increasinG tRust with eId for Developing buSiness

D3.2 Customisation of 360kompany services

Document Identification			
Status	Final	**Due Date**	31/01/2021
Version	1.0	**Submission Date**	12/02/2021

Related Activity	Act 1	**Document Reference**	D3.2
Related Deliverable(s)			
Lead Participant	KOMPANY	**Lead Author**	Peter Bainbridge-Clayton (KOMPANY)
Contributors	KOMPANY ATOS UAEGEAN	**Reviewers**	Ross Little (ATOS) Nikos Triantafyllou (UAEGEAN)

Keywords
eIDAS, KYC

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
Peter Bainbridge-Clayton	KOMPANY
Ross Little Armitt	ATOS
Nikos Triantafyllou	UAEGEAN

Document History			
Version	Date	Change editors	Changes
0.1	31/01/2021	Peter Bainbridge-Clayton	First version for feeedback
0.2	11/02/2021	Peter Bainbridge-Clayton	Version for QC
1.0	12/02/2021	Carmen San roman	Final QA

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Peter Bainbridge-Clayton	11/02/2021
Peer reviewers	Ross Little Nikos Triantafyllou	11/02/2021
Quality Manager	Carmen San Román	12/02/2021

Table of Contents

List of Tables

List of Figures

List of Acronyms

Table 1: 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
OIDC	OpenID Connect
OIDC IDA	OpenID Connect for IDentity Assurance
JWKS	JSON Web Key Set

Executive Summary

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

GRIDS is composed of a number of actors, one of which are the Data Providers. In order to integrate into the GRIDS infrastructure, it is the responsibility of the DPs to provide certain interfaces, utilise certain interfaces, provide appropriate logic to interoperate with the other relevant actors, and provide new services or provide access to existing services in order to fulfil the needs of the other actors, in particular the Data Consumers.

This document outlines the work required for a DP in general, and for 360kompany AG acting as a DP specifically.

1 Introduction

1.1 Purpose of the document

This document is intended to give insight into the design and nature of work carried out within 360kompany AG (hereafter kompany) [www.kompany.com] in order to integrate the services it provides into the GRIDS framework. Some of this work will be generic in nature, i.e., would need to be performed by any Data Provider, and some is specific to kompany. This document does not cover the integration of Data Consumers into the GRIDS platform, this is covered in Activity 4.

Although some aspects of this work are generic to any Data Provider, particularly the GRIDS level interfaces between the Data Provider (DP), the Business Attributes Aggregator (BAA) and the Data Consumer (DC), this document is not intended to be used as a reference for other Data Providers, as the method of implementation will vary from one DP to another.

Specifically, section 7 is kompany specific. Other sections can be used as guidance and reference by other DPs in their own implementation.

1.2 Relation to other project work

The work described in this deliverable is limited to that covered by Task 3.2, but is connected to other tasks under Activities 3 and 4, in particular the design and development of the BAA and the Integration of Data Consumers into GRIDS.

2 Data Providers

Within the GRIDS platform, a Data Provider is a company which provides KYC services on behalf of a Data Consumer. Within the scope of GRIDS, these services will generally be, but are not limited to, those which pertain to the KYC checks performed on a legal person, a representative of a business, and/or a business itself.

The KYC request made to a DP is made within the scope of first performing a cross-border identity check over the eIDAS network, so to provide the DP with authenticated identity claims, with a qualified level of assurance. GRIDS supports both natural and legal person claims requested over eIDAS, but it is recognised at present that there is currently not much support for legal persons over eIDAS. Therefore, in GRIDS project we will likely authenticate natural persons, and the DP will make use of the resultant assured identity claims to complement the legal and business level KYC checks related to the person.

2.1 Types of Data Provider

It is expected that there will be many types of DPs within the GRIDS system as a whole, and each will provide different capabilities, different products, and will have different payment and registration requirements. The Business Attributes Aggregator (BAA) platform has been designed to allow for these variances as much as possible whilst maintaining a consistent interface between the DC, DP and BAA.

