H2020-SC6-GOVERNANCE-2018-2019-2020

DT-GOVERNANCE-05-2018-2019-2020

ACROSS Towards user journeys for the delivery of cross-border services ensuring data sovereignty

D3.3: Implementation of the ACROSS Data Governance framework for data sovereignty - Initial

Project Reference No	959157 — ACROSS — H2020-SC6-GOVERNANCE-2018-2019-2020
Deliverable	D3.3: Implementation of the ACROSS Data Governance framework for data sovereignty - Initial
Work package	WP3: ACROSS Data Governance framework
Nature	Other
Dissemination Level	Public
Date	22/02/2022
Status	Final version
Editor(s)	Valentín Sánchez (TEC)
Contributor(s)	-
Reviewer(s)	Vincenzo Savarino (ENG), Jefferson Kühl (DATAPORT), Enrique Areizaga (TEC), Idoia Murua (TEC)
Document description	This report includes the analysis of the applicability of a concrete set of technologies/products: CaPe, IDS Data usage control, Personal wallet and Attribute Based Credentials. Furthermore, this deliverable includes the specification and design of a first version of the ACROSS Personal Data Management Framework covering the basic set of functionalities, the so-called a minimum viable product.

About

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

DISCLAIMER

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use, which may be made of the information contained therein.

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V0.1	14/02/2021	First draft for revision	TECNALIA
V0.2	15/02/2022	Second draft for revision	ENGINEERING
V0.3	16/02/2022	Third draft for revision	DATAPORT
V1.0	22/02/2022	Final version	TECNALIA

Executive Summary

The main objective of the ACROSS project is to provide the means (tools, methods and techniques) to enable user-centric design and implementation of interoperable cross-border (digital) public services compliant with the current European regulations (e.g. the Single Digital Gateway (SDG) and Once-Only principle (OOP), European Interoperability Framework (EIF)) where the private sector can also interconnect their services **while ensuring the data sovereignty of the citizens, who can set the privacy level that will allow the public and private sector to access to their data based on their requirements**.

In order to ensure the protection of personal data (and documents) and its compliance with GDPR and other relevant regulations, especially when shared between organizations, ACROSS will design and implement with **a data governance framework** where data subjects can control the use of their personal data empowering them**.**

The **data governance framework will** allow users to:

1. monitor which data are available and how they are used or how it has been accessed,
2. control: add, delete or change data, provide or block access to public bodies (where permitted or enforced by the law), businesses or data brokers, giving individuals the power to determine how their data can be used.

Previous deliverables have gathered the ACROSS data governance framework requirements, including the data governance, security and privacy requirements from the use cases, considering both the technical and operational perspectives, the final user expectations regarding data privacy and the ACROSS platform integration strategy. Also, a draft version of the framework architecture has been depicted and a set of relevant baseline technologies that could be used for the implementation of the data governance framework has been identified.

This report includes the analysis of the applicability of a concrete set of technologies/products:

1. **MyData[1] model for human-centered personal data management and processing**: CaPe[2] open source implementation of the MyData Operator concept.

[1] https://mydata.org/
[2] https://github.com/OPSILab/Cape

2. **Attribute-Based Credentials techniques**: DECODE[3] project and IRMA[4].
3. **IDSA data sovereignty concept and *data usage policies*[5] enforcement**: Data usage application implementation by TECNALIA.

Resulting from this analysis some extensions or adaptations have been identified.

Furthermore, this deliverable includes the specification and design of a first version of the ACROSS Personal Data Management Framework covering the basic set of functionalities, the so-called a minimum viable product. This initial version will be extended along the project to produce the final implementation of the ACROSS Data Governance framework for data sovereignty.

[3] http://decodeproject.eu/
[4] https://privacybydesign.foundation/en/
[5] https://internationaldataspaces.org/data-sovereignty-updated-position-paper-on-data-usage-control-in-the-ids/

Table of Contents

List of Figures

List of Tables

List of Terms and Abbreviations

Abbreviation	Definition
IDSA	International Data Space Association
CPSV-AP	Core Public Service Vocabulary Application Profile
ABC	Attribute Based Credentials
GDPR	General Data Protection Regulation
DGA	Data Governance Act
PIMS	Personal Information Management System
SDGR	Single Digital Gateway Regulation
OOP	Once-only principle
CRUD	Create, Read, Update and Delete
DPV	Data Privacy Vocabulary

1 Introduction

1.1 Context

One of the ACROSS objectives is **to ensure the protection of personal data (**and documents**) and its compliance with GDPR and other relevant regulations, especially when shared between organizations.** This objective will be fulfilled by designing and implementing a private/personal data governance framework where data subjects can control the use of their personal data empowering them.

ACROSS will offer the citizen the possibility of defining which public and private organization will be allowed to *access which data and for what purpose* trough the **ACROSS Data Governance Framework.** The main aim is to give the citizen the chance of **govern the access to** their data, profiting from a set of usage policies that implement levels of access and they can be the **sovereign owner** of such data.

The **data governance framework,** that allows users to

1) monitor which data are available and how they are used or how it has been accessed,
2) to control: add, delete or change data, provide or block access to public bodies (where permitted or enforced by the law) businesses or data brokers, giving individuals the power to determine how their data can be used.

From a technical point of view the Data governance framework includes:

1) A "private/personal data" governance platform including a Personal data management site which provides a user interface to define manage and control the use of personal data. (Data portal)
2) A set of APIs/libraries to interact with the ACROSS platform

The governance framework will be based on existing initiatives and techniques.

1. **MyData**[6] model for human-centered personal data management and processing and MyData operator concept[7] (See section 8.1.2)
2. Built on experiences around **Attribute-Based Credentials** approaches in the DECODE[8] project,
3. Include generic ***data usage policies***[9] when the private data needs to be transferred among several stakeholders (IDSA Data Sovereignty)

[6] https://mydata.org/
[7] https://mydata.org/mydata-operators/
[8] http://decodeproject.eu/
[9] https://internationaldataspaces.org/data-sovereignty-updated-position-paper-on-data-usage-control-in-the-ids/

D3.1 (Design of the ACROSS Data Governance framework for data sovereignty – Initial) provided an accurate description of the ACROSS data governance framework requirements, along with a first draft of technical architecture, modules, and APIs.

Besides, a set of relevant baseline technologies that will be used for the implementation of the data governance framework were described and their applicability to ACROSS was analysed.

These following conclusions from D3.1 have driven the evolution of the data governance framework design and its implementation.

- The ACROSS Personal Data Governance Framework is part of the so-called ACROSS platform, useful in the context of cross-border public/private services for the citizens. However, it has been designed to be an independent framework useful also for the individuals to manage their personal data according to the GDPR in any other context.
- ACROSS data governance framework does not cover the following functionalities included in most of the initiatives:
  - Secure Data Storage
  - Secure Data transfer among services
- ACROSS will analyse how to extend the MyData operator with the following functionalities:
  - Data minimization via the ABC technology
  - Data usage policies

1.2 Purpose and Scope

Based on the results gathered in D3.1 the applicability of a concrete set of technologies/products have been analysed:

4. **MyData[10] model for human-centered personal data management and processing**: CaPe[11] as open source implementation of the MyData Operator concepts.
5. **Attribute-Based Credentials techniques**: DECODE[12] project and IRMA[13].
6. **IDSA data sovereignty concept and *data usage policies*[14] enforcement**: Data usage application implementation by TECNALIA.

[10] https://mydata.org/
[11] https://github.com/OPSILab/Cape
[12] http://decodeproject.eu/
[13] https://privacybydesign.foundation/en/
[14] https://internationaldataspaces.org/data-sovereignty-updated-position-paper-on-data-usage-control-in-the-ids/

Resulting from this analysis, some technologies/products have been discarded, while some extensions or adaptations have been identified in other cases.

This deliverable includes the specification and design of a first version of the ACROSS Personal Data Management Framework covering the basic set of functionalities (the so-called a minimum viable product) that will be the base for D3.2 “Design of the ACROSS Data Governance framework for data sovereignty – Final”. This initial version will be extended along the project to produce D3.4 and D3.5: Implementation of the ACROSS Data Governance framework for data sovereignty – Intermediate and Final.

Finally, some conclusions are presented along with a set of next steps.

1.3 Approach for Work Package and Relation to other Work Packages and Deliverables

The goal of WP3 is to design, implement and deploy a “private/personal data” governance framework that allows the citizens to control how their data and their activities are created or used by businesses, governments, or data brokers, giving individuals the power to determine how their data can be used. The governance framework will be based on existing solutions such as MyData model for human-centred personal data management and processing and built on experiences around Attribute-Based Credentials approaches in the DECODE project, but it will also include generic data usage policies when the private data needs to be transferred among several stakeholders.

