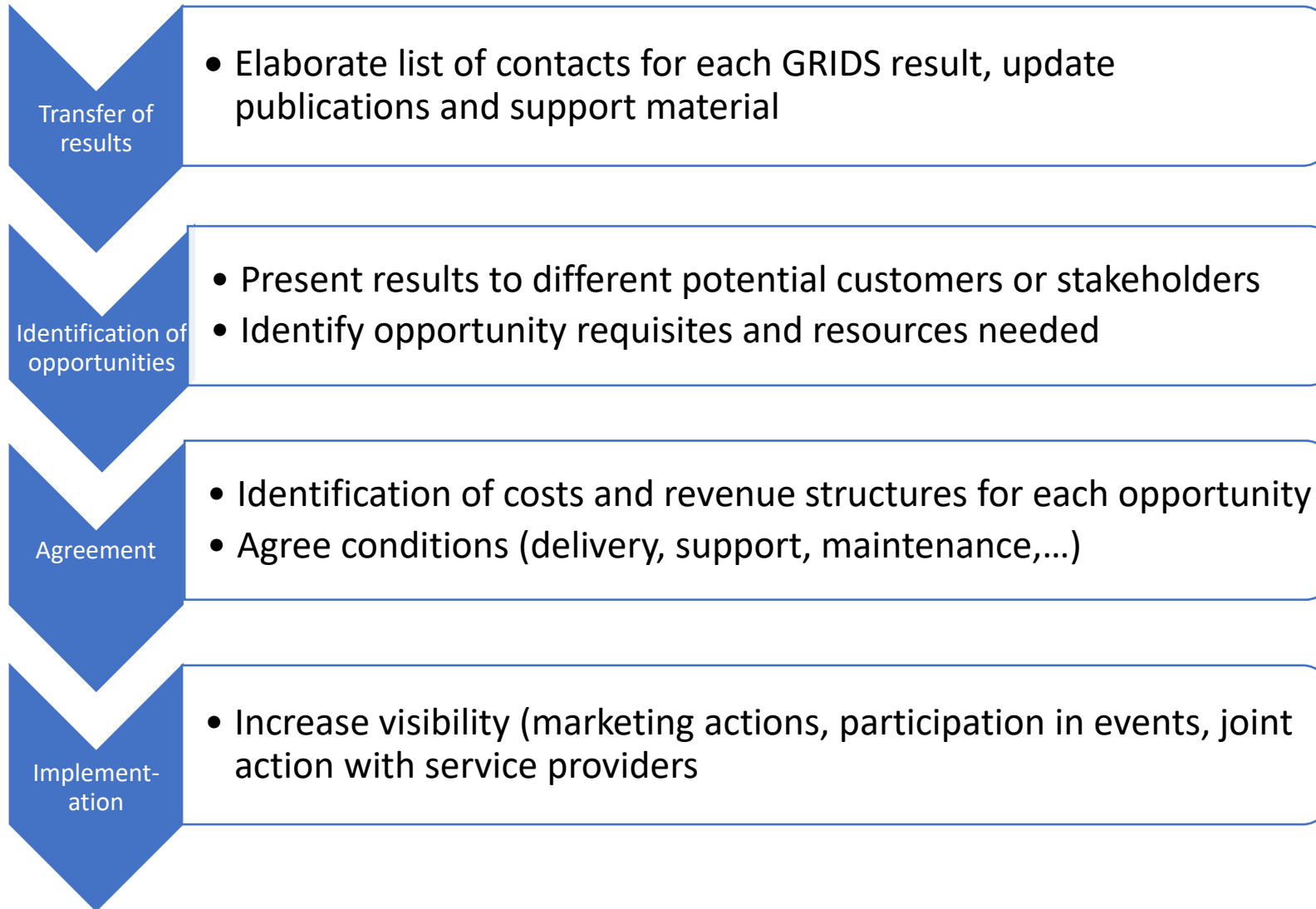
Regulators:

- eID schemes need to be accepted for regulated AML/CDD activities

EU Commission:

- Needs to increase lobbying/promotion of the benefits of ,Connecting Europe‘
- Needs to continue to make efforts to standardise pan-EU AML standards and consistent AMLD implementation/interpretation

Sustainability & Uptake: Internal Next steps



Sustainability & Uptake: Internal Next steps

Exploitation Coordination & Business Opportunity Committee


- Making proposals to the Parties for the review and/or amendment of the terms of the Exploitation Agreement
- Establishment of a Business Opportunity Committee (BOC) for the identified Business Opportunities.
 - Composed of one representative of each of the Parties involved
 - Finalisation of pricing strategy
 - Defining new types of roles for the Parties (or modifying the current definitions) as well as their associated rights and obligations
 - Updating the roles performed by each Party
 - Making proposals to the Parties and assigning tasks to specific entities
 - Identify possible distributors and customers
 - identify possible strategic alliances with other organizations for future deployment
 - Establishing links with existing and future technology providers.
 - Coordinate marketing actions.

8

Q & A

A white square with a thin white border containing the text "Q&A" in a bold, white, sans-serif font. The square is positioned in the upper right area of the slide, overlapping a large, semi-transparent blue arrow pointing to the right.

Q&A

- Do you agree with our assumed GRIDS benefits?
 - What additional challenges might GRIDS need to overcome before widespread uptake?
 - How do you see the current eIDAS and eIDs evolving as a result of the proposed eID 2.0?
 - Do you agree eIDAS has not fulfilled its potential? Why is this?
 - Is there anything else you think the GRIDS team should have addressed or is missing?
- 
- A large, stylized arrow pointing to the right, located in the bottom right corner of the slide. It is composed of two overlapping shapes: a light blue arrow and a yellow arrow, both pointing right. The yellow arrow is slightly offset and larger than the blue one, creating a layered effect.



Thanks !

<https://grids-cef.eu/>
<https://twitter.com/CefGrids>

Atos



UNIVERSITY OF THE AEGEAN



Agreement number: INEA/CEF/ICT/A2019/1926018
Action No: 2019-EU-IA-0044