Some examples of a DP would include:

- **Business KYC DAAS provider**

  For example, kompany provides business-centric KYC data and documents from the official government source in excess of 200 jurisdictions globally and in real time, with value added services such as VAT checks, document translation, Sanctions and Politically Exposed Persons checks and others.

- **Credit Reference Agencies**

  Who provide credit check and assessment services for individuals and businesses

- **Risk Assessment Companies**

  Who do deep analysis of a company's trading status and fundamentals to give a risk profile to an interested party such as a bank or trading partner.

This document will focus on the changes required for the customisation and integration of kompany services into the GRIDS platform.

2.2 Types of Services Offered

The GRIDS design approach follows the OIDC Identity Assurance 1.0 specification with distributed claims served by Data Providers. It is incumbent, therefore, on DPs in the GRIDS network must comply with the required OIDC interfaces (https://openid.net/specs/openid-connect-4-identity-assurance-1_0-ID2.html#name-op-metadata).

The design of the GRIDS platform specifies no restrictions on the types of KYC service that can be offered by a DP. GRIDS effectively creates a KYC Services marketplace where DPs can provide services to DCs without the necessity of there being a prior direct relationship between the two, but not excluding the existence of such a relationship.

Because a DP must adhere to the OIDC interfaces, the services offered by that DP must be able to be packaged into these interfaces. However the OIDC IDA Working Group do allow extensions to be used and proposed to them for ratification. Obviously, DPs are free to provide services to DCs through non-GRIDS interfaces should the need arise.

kompany proposes the following services, listed below, to be exposed through the GRIDS platform. These services are based on typical use cases for our customers. It is important to remember that kompany specialises in the provision of business-centric data and documents, and does NOT provide data on natural persons, except within the scope of their relationship to a given company (e.g. Managing Directors, Officers, Shareholders etc), and the data and documents are limited to those available within the scope of this relationship.

2.2.1 kompany lower-level Services Exposed Through GRIDS

- Legal Person Verification
- Legal Person Dataset
- Legal Person Documentation
- Legal Person VAT lookup
- Natural Person associated with Legal Person Verification
- Natural Person associated with Legal Person Dataset
- Natural Person associated with Legal Person Documentation

Note – these are the already existing services currently exposed through the kompany API which will be used to offer higher level GRIDS services which are defined further below. These higher-level GRIDS services will be based upon these lower-level services with an extra layer of processing and logic.

It is expected that kompany will extend the use of its existing low-level services to offer more high-level GRIDS services, and also to update these services as the capabilities increase.

The first three of these services allow a company (as a Legal Person) to be discovered and the basic claims verified, supported with a dataset, and supported with documentation. These represent a sequence of degrees of verification.

The last three allow a natural person claiming an association with a legal person to be verified, supported with a dataset and supported with documentation. The last three are extensions of the first three, with the extra layer of natural person verification overlaid.

3 Legal Person and Corporate Know Your Customer Requirements

3.1 Introduction

The KYC requirements for Legal Persons and Corporates revolve around doing sufficient checks to provide assurance that the entity or person making a particular claim on behalf of that entity is indeed who they claim to be, that they can legally perform the operation they are attempting to do, and the entity for which they are attempting to perform the operation is as claimed. In the GRIDS platform this involves a series of 'claims' which may or may not have supporting 'evidence' and are gathered within one or more 'trust frameworks'. 'Claim', 'evidence' and 'trust framework' are used within the sense of the OpenID Connect for Identity Assurance specification. There are a number of predefined 'claims', 'evidence' and 'trust frameworks' already in use, but which are allowed to be expanded upon. Given that the existing trust frameworks are focused on Natural Persons, it is proposed in the GRIDS project to extend the standard to have one extra trust framework and other claims and evidence values, in order to support the KYC of legal persons.