The services from this WP will be integrated into the platform created in WP5 and will demonstrate the functionality of the use cases in WP6.

WP5 aims at providing the architectural and implementation aspects for the delivery of the ACROSS tools taking into account the full range of requirements for such service. The design of the ACROSS platform will drive the design and implementation of the various components produced in the context of WPs WP3, WP4 & WP5.

WP2 and WP6 together have defined the so-called user journeys based on the results several interviews with people from the three pilot countries. The aim of the interview process is to form potential user journeys, building on initial ideas. User journeys can include actions, touch points, emotions, pain points, and phases. Eventually to result in concrete (socio-technical) requirements for the ACROSS platform modules. A specific section about Data privacy issues has been included in the questionnaire in order to gather requirements for the Data Governance Framework.

The Data Governance Framework will be designed as an independent platform, but it will share some components with the ACROSS platform (defined in WP4 and WP5). Furthermore, a set of APIs will be defined to interact with some other modules, as the User Journey Service Engine.

The decisions presented in this deliverable are a subject to refinements and modifications, based on the progress of the other work packages, as well as the validation and evaluation phases.

1.4 Structure of the Deliverable

This deliverable has been structured in the following sections:

- **Section 2** analyses the CaPe open source implementation of the MyData Operator concept and its applicability to ACROSS.
- **Section 3** includes a description of the IDS approach to data usage control, the open data usage app developed by TECNALIA and the adaptation needed to be used by the ACROSS personal data framework.
- **Section 4** describe the result of the analysis of several ABC technologies and projects.
- **Section 5** includes the specification and design of a first version of the ACROSS Personal Data Management Framework covering the basic set of functionalities.
- Finally, some conclusions are drawn together with recommendations for future work.

2 CAPE vs ACROSS Personal Data Framework

This section presents the results of the analysis of CaPe[15], an open source solution that implements MyData principles and MyData Operator concepts, from the point of view of its applicability to the ACROSS Personal Data Framework.

First, the CaPe approach and architecture is described, based on the product documentation[16]. The description includes the CaPe basic architecture, its modules and the functionality they provide. A second subsection is dedicated to the CaPe workflow which explains how each core component is involved to support the end to end process of consent management. The workflow also describes the actors involved in the process and how they interact with CaPe. These two first sections provide a summary of the more detailed information in the CaPe documentation, containing only the information needed for the analysis.

The CaPe workflow has been analysed taking into account the requirements and constraints imposed by the ACROSS User journey workflow engine, the current and (possibly) future authentication and authorization frameworks and the current implementation and deployment of both public and private services.

Resulting from this analysis, some extensions or adaptations have been identified.

2.1 CAPE approach and architecture

CaPe is a consent-based and user-centric platform targeted at organizations acting as Data Processors, in the private or public sector. It enables them to take advantage of the value of personal data in compliance with GDPR while providing data subjects the natural need to detain both the use and the protection on their own data. CaPe acts as an intermediary and creates a communication channel between Data Subjects and Data Controllers and related processors.

[15] https://github.com/OPSILab/Cape
[16] CaPe (cape-suite.readthedocs.io)

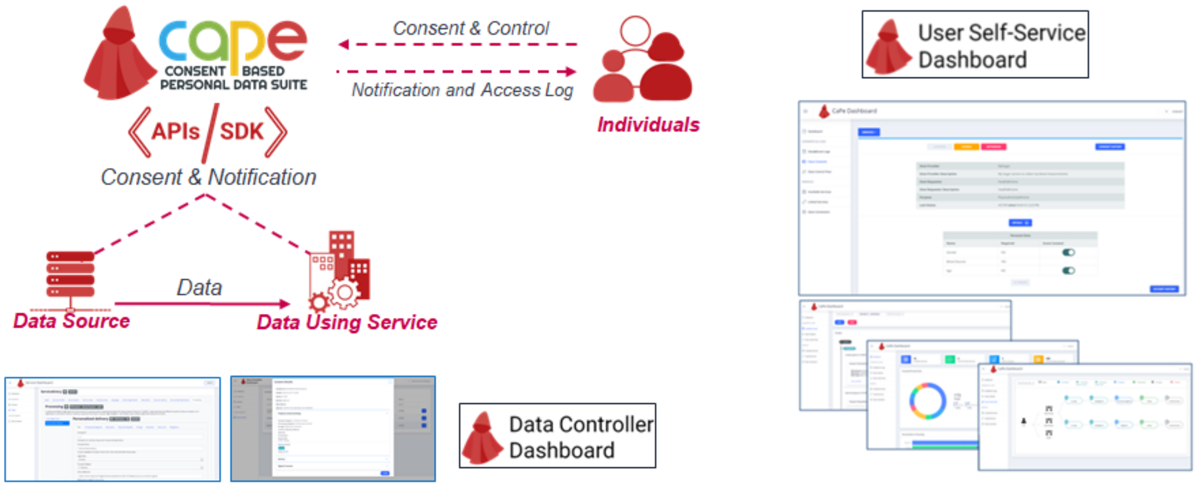

cape
CONSENT BASED PERSONAL DATA SUITE
Consent & Control
Notification and Access Log
Individuals
APIs
SDK
Consent & Notification
Data
Data Source
Data Using Service
User Self-Service Dashboard
Data Controller Dashboard

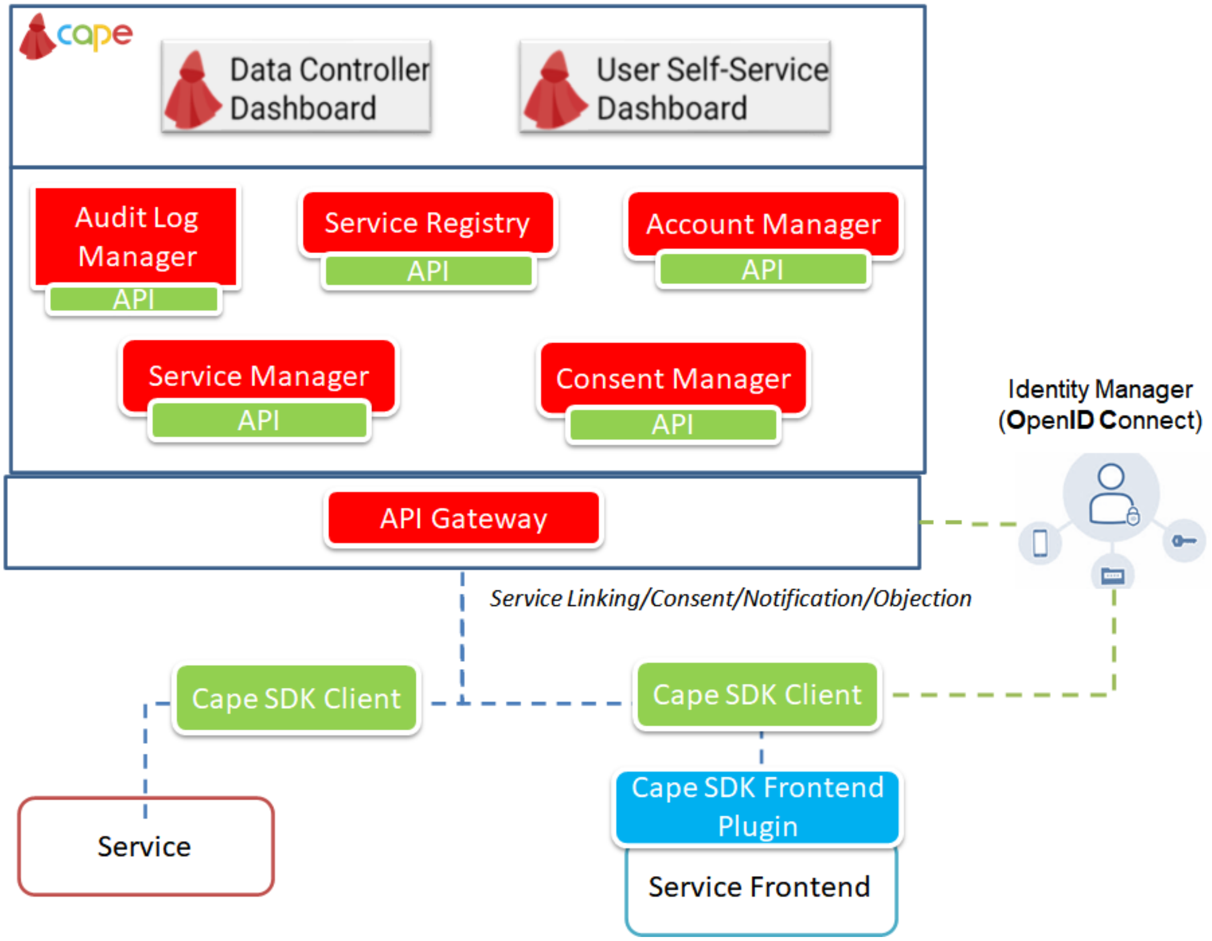
Figure 1 CaPe solution as an intermediary between Data Controller/Processor and Data Subject

CaPe platform provides a suite of tools and services providing:

- **Consent Management** – to manage data owner's consent to leverage personal data lawfully
- **Transparency tools** – to allow individuals to have control over the use and sharing of their data
- **SDK/APIs Ecosystem** – to build innovative applications and interact with existing legacy systems/services

2.1.1 CaPe Architecture Overview

CaPe suite is a platform based on the microservices paradigm, in which several modules expose a set of APIs through an API Gateway, to be consumed by Frontend Apps and external services. The following picture illustrates the architecture of the CaPe Suite.