KYC checks for corporate clients differs greatly from that for natural persons. Concepts such as identity cards, face to face validation, etc. are not valid for business KYC (KYB), although they are valid for natural persons representing a legal person – in such cases, though the validation of the natural person is not adequate to meet the requirements for KYB. The requirements are usually met by a series of business specific datasets, processes and documentation from official government business registers, which feed into a larger Governance, Risk and Compliance (GRC) model. It is these services that GRIDS and kompany in particular will be supplying. In the GRIDS model, the natural person will have been authenticated by eIDAS, and the DP will supply the business level information required on receipt of the validated natural person claims.

4 360kompany AG (kompany)

4.1 kompany Services

4.1.1 Introduction

As noted above, the lower level services kompany will indirectly expose through GRIDS will include:

- Legal Person Verification
- Legal Person Dataset
- Legal Person Documentation
- Legal Person VAT lookup
- Natural Person associated with Legal Person Verification
- Natural Person associated with Legal Person Dataset
- Natural Person associated with Legal Person Documentation

These will not be directly exposed to DCs through the GRIDS interface, but will be behind an interface and business logic layer. The business logic layer provides the access to existing API services present in kompany and will coordinate the sequencing and result manipulation to convert from the lower level services to the higher level services exposed through GRIDS.

4.1.2 High Level Architecture

The overall architecture is that of an interface layer which coordinates the communication between kompany, the BAA and the DC. This ensures the sequencing, validation, and processing of requests and responses to and from the other GRIDS components and the DPs themselves. This sits atop a translation layer which handles the bundling and translation of the services exposed through GRIDS into services which can be processed by our existing API infrastructure. The high level architecture of the system is as follows:

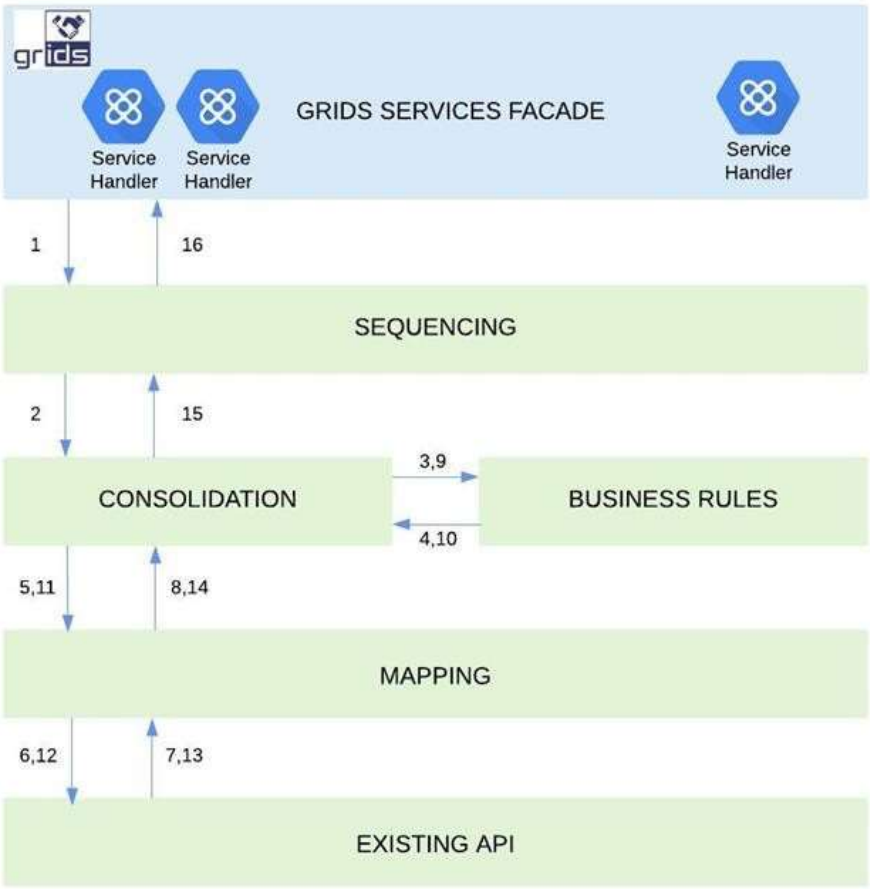

Figure 1: kompany Customisation Architecture

4.2 OpenID Connect Data Structures

4.2.1 Introduction

The interfaces within the system and between DC and DP are based on the OpenID Connect for Identity Assurance (IDA) specification implementing Distributed Claims, but due to the different requirements for business KYC as opposed to natural person KYC, a small number of extensions are proposed. These are designed to expose as much DP functionality and information as possible to the DC without wholesale alterations to the interface or forcing the DP to create multiple interfaces.

The IDA specification is defined in terms of 'trust frameworks' which categorize a validation process, 'claims' which are data points which may be requested to be verified ('verified_claims'), and 'evidence' which determines or indicates the sources of information that are, or can be, used to verify claims.

4.2.2 Trust Frameworks

For the support of business KYC activities as provided by kompany, a new trust framework 'grids_kyb' will be supported. This will allow business KYC specific requests to be made within the scope of the existing interface. There are existing frameworks defined, but these are not suitable for KYB. This does not preclude any other DP from supporting one of the predefined trust frameworks.

4.2.3 Supported Claims

As our focus is on KYB, we are mostly interested in Legal Persons. The predefined set of claims for Legal Persons within eIDAS is as follows:

Table 2: Supported Claims

Claim name	Data type
legal_name	string
legal_person_identifier	string
vat_registration	string
address	string
tax_reference	string
business_codes	string
lei	string
eori	string
seed	string
sic	string

Not all of these are fully or partially supported throughout Europe, and only the first two are declared as mandatory in the eIDAS minimum data set as derived from the ISA Core Vocabulary (https://joinup.ec.europa.eu/collection/registered-organization-vocabulary/solution/registered-organization-vocabulary/release/100). Furthermore, not all companies will have some of the optional claims (e.g. LEI), and the DP may not have access to some claims for all companies.

For kompany's purposes, the accepted verified claims will be:

- **legal_name** – assumed to be the registered name of the company
- **legal_person_identifier** – assumed to be the jurisdiction and the registration number of the company in the appropriate jurisdiction in the form XX/<registration number>, where XX is an ISO3166-1-alpha2 country code, and <registration number> is whatever format is issued for that jurisdiction.
- **lei** - assumed to be the LEI of the company
- **vat_registration** – assumed to be the vat number as registered for that company
- **address** – assumed to be the address of the Registered Office of the company as recorded in the appropriate register

kompany will also support the following legal person claims (not verified claims) where available and where appropriate:

- **tax_reference**
- **sic**

For support of natural persons associated with legal persons, kompany will also accept the following natural persons verified claims:

- **family_name**
- **given_name**
- **person_identifier**
- **birthdate**

In order to fully support the requirements for business KYC, it is proposed to extend the schema with some extra verified claims:

- **trading_status** – this is used to carry the status of the company back to the DC. It is an **optional** claim of type **String**.
- **business_role** – this is for use when a natural person is acting for a legal person, and indicates the capacity in which they are acting, for example, managing director, secretary, etc. It will be an **optional** claim of type **String**.
- **sub_jurisdiction** – this is for jurisdictions that can have name and/or registration number collisions within the same overall jurisdiction (e.g. Germany). This allows the DC to specify which jurisdiction the particular company is registered. It is an **optional** claim of type **String**.

4.2.4 Supported Evidence

The currently defined evidence types are:

- id_document
- utility_bill
- qes

For the purposes of legal persons, these are of little value (except, possibly the qes). To more accurately reflect the options available for legal person KYC, it is proposed to extend the specification with the following evidence types:

- **register_data** – this represents data which has been extracted from the relevant company register;
- **register_extract** – this represents an 'extract' from the corporate register which is a widely supported document version of the register_data;
- **register_document** – this represents any filed document(s) which may be available from the register for that company. For example, a DC might want the validate the company, obtain a **register_extract** and also the formation documents.