The architecture is composed by a set of core backend microservices (**Cape Server** and **Cape SDK**) and a set of frontend apps (**User Dashboard** and **Data Controller Dashboard**).

2.1.1.1 CaPe Server

This is the core of the CaPe platform. It implements and exposes all the main functionalities provided by CaPe, regarding the lifecycle management and storage of Service Descriptions, Service Linking, Consent Records and Auditing.

Its main components are:

- **Account Manager**: Manage the lifecycle of the Cape Account, Account signing keys for Service Linking.
- **Service Manager**: Manage the Service Linking internal processes and Service Link Record storage.
- **Consent Manager**: Manage the Consent Records lifecycle, the generation of Consent Forms, etc.

- **Auditlog Manager**: Collects aggregated auditing statistics, triggered by incoming Event Logs (ServiceLink, Consent or Data Processing) regarding a specific Account.
- **Service Registry**: Collects the Service Descriptions and registrations (Signing keys and certificates).

Each of the components above will be deployed with a tightly coupled storage service.

2.1.1.2 CaPe SDK

CaPe functionalities, such as Service Linking and Consent Management, can be accessed by a generic external Service, previously described and registered in CaPe by its Service Provider, acting as Data Controller. The Service Provider wanting to use CaPe, will use the **Cape Service SDK** package composed by:

- **CaPe SDK Client**: Backend application acting as a client between the Service itself and CaPe Server APIs, exposing also its own APIs to interact with SDK Frontend and Data Controller Dashboard. It comprises also the storage to hold the assets received by Cape Server (Signing keys, Service Link Records and Consent Records).
- **CaPe SDK Frontend Plugins**: Frontend plugins (e.g. Angular module with an Action Menu) to be embedded in the Service frontend, providing Service Linking and Consenting functionalities, communicating with the SDK Client and then with CaPe Server.

2.1.1.3 CaPe Dashboards

The CaPe Suite comprises the following Frontend dashboards, which will be used by the End User (Data Subject) and Service Provider (Data Controller) respectively:

- **User Self-Service Dashboard**: Single point for the End User to have an overview, verify and modify which data are used, and how and for which purpose. In addition, the user can view Event Logs and modify Linked Services and Consents previously given when logged at the Service ends.
- **Data Controller Dashboard**: Entry point for the Service Provider to manage the Semantic Descriptions and registrations of its own provided Services, view and manage the Service Linking and Consents status given by all the Users of its registered services.

2.1.1.4 Identity and Access Management

CaPe must interact with any Identity Manager that supports OpenID Connect and OAuth2 authorization framework. Cape Dashboards will use the Open Id Connect protocol upon the OAuth2 Authorization workflows, in order to perform User authentication and obtain an Access Token (JWT), which will be used to grant access to CapPe APIs. Similarly, a client application/service wanting to integrate with CaPe, will perform OAuth2 Authorization, obtaining an Access Token to be used in the request made to the CaPe Service SDK APIs.

2.1.2 CaPe Workflow

Each CaPe core component is involved to support the end to end process of consent management. In order to use all the functionalities, a workflow has been designed and consists of the following steps:

1. Service description and registration
2. Service Linking
3. Consent Request (for processing within a service or sharing among services)
4. Data Request, Notification and Activity Logs
5. Consent Management & User Data Usage Control

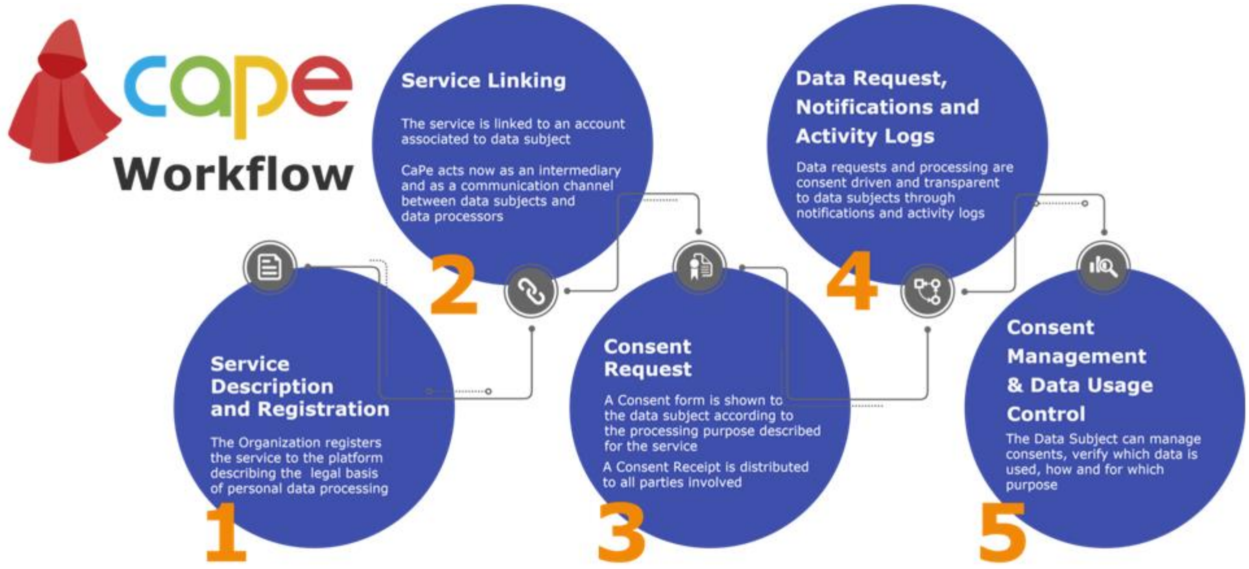
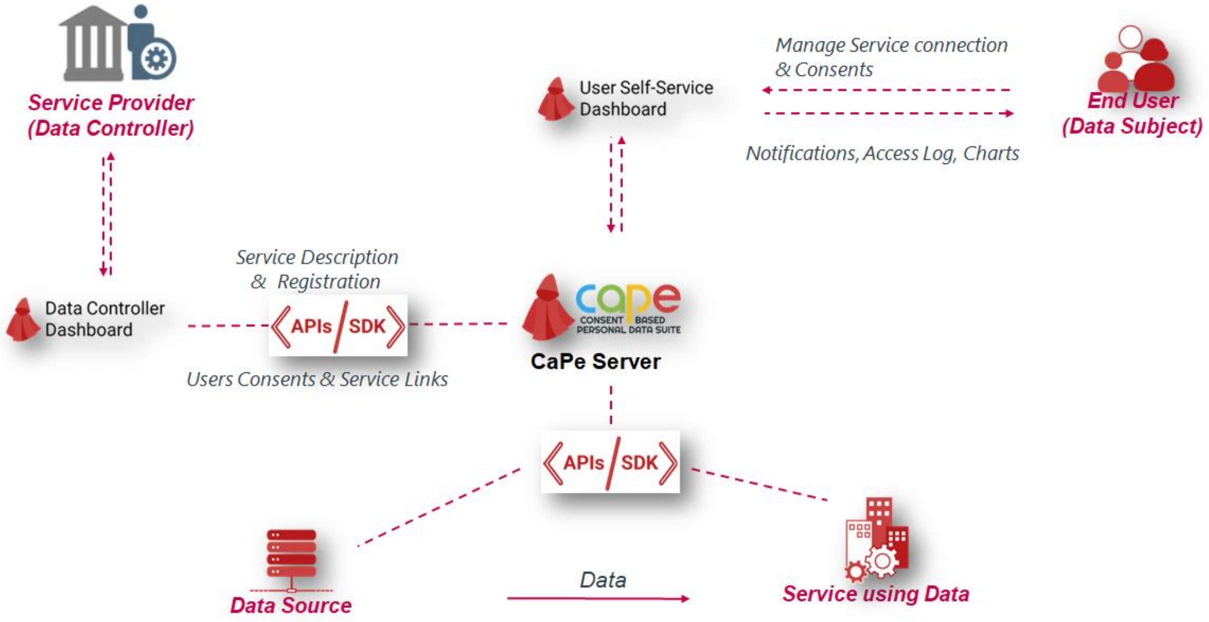

cape
Workflow
Service Linking
The service is linked to an account associated to data subject
CaPe acts now as an intermediary and as a communication channel between data subjects and data processors
2
Data Request, Notifications and Activity Logs
Data requests and processing are consent driven and transparent to data subjects through notifications and activity logs
4
Service Description and Registration
The Organization registers the service to the platform describing the legal basis of personal data processing
1
Consent Request
A Consent form is shown to the data subject according to the processing purpose described for the service
A Consent Receipt is distributed to all parties involved
3
Consent Management & Data Usage Control
The Data Subject can manage consents, verify which data is used, how and for which purpose
5

Figure 2 CaPe Workflow

Next figure shows tha actors and interacitons among them, including:

- **Service provider** acting as data controller and interacting with CaPe throught the Data Controller dashboard.
- End user acting as data subject and interacting with CaPe throught the User Self-service Dashboard.

- Service acting as **Data source**: System sending data to the data sync and interactingh with CaPe thought the CaPe APIs.
- Service acting as **Data sink**: System receiving data from the data source and interacting with CaPe thought the CaPe APIs.


Service Provider (Data Controller)
User Self-Service Dashboard
Manage Service connection & Consents
Notifications, Access Log, Charts
End User (Data Subject)
Service Description & Registration
Data Controller Dashboard
APIs SDK
Users Consents & Service Links
cape CONSENT BASED PERSONAL DATA SUITE
CaPe Server
APIs SDK
Data Source
Data
Service using Data

2.1.2.1 Service description and registration

The Service registration on CaPe consists of two mandatory steps:

- Service Description
- Service Registration

Each service that will interact with CaPe must be described and registered in the CaPe platform (Service Registry). The description in particular provides, as well as basic information, the description of the data that will be processed for each purpose with reference to a specific privacy statement. Service description can be provided by the following:

1. Using the Service Editor tool provided in the Data Controller Dashboard.
2. Directly issuing the Service Description through specific APIs exposed by Service Registry and accessed through CaPe SDK APIs.

Service Description refers to a specific metamodel, defined by extending MyData specifications and ISA2 Common Public Service Vocabulary Application Profile (CPSV-AP) and specifying semantic description of legal basis of personal data processing.

2.1.2.2 Service Linking

In order to interact with a specific Data Subject and request a lawfully data processing consent, each registered service must be linked with a specific User's CaPe Account that identifies the data subject at CaPe system. This "Service Linking" phase creates a one-to-many reference between the identification of the data subject at CaPe (Account Id) and his/her identification at each service (Surrogate Id).

2.1.2.3 Consent Request (for processing within a service or sharing among services)

Once a service has been linked to a Cape Account, the service can be authorised to process data by conducting the Consenting phase This process always starts when the user either accesses the service for the first time or the processing conditions for that specific purpose have changed.

CaPe supports two types of consent:

- **Within a service**: Consent is required for processing of data within a single service itself, for different purposes for which personal data have been obtained and if it optionally will share them with other companies/services for the declared purposes. The generated Consent will have the **Resource Set**, containing the datasets with data concepts being object of each specific processing purpose.
- **Sharing between services**: Consent is required for the explicit sharing of personal data between data sources (Source) and data using services (Sink), for a specific processing purpose. After a Source and a Sink have been linked to CaPe Account, the Sink can be authorised to access data on the Source by conducting a two-party Consenting step. The step results in a pair of Consent Records. The Consent pair will have also in this case the **Resource Set**, but containing datasets matching with the intersection between datasets provided by Sink and Source descriptions. Once a Source and a Sink have been linked to CaPe Account, the Sink can be authorised to access data on the Source by conducting a two-party Consenting step. The step results in a pair of Consent Records. The Consent pair will have also in this case the Resource Set, but containing datasets matching with the intersection between datasets provided by Sink and Source descriptions.

Consent Record (CR): is the outcome of the Consenting phase, it documents the permission the End User (Data Subject) has granted to a specific service for a specific processing purpose. It contains all the policies information about the data processing type, purpose category, datasets involved (Resource Set), sharing with third parties, storage, etc. Service's service description contains a description of all data a service can provision or process. End User creates (through CaPe) a Resource Set while creating a consent by selecting a set of data for processing (depending on purposes defined by the Service).

In order to define the consent, the End User has to log in the Service for which wants to consent data processing for a specific purpose.

- End User views the Consent Form dynamically generated by CaPe relying on the processing purpose and details (processing categories, legal basis, resource set, etc.) described during service description phase.
- Selects/deselect optional data and visualizes required data and policies for processing.
- End User gives the consent by submitting the Consent Form to CaPe server.

2.1.2.4 Data Request, Notification and Activity Logs

Once the Consent has been given for a specific linked Service or Sink/Source services pair, the data processing/data transfer request can take place and will be regulated by CaPe's Consent enforcement. In particular:

- **Within service case**: Service will process End User's personal data according to status, rules and policies defined in the related Consent Record issued by End User consenting phase.
- **Sharing between services**: Both Source and Sink have their own Consent Record, which contains role specific information necessary in establishing a Data Connection between Source and Sink.

Enforcement of an issued Consent Record can be accomplished by integrated Service by interacting with CaPe SDK APIs, according to increasing steps of interaction with CaPe capabilities and complexity:

- **Consent Enforcement:** Consent Record MUST be validated every time data is processed based on the consent. Service processing End User personal data and being part of a Consent issued by the user itself, will use Consent Record APIs of CaPe SDK to verify the existence of that Consent Record for the specific User and Dataset being processed and its relative Consent Status.
  With this level of interaction, CaPe is responsible only of issuing signed Consent Records. In this way CaPe does not guarantee that the data is actually processed according to the held consent, but only guarantees the integrity of Consent Record. It is up to the specific Service implementation to check that the retrieved Consent Record is valid before processing related End User personal Data
- **Usage Rules Enforcement with input Data Payload:** Relying on held Consent Records, CaPe is capable of generating related Usage Rules that will use internally to filter input Data Payloads. Service processing End User personal data and being part of a Consent issued by the User itself, will use

Enforcement API of Cape SDK to issue Data payloads (JSON body) containing personal data, to be filtered out according to enabled Personal Data Concepts contained in the Dataset inside the specific Consent Record (if any). Indeed, if there is no active Consent Record for the specified User and dataset, CaPe will reject the whole payload returning a 404 Not Found error.
With this level of interaction, CaPe is responsible also of actually enforcing Usage Rules derived from held Consent Records to personal data payloads. In this way, Service is eased by the burden of implementing checks on Consent Records and data filtering.

- **Data Request:** Relying on previously described steps, in case of sharing between Sink and Source services, CaPe provides a stricter Data Transfer functionality. The Sink service will send to the Source service a CaPe specific Data Request, in order to retrieve from it the datasets regulated by a Consent Record. This is the most advanced and complex level of integration with CaPe. In this case CaPe will guarantee the whole process of enforcing Consent Records and derived Usage Rules but even the Data exchange between Sink and Source, by regulating Data request with Pop Key and Authorisation Token enforcement.

2.1.2.5 Consent Management & User Data Usage Control

CaPe End Users can manage the overall lifecycle of their own Data Usage Consents by interacting with CaPe User Self-Service Dashboard. Data Usage Control is not covered by now.

2.2 Applicability of CaPe to the ACROSS Data Governance Framework

The following design principles has been taken into account in the definition and design of the ACROSS Data Governance Framework.

- Minimize the Service providers adaptation needed to use the framework.
- To be compliant with the emerging initiatives in the area of authentication and authorization, i.e. eIDAS and SSI.
- Secure storage is provided by leveraging the personal data wallet technologies

Next table shows the mapping between the actors participating in CaPe and those defined in ACROSS.