These have the following structures:

register_data has the following structure in a request:

```
{
      "type": {
            "value": "register_data"
            },
      "time":{
            "max_age": 12345
            }
}
```

And the following structure in a response:

```
{
      "type": {
            "value": "register_data"
            },
      "time":{
            "max_age": 12345
            "timestamp": <actual age of the data>
            }
      "data":{
            <data returned to the DC on top of validated claims>
            }
}
```

register_extract has the following structure in a request

```
{
      "type":{
            "value": "register_extract"
            }
}
```

And the following in a response:

```
{
      "type":{
            "value": "register_extract"
            },
      "document":      {
                  "url": <The URL from which to grab the document>
                  }
}
```

register_document has the following structure in a request:

```
{
      "type":{
            "value": "register_document"
            },
      "document":      {
                  "sku": <SKU to define the document requested>
                  "option": <Defines an option within the SKU>
                  }
}
```

And the following in a response:

```
{
      "type":{
            "value": "register_document"
            },
      "document":      {
                  "sku": <SKU to define the document requested>
                  "option": <Defines an option within the SKU>
                  "url": <The URL from which to grab the document>
                  }
}
```

Thus, the well-known configuration OP metadata snippet for kompany as a GRIDS DP for the request/response mechanism will look like:

```
{
…
      "claims_supported": [
            ],
      "verified_claims_supported": true,
      "trust_frameworks_supported": [
            "grids_kyb"
            ],
      "evidence_supported": [
            "register_data",
            "register_extract",
            "register_document"
            ],
      "claims_in_verified_claims_supported": [
            "legal_name",
```

```
            "legal_person_identifier",
            "lei",
            "vat_registration",
            "address",
            "tax_reference",
            "sic",
            "business_role",
            "sub_jurisdiction",
            "trading_status",
            "family_name",
            "given_name",
            "birthdate",
            "person_identifier"
            ],
…
}
```

The exact behaviour of the system depends upon the particular claims and evidence requested.

5 Data Provider Interfaces with GRIDS

5.1 Introduction

This section will detail the interfaces which kompany will provide and utilize in order to operate within the GRIDS framework. The interfaces themselves are covered in greater detail in the BAA Design document.

Implementation within kompany will be done in the form of a microservices framework.

5.2 Configuration Interface

5.2.1 Purpose

The well-known OIDC configuration endpoint interface is provided by the GRIDS Sequencing Layer, and is used to provide the BAA Configuration Manager with up to date metadata concerning the capabilities that are supported, such as the trust frameworks, the claims and evidence supported, etc. It is also used to report service health.

5.2.2 Specification

The interface is based on the OpenId Provider Configuration Information interface as described at: https://openid.net/specs/openid-connect-discovery-1_0.html#ProviderConfig.

5.3 UserInfo Interface

5.3.1 Purpose

The UserInfo interface is provided to allow the Data Consumer to access the services provided by kompany once the DC has established a trust token with the BAA which is passed to the kompany. This is the same format interface as the DC will have used to communicate with the BAA initially, but to the DP specific interface.

5.3.2 Specification

This interface is based on the OpenId Connect Core UserInfo interface described at: https://openid.net/specs/openid-connect-core-1_0.html#UserInfo.

5.4 JWKS (Java Web KeySet) Interface

5.4.1 Purpose

This interface exposes the public encryption keys that kompany will support for use within the GRIDS platform in a standard format. These keys can be read by the BAA and is used to encode the access token sent in the UserInfo query.

5.4.2 Specification

This data structure is defined by the IETF specification RFC7517 (https://tools.ietf.org/html/rfc75170), and the interface itself is a simple http GET, expected to be performed over https.

5.5 Data Consumer JWKS Interface

5.5.1 Purpose

This interface is used by the GRIDS Sequencing layer to request encryption keys that are suitable for use by the Data Consumer, in order to encrypt the responses to their requests.

5.5.2 Specification

This data structure is defined by the IETF specification RFC7517 (https://tools.ietf.org/html/rfc75170), and the interface itself is a simple http GET, expected to be performed over https.