Table 1 Cape actors mapping in ACROSS

CAPE	ACROSS	Type of actor/interaction
Service provider acting as data controller and interacting with CaPe through the Data Controller dashboard	Public or private service providing cross border services	Person interacting through a Graphical user interface
End user acting as data subject and interacting with CaPe throught the User Self-service Dashboard	End user acting as data subject and interacting with the ACROSS Personal data framework throught the Transparency Dashboard	Person interacting through a Graphical user interface
Service acting as **Data source.** System sending data to the data Sink and interacting with CaPe throught the CaPe SDK/APIs.	ACROSS Platform, specifically the ACROSS User Journey Workflow Engine.	Software interacting with other systems via an API with the support of an SDK.
Service acting as **Data Sink.** System receiving data from the data source and interactingh with CaPe thought the CaPe SDK/APIs.	Public or private service provider included in the workflow.	Software interacting with other systems via an API with the support of an SDK.

Next figure shows the actors mapping. In order to minimize the service providers adaptation needed to use the framework, there will be no interaction among the public/private services used by the workflow engine and the Personal Data Framework.

The only requirement for the service provider will be to register the service in ACROSS using the Service Registry front-end.

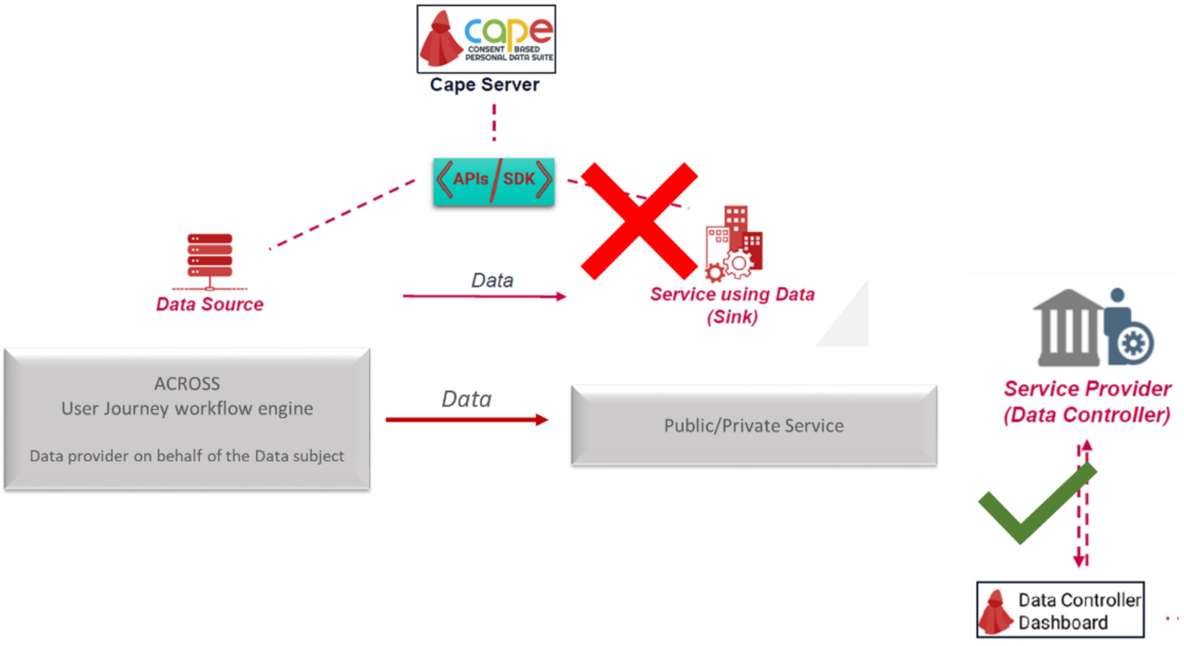

cape CONSENT BASED PERSONAL DATA SUITE
Cape Server
APIs SDK
Data Source
Data
Service using Data (Sink)
Service Provider (Data Controller)
ACROSS
User Journey workflow engine
Data provider on behalf of the Data subject
Data
Public/Private Service
Data Controller Dashboard

Figure 3 ACROSS actors

2.2.1 CaPe workflow analysis

The CaPe workflow has been analysed taking into account the requirements and constraints imposed by the ACROSS User journey workflow engine, the current and (possibly) future authentication and authorization frameworks and the current implementation and deployment of both public and private services. The result of the analysis is presented in the next table.

Table 2 CAPE workflow vs ACROSS workflow

	CaPe	ACROSS
Service description and registration	CPSV-AP extended with personal data related data model: Purpose, processing, legal base.	CAPE extended with • Information about Personal data needed by the service, including optional data. • information about the REST service channel if available.
Service Linking	This "Service Linking" phase creates a one-to-many reference between the identification of the data subject at CaPe (**Account Id** and his/her	Not needed. Authentication provided by SSI and Personal Wallet technologies.

	identification at each service (**Surrogate Id**). The Service Linking phase is based on a process of identification, and possibly authentication of the data subject both at CaPe and at the service.	
Consent Request	End User is logged in the Service for which wants to consent data processing for a specific purpose. End user views the Consent Form dynamically generated by CaPe (by using the SDK) relying on the processing purpose and details (processing categories, legal basis, resource set, etc.) described during service description phase. Selects/deselects optional data and visualizes required data and policies for processing. End User gives the consent by submitting the Consent Form.	End User is logged in the ACROSS Personal data governance framework and selects a service. End user views the Consent Form dynamically generated relying on the processing purpose and details (processing categories, legal basis, resource set, etc.) described during service description phase. Selects/deselects optional data and visualizes required data and policies for processing. End User gives the consent by submitting the Consent Form.
Data Request, Notification and Activity Logs	Enforcement of an issued Consent Record can be accomplished by integrated Service by interacting with Cape SDK APIs, according to increasing steps of interaction with Cape capabilities and complexity: • Consent Enforcement • Usage Rules Enforcement with input Data Payload • Data Request	Check consent and consent enforcement only by the User Journey workflow engine before sending personal data to the public/private service.

	All notifications will be tracked by CaPe as Event Logs that can be viewed both by the Data Subject (via Use Self-Service dashboard) and by the Service Provider (via Data Controller dashboard)	All notifications will be tracked by the ACROSS data governance framework as Event Logs that can be viewed both by the Data Subject (via Use Self-Service dashboard) and by the Service Provider (via Data Controller dashboard)
Consent Management & User Data Usage Control	For each Consent End User can change the **Status** of the relative Consent: • **Activate**: enables the previously disabled Consent • **Disable**: disable the Consent • **Withdraw**: revoke the Consent, a new one must be given by the Consenting phase. ODRL based user **data usage control** to be implemented.	For each Consent End User can change the **Status** of the relative Consent: • **Activate**: enables the previously disabled Consent • **Disable**: disable the Consent • **Withdraw**: revoke the Consent, a new one must be given by the Consenting phase. **Data Usage Control**: to be implemented as an extension of the Data usage app integrated with the IDS connector. (See next section)

2.2.2 Conclusions from the analysis

CaPe provides most of the functionalities included by the MyData operator concept (See section 8.1.2) and provides data subjects with a simple way to grant and withdraw consent to the use or sharing of personal data within an ecosystem of inter or cross organizational digital services and check at any time: what data is shared, with whom, for what purpose and how they are processed. Besides, it supports public and private companies at every stage of the acquisition and consent management process.

The ACROSS personal data government framework strategy is to minimize the service providers adaptation needed to use the framework, assuming the responsibility of performing consent management and executing the consent enforcement before transferring the personal data to the service.

Therefore, some adaptation and extensions would be needed to adapt CAPE to ACROSS Data Governance Framework requirements and constraints, since It is currently not feasible to ask public and private services to adapt to CaPe by changing the way they work integrating the CaPe SDK/APIs.

Since CaPe is a modular product some modules could be adapted to be used by the ACROSS Personal data governance framework by providing a new API or relaxing some constraints, as for example the use of surrogateIDs created during the service linking phase.

The linking process that creates the surrogate ID is involved when services use different identity systems in order to identify in a unique manner a user among different services. As documented if a user is identified uniquely (SSI, eiDAS, or in future with digital wallet) surrogate ID would be used only as an internal identification of user.

The following CAPE modules are candidates to be adapted:

- **Account Manager**: Manage the lifecycle of the Cape user account.
- **Consent Manager**: Manage the Consent Records lifecycle, the generation of Consent Forms, etc.
- **Auditlog Manager**: Collects aggregated auditing statistics, triggered by incoming Event Logs (Consent, Data Processing) regarding a specific Account. This module could be extended to be used as the ACROSS Autidlog manager.
- **Service Registry**: Collects the Service Descriptions and registrations

3 Data usage control

3.1 IDS data usage control

The International Data Spaces (IDS) objective is to create data spaces where businesses can exchange and exploit data in a secure manner. For the IDS as well as other data driven businesses, data sovereignty is a key success factor. Data sovereignty has the goal to provide a Data Owner with full control over his data. This includes being able to control the usage of his data by the Data Consumer.

Data usage control offers possibilities to control future data usages beyond the initial access (also known as obligations). Usage control is an extension to traditional access control (See Figure 4). It is about the specification and enforcement of restrictions regulating what must (not) happen to data. Thus, usage control is concerned with requirements that pertain to data processing (obligations), rather than data access (provisions). Usage control is relevant in the context of intellectual property protection, compliance with regulations, and digital rights management.

On the one hand, companies may use usage control to prevent misuse of their own data, to protect their intellectual property, and to preserve the data value (intrinsic motivation). On the other hand, companies have to comply with legal obligations such as the European Union General Data Protection Regulation EU-GDPR (extrinsic motivation). Hence, companies have to prevent misuse of other persons or companies' data.

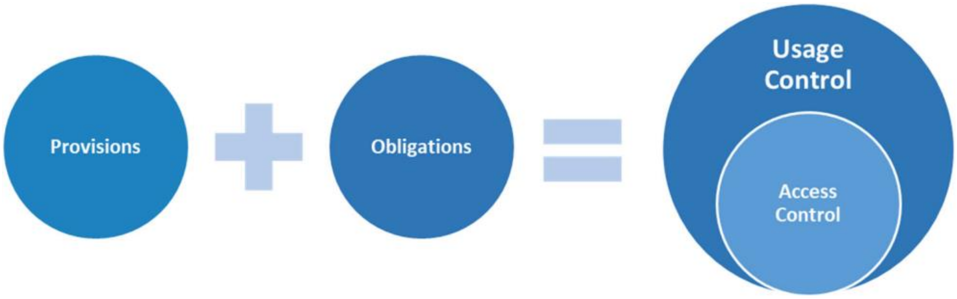


Figure 4 Usage Control consists of provisions and obligations

3.1.1.1 Usage Control

In contrast to access control, where access to specific resources (e.g., a service or a file) is restricted, the IDS architecture additionally supports data-centric usage control. In general, the overall goal is to enforce usage restrictions for data after access has been granted. Therefore, the purpose of usage control is to bind policies to data being exchanged and to continuously control the way how messages may be processed, aggregated, or forwarded to other endpoints. This data-centric perspective allows the user to continuously control data flows, rather than accesses to services. At configuration time, these policies support developers and administrators in setting up correct data flows.

At runtime, the usage control enforcement prevents IDS connectors from treating data in an undesired way, for example by forwarding personal data to public endpoints. Thus, usage control is both a tool for system integrators to ensure they are not building an architecture that violates security requirements, and an audit mechanism, which creates evidence of a compliant data usage.

3.1.2 Open-Source Data Usage Control module

The Data Usage Control module has been developed by modifying the open-source IDS Dataspace Connector[17]. Specifically, version v5.0.1 of the Dataspace Connector has been used as the starting point for the development, extracting the Java packages required for this module.

This code has been improved by adding the following new functionalities:

- REST services to get, upload and remove the Contract Agreements from the Contract Agreements storage. The format of these Contract Agreements is the one specified by the IDS Information Model[18]. These contracts are used to apply the Data Usage Control enforcement.
- A REST service to apply the Data Usage Control enforcement on the input data according to the Contract Agreements related to the pair consumer-producer indicated as input parameters.

The following figure shows the architecture of this module.

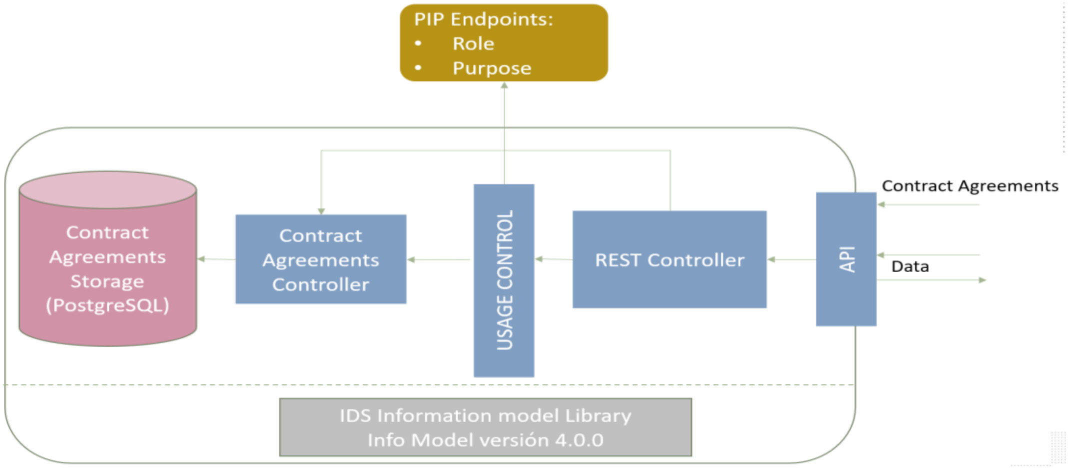
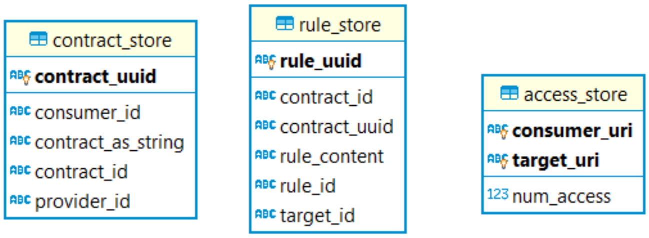


Figure 5 - Data Usage Control architecture

[17] https://github.com/International-Data-Spaces-Association/DataspaceConnector
[18] https://international-data-spaces-association.github.io/InformationModel/docs/index.html#

The Data Usage Control is composed of the following components:

- A PostgreSQL database, where the Constract Agreements are stored. This database contains the following tables:
    - **Contract_store:** the whole contract agreement content in JSON-LD format is stored in the "contract_as_string" column.
    - **Rule_store:** a contract may contain several rules. Each of these rules is stored in this table and the rule content in JSON-LD format is stored in the "rule_content" column.
    - **Access_store:** this table stores the number of times a consumer has accessed a specific target/data, in the "num_access" column. This table is used to apply the policy pattern "N Times Usage".



contract_store
contract_uuid
consumer_id
contract_as_string
contract_id
provider_id

rule_store
rule_uuid
contract_id
contract_uuid
rule_content
rule_id
target_id

access_store
consumer_uri
target_uri
num_access

Figure 6 - Data Usage Control database schema

- The Contract Agreement Controller, which implements the REST services to get, update and remove the Contract Agreements in the database.
- The Usage Control module, which applies the usage control enforcement over the input data according to the rules specified in the corresponding Contract Agreements.
- The REST Controller.

On the other hand, Policy Information Point (PIP) endpoints have been also developed to get the Role and Purpose of the data consumer. These PIP endpoints are only for testing purposes. The URL-s of these endpoints are specified in the Contract Agreements when the rule is referred to a Purpose/Role based permission/prohibition/obligation. Each consumer should implement its PIP endpoint, to inform about its Role or Purpose when consuming the data.

The steps to be taken to do enforcement are the following:

1. Once the consumer and provider connectors have negotiated and established a Contract Agreement, this Contract Agreement is stored in the Data Usage Control by invoking the corresponding REST service.
2. The usage control enforcement REST service is invoked before transferring the data from the Provider Connector to the Consumer Connector (parameter consuming=false), and before transferring the data from the Consumer Connector to the Data App (parameter

consuming=true). This service will return the data according to the policies defined in the Contract Agreement.

The data Usage Control module supports usage policies written in the IDS Usage Control Language[19] based on ODRL[20]. The policy patterns supported by the Data Usage Control module are the following ones:

- Allow the Usage of the Data: it provides data usage without any restrictions.
- Prohibit the Usage of the Data: it prohibits data usage.
- Interval-restricted Data Usage: provides data usage within a specified time interval.
- Duration-restricted Data Usage: allows data usage for a specified time period.
- Role-restricted Data Usage.
- Purpose-restricted Data Usage Policy.
- Restricted Number of Usages allows data usage for n times.