5.6 Introspection Interface

5.6.1 Purpose

This interface allows the DP (kompany) to query the BAA for information on the DC requesting a KYC service. The introspection access token passed to the DC by the BAA will be passed from the DC to kompany which will use this token to query the clientId to the BAA via this interface. The BAA will respond with the client data including the JWKS uri.

5.6.2 Specification

Information regarding this interface can be found at: https://www.oauth.com/oauth2-servers/token-introspection-endpoint/

5.7 BAA Configuration Interface

5.7.1 Purpose

This interface is used by the DP to request information from the BAA regarding the list of trusted BAAs who can issue JWT UserInfo requests, and also to query the issuing BAA for the JWKS URI for the requesting DP

5.7.2 Specification

The interface is based on the OpenId Provider Configuration Information interface as described at: https://openid.net/specs/openid-connect-discovery-1_0.html#ProviderConfig

6 GRIDS Sequencing Layer

6.1 Introduction

The role of the GRIDS Sequencing Layer is to provide the microservice framework for the inbound interfaces, and liaise between them, the kompany Translation Layer, and the outbound interfaces as described above. It is also responsible for correctly formatting the responses to the DC requests, including any encryption necessary, and for the kompany API key of the DC through to the kompany Translation Layer, so that can be used for the low level API requests.

The primary purpose is to handle requests from DCs coming through the UserInfo interface, liaising with the BAA, handling the request and replying to the DC.