Depending on the input parameter “consuming” passed to the REST service in charge of doing the usage control enforcement, the policy patterns to be verified are:

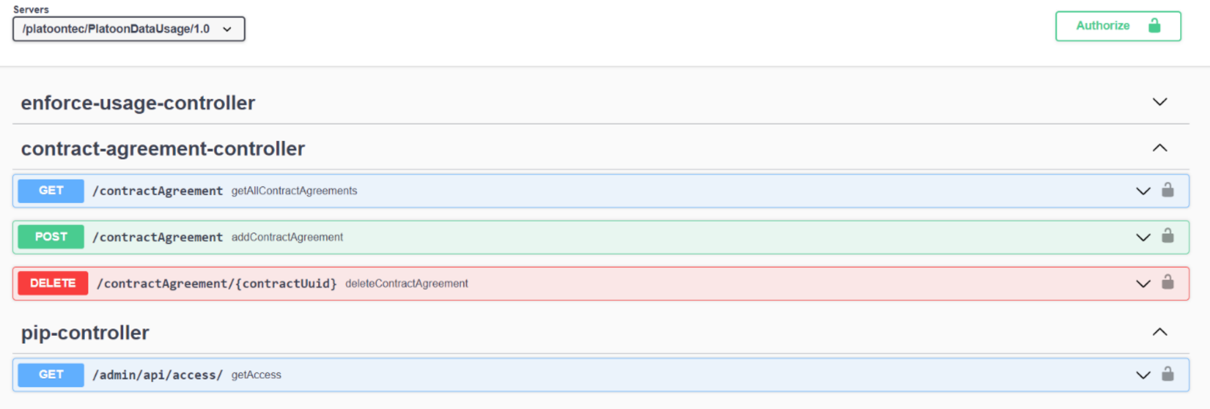
- Consuming=False. Providing data to another connector:
  - Allow the Usage of the Data
  - Prohibit the Usage of Data
  - Interval-restricted Data Usage
- Consuming=True. Consuming data:
  - Interval-restricted Data Usage
  - Duration-restricted Data Usage
  - Restricted Number of Usages
  - Role-restricted Data Usage
  - Purpose-restricted Data Usage

3.1.3 Data Usage Control APIs

Data Usage Control exposes a set of APIs which implement the functionalities of the Data Usage Control. Swagger-UI screenshots are reported below, in order to give an overview of each of the API parameters. The following figure shows a summary of the API-s offered by the UC module.

[19] https://internationaldataspaces.org/wp-content/uploads/IDSA-Position-Paper-Usage-Control-in-the-IDS-V3.0.pdf

[20] https://www.w3.org/TR/odrl-model/



Servers
/platoontec/PlatoonDataUsage/1.0

enforce-usage-controller

contract-agreement-controller

GET /contractAgreement getAllContractAgreements

POST /contractAgreement addContractAgreement

DELETE /contractAgreement/{contractUuid} deleteContractAgreement

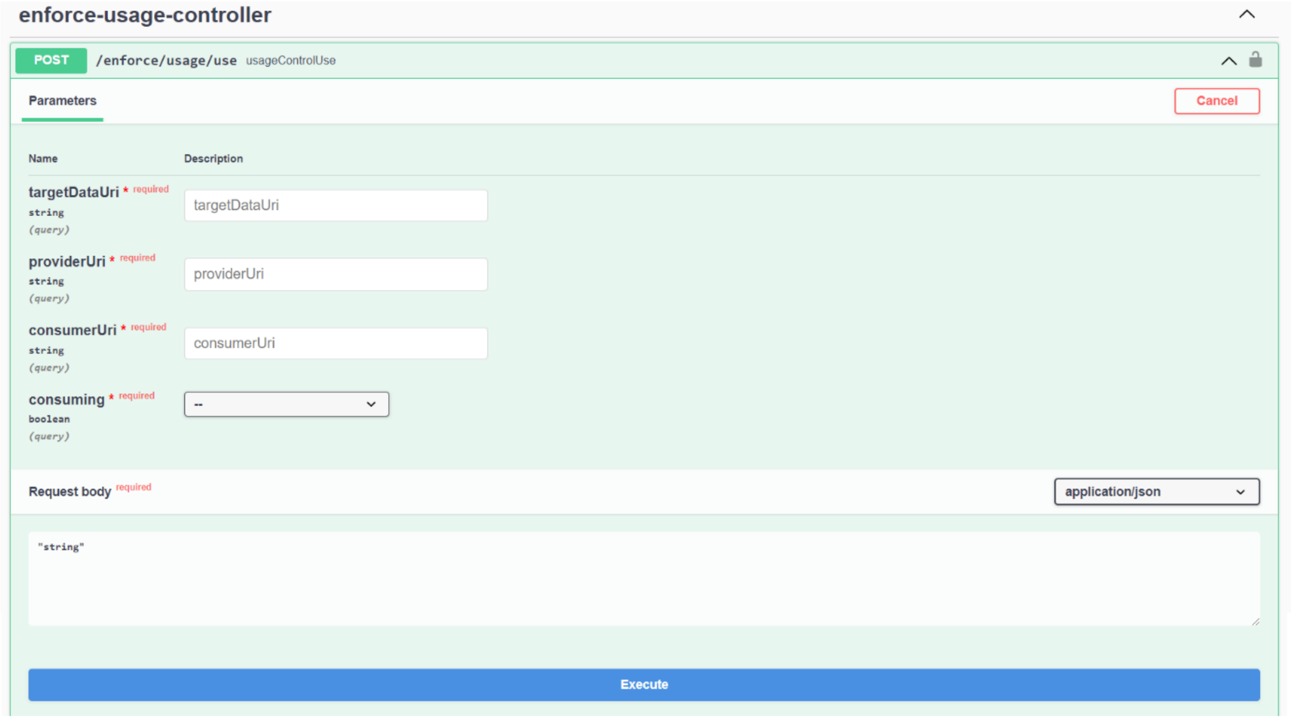
pip-controller

GET /admin/api/access/ getAccess

Figure 7 – Data Usage Control: summary of offered API-s

3.1.3.1 *Enforce usage rules*

This service applies the usage control enforcement on the input data according to the rules included in the Contract Agreement. The Contract Agreement applied will be the one that corresponds according to the input parameters provided to the service.



enforce-usage-controller

POST /enforce/usage/use usageControlUse

Parameters

Name	Description
targetDataUri * required string (query)	targetDataUri
providerUri * required string (query)	providerUri
consumerUri * required string (query)	consumerUri
consuming * required boolean (query)	--

Request body required — application/json

```
"string"
```

Figure 8 – Data Usage Control: Usage Rules Enforcement API

Mandatory parameters to do this service are:

- ***targetDataUri*:** Id of the dataset. E.g.: https://w3id.org/idsa/autogen/artifact/8e3a5056-1e46-42e1-a1c3-37aa08b2aedd .
- ***providerUri:*** Id of the Provider Connector. E.g.: https://w3id.org/idsa/autogen/baseConnector/7b934432-a85e-41c5-9f65-669219dde4ea .
- ***consumeruri:*** Id of the Consumer Connector. E.g.: https://w3id.org/idsa/autogen/baseConnector/7b934432-a85e-41c5-9f65-669219dde4ea .
- ***consuming:*** true/false. Boolean value which informs if the data is being provided by a Provider Connector (false) or if the data is being consumed at the Consumer Connector (true).

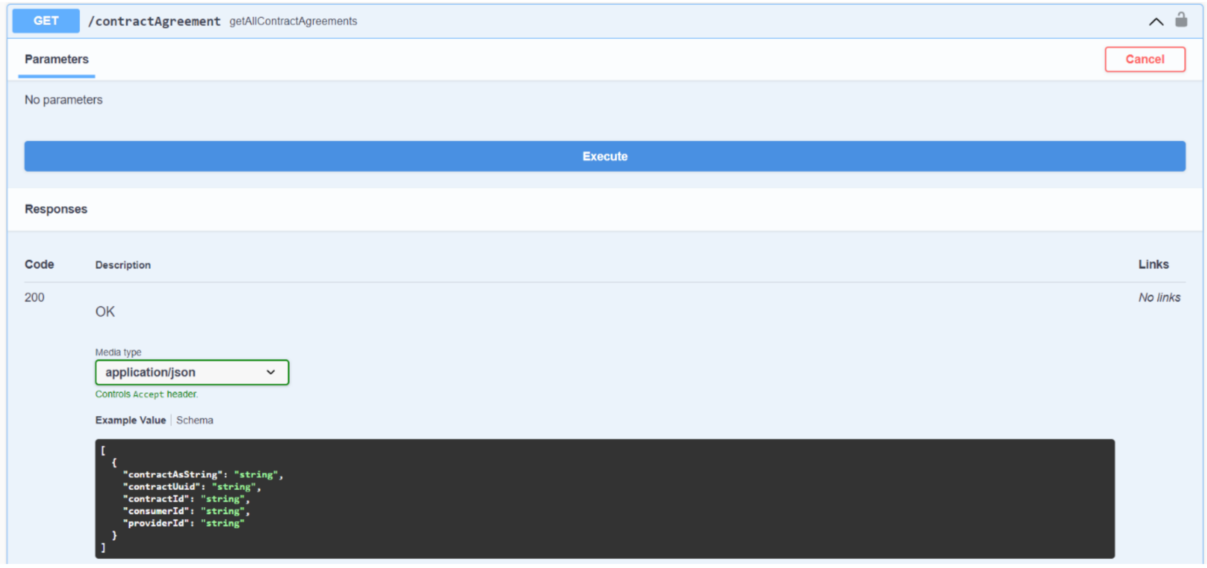
Request Body is also mandatory, and it will contain the data on which the usage rules defined in the Contract Agreement must be applied.