6.2 Interface Sequencing

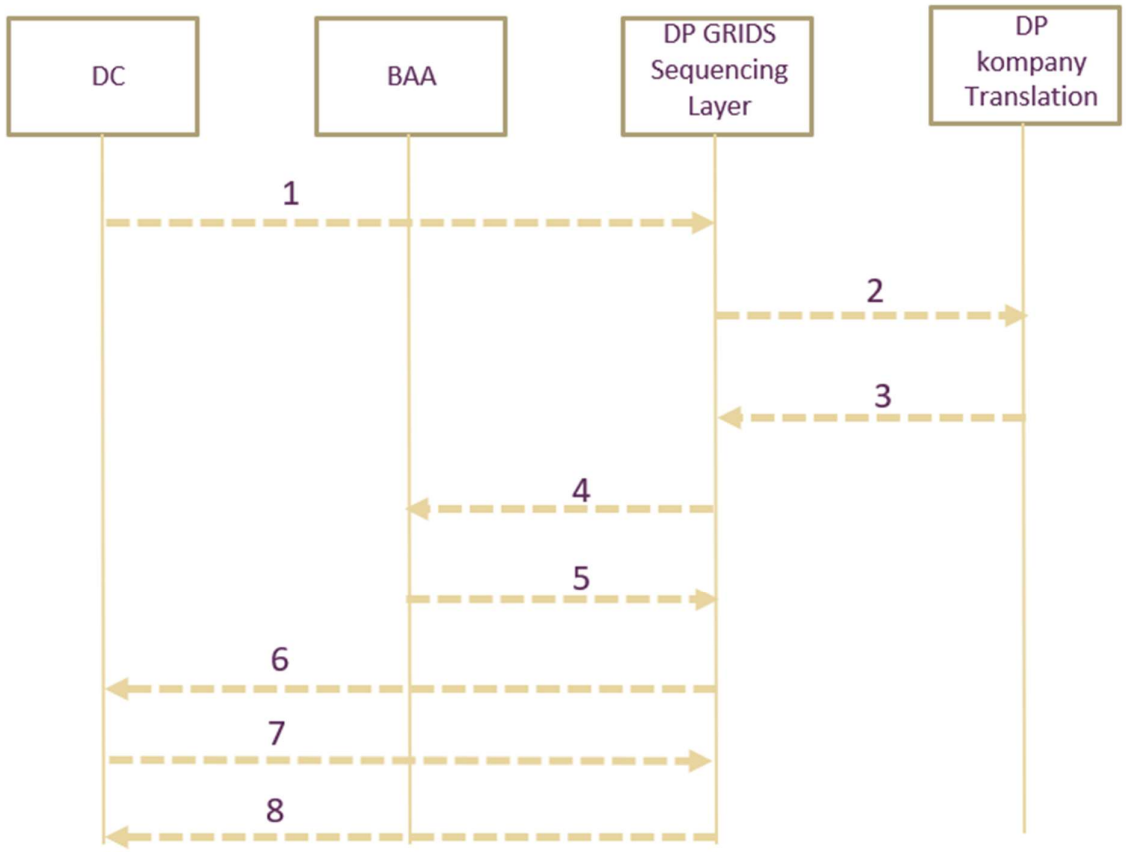

Figure 2: GRIDS Layer Interface Sequencing

1. DP receives request from DC over the UserInfo request, decodes the self-describing token and extracts the claims and verifying charging information
2. DP passes the through to the kompany Translation Layer
3. DP receives the response from the kompany Translation Layer
4. DP queries the BAA Client Introspection Interface for the client JWK URI
5. BAA replies with the client JWK URI
6. DP queries the DC JWKS interface for the manner in which the reply should be handled
7. DC replies as appropriate
8. DP prepares the token response as per the DCs JWKS either, plain, signed and/or encrypted.

6.3 Error Handling

This layer is required to handle errors which may occur during its own processing, as well as those which may be encountered during the handling of any requests passed to the kompany Transation Layer. These errors should be logged through to the event interface.

7 kompany Translation Layer

7.1 Introduction

This layer handles the conversion of GRIDS calls into kompany API calls, including processing of the subsequent responses including data matching and correlation, and creation of the response to be passed back to the DC via the GRIDS Sequencing Layer. This layer also handles the charging and authentication at API level, which for kompany requires each DC to have an API account with us, and for which they will have to provide in the UserInfo Interface request.

7.2 API call translation

Each GRIDS level call will result in one or more calls to our existing API. In the case of a single call, this layer will be responsible for making the call, performing any processing or matching logic, and formatting the response for passing back to the GRIDS Sequencing Layer, which will pass onto the requesting DC.

In the case of multiple API calls, this layer is also responsible for maintaining the relationship between the calls, and performing any correlation or intra-dataset processing before formatting the final response for passing back to the GRIDS Sequencing Layer for onward transfer to the requesting DC.

This structure allows us to provide complex matching of data for Legal Persons and Natural Persons associated with Legal Persons without the need for the DC to make multiple requests and provide complex logic themselves.

7.3 Error Handling

As each GRIDS call is translated into one or more API calls, there are numerous sources of errors. This layer needs to be resilient and to pass exceptions to the centralized kompany error logging mechanism, including the 'txn' reference passed from the BAA for wider debugging.

7.4 Architecture and Call Sequences

The architecture of the Translation Layer is shown in Figure 3

It consists of a GRIDS Service Façade Layer acting as the interface between the GRIDS Sequencing Layer and the rest of the architecture. It has dedicated Service Handler modules, which represent a 1:1 relationship between them and each GRIDS service exposed through the UserInfo interface. The Service Handler is responsible for translating the data structures to and from those sent through the UserInfo interface.

The Service Handlers within the Services Façade Layer communicate to the Sequencing Layer, which is responsible for specifying the flow of calls to the existing API, particularly for when a single GRIDS service maps to two or more invocations of existing API calls.

The Sequencing Layer passes the list of individual API call requests to the Consolidation Layer, which makes calls to the Mapping Layer, which converts them to the actual calls made to the existing API. The Consolidation Layer uses a Business Rules module to make business decisions based on the content of the request, and the results of calls made to the API.

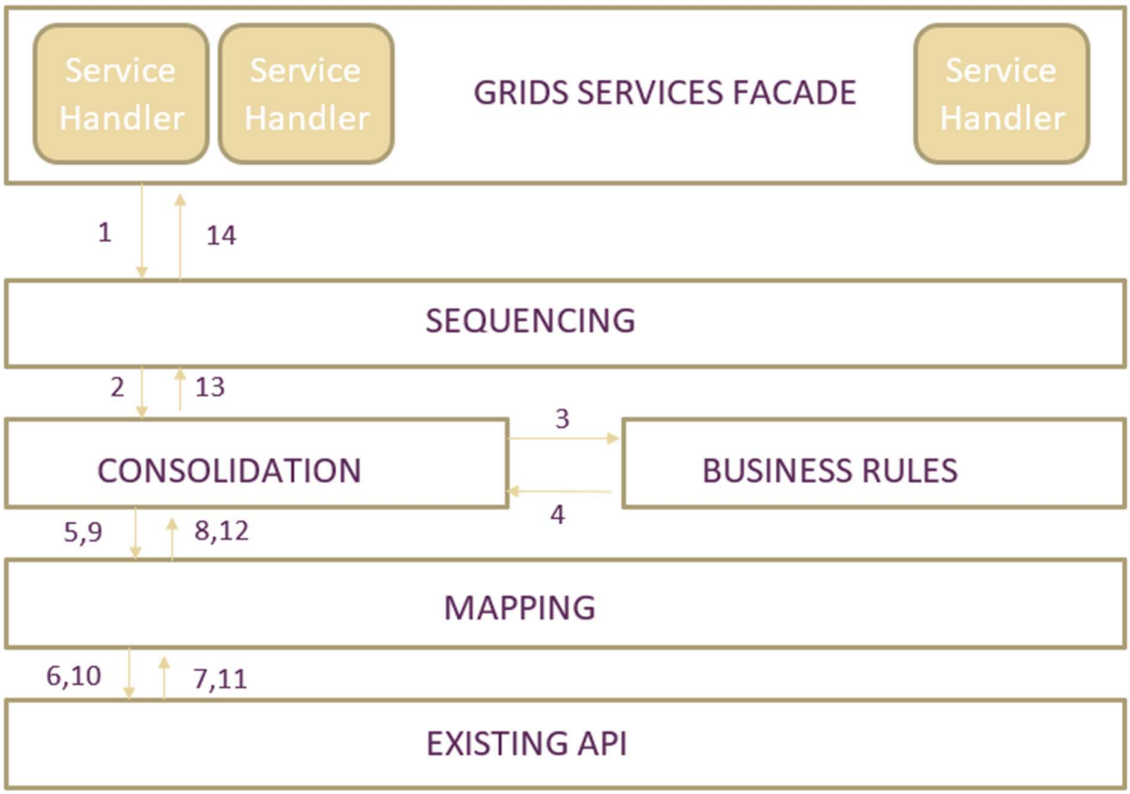

Figure 3: kompany Translation Layer

A typical flow involving double lower-level calls would be as follows:

1. A request made through the UserInfo interface is passed through to the appropriate Service Handler in the GRIDS Services Façade Layer, which hands it off to the Sequencing Layer
2. The Sequencing Layer determines the sequence of lower level API calls should be made and instructs the Consolidation Layer
3. The Consolidation Layer uses the Business Rules to determine what special handling should be performed for the request
4. Business Rules module returns any special instructions
5. The call is passed to the Mapping Layer which translates it into the appropriate call to the existing kompany API
6. Mapping Layer makes the call to the API
7. The response from the API passes back to the Mapping Layer
8. Mapping Layer passes it back to the Consolidation Layer
9. Consolidation sends the 2nd request to Mapping
10. Mapping makes the 2nd request to the API
11. API replies to the Mapping Layer
12. Mapping transfers the reply to the Consolidation Layer
13. Consolidation layer prepares the response based on the results and the business rules, and hands it back to the Sequencing Layer
14. Sequencing Layer hands the result back to the Service Handler for onward transmission

8 Conclusions

The work necessary to integrate kompany into GRIDS is considerable, but manageable. The use of standardised, well specified interfaces enables this with some specific architectural layers which sit on top of existing services.