The following possible responses can be returned by this service:

- HTTP 200 OK: the response body will contain the data filtered according to the rules defined in the Contract Agreement and applied according to the input parameters provided.
- HTTP 403 Forbidden: this code will be returned when after applying the rules defined in the Contract Agreement, it concludes that data usage is not allowed.
- HTTP 400 Bad Request: this code will be returned when no valid Contract Agreements are found for the consumer/provider/target values provided as input parameters to the service.

3.1.3.2 Get All Contract Agreements

This service returns the Contract Agreements stored in the Data Usage Control database.



No parameters

200 OK — No links

```
[
  {
    "contractAsString": "string",
    "contractUuid": "string",
    "contractId": "string",
    "consumerId": "string",
    "providerId": "string"
  }
]
```

Figure 9 – Data Usage Control: Get Contract Agreements API

No input parameters are required.

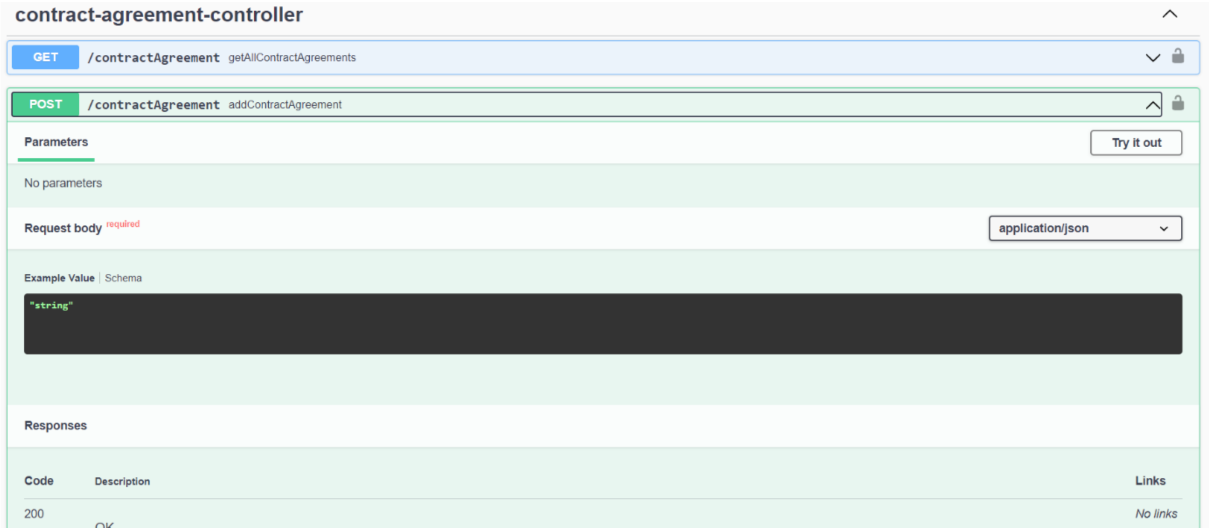
The following possible responses can be returned by this service:

- HTTP 200 OK: the response body will contain a JSON array with the Contract Agreements stored in the database. E.g.:

```
[
 {
   "contractAsString":
"{\"@context\":{\"ids\":\"https://w3id.org/idsa/core/\"},\"@type\":\"ids:ContractAgreement\",\"@id\":\"https://w3id.org/idsa/autogen/contractAgreement/contractAgree4\",\"ids:permission\":[{\"@type\":\"ids:Permission\",\"@id\":\"https://w3id.org/idsa/autogen/permission/perm4\",\"ids:target\":{\"@id\":\"https://w3id.org/idsa/autogen/artifact/4\"},\"ids:title\":[{\"@value\":\"Example Usage Policy N Times Usage\",\"@type\":\"http://www.w3.org/2001/XMLSchema#string\"}],\"ids:description\":[{\"@value\":\"n-times-usage\",\"@type\":\"http://www.w3.org/2001/XMLSchema#string\"}],\"ids:action\":[{\"@id\":\"idsc:USE\"}],\"ids:constraint\":[{\"@type\":\"ids:Constraint\",\"@id\":\"https://w3id.org/idsa/autogen/constraint/2030a8f2-f03d-4af9-bce5-b9222e129dce\",\"ids:rightOperand\":{\"@value\":\"5\",\"@type\":\"xsd:double\"},\"ids:operator\":{\"@id\":\"idsc:LTEQ\"},\"ids:leftOperand\":{\"@id\":\"idsc:COUNT\"},\"ids:pipEndpoint\":{\"@id\":\"http://localhost:8080/platoontec/PlatoonDataUsage/1.0/admin/api/access/\"}}]}],\"ids:provider\":{\"@id\":\"https://w3id.org/idsa/autogen/baseConnector/provider1\"},\"ids:consumer\":{\"@id\":\"https://w3id.org/idsa/autogen/baseConnector/consumer1\"},\"ids:contractDate\":{\"@value\":\"2021-02-18T10:15:21.137Z\",\"@type\":\"http://www.w3.org/2001/XMLSchema#dateTimeStamp\"},\"ids:contractStart\":{\"@value\":\"2021-02-18T10:15:21.137Z\",\"@type\":\"http://www.w3.org/2001/XMLSchema#dateTimeStamp\"}}",
   "contractUuid": "b7b88b8f-0f36-4b60-9479-c530204176cf",
   "contractId": "https://w3id.org/idsa/autogen/contractAgreement/contractAgree4",
   "consumerId": "https://w3id.org/idsa/autogen/baseConnector/consumer1",
    "providerId": "https://w3id.org/idsa/autogen/baseConnector/provider1"
  },
…
]
```

3.1.3.3 Insert/Update a Contract Agreement

This service is used to insert or update a Contract Agreement in the Data Usage Control database.



contract-agreement-controller

GET /contractAgreement getAllContractAgreements

POST /contractAgreement addContractAgreement

Parameters

Try it out

No parameters

Request body required

application/json

Example Value | Schema

```
"string"
```

Responses

Code	Description	Links
200	OK	No links

Figure 10 - Data Usage Control: Insert/Update Contract Agreement API

It does not require any input parameters.

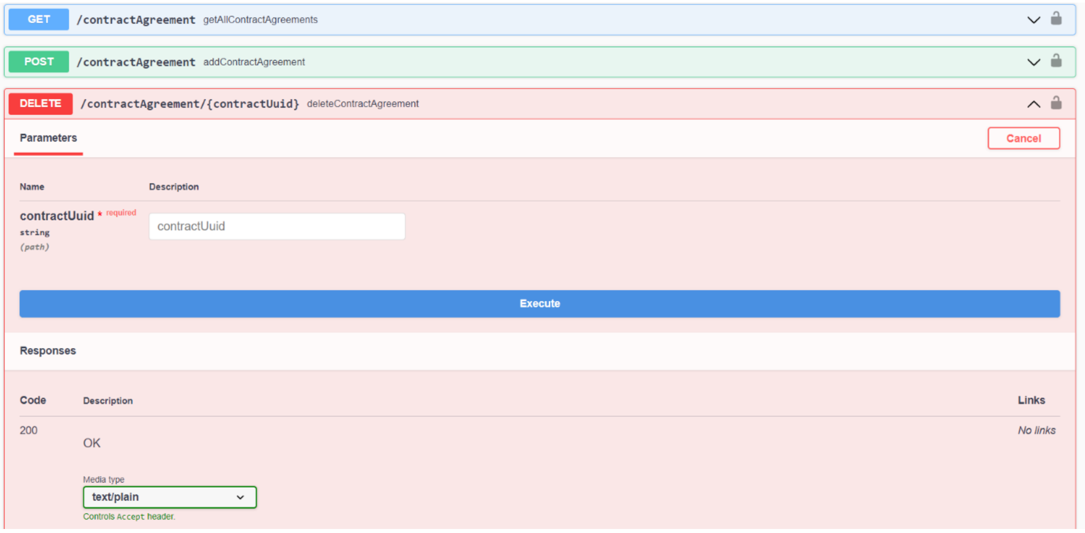
Request Body is mandatory, and it will contain the Contract Agreement to be inserted or updated in JSON-LD format. E.g.:

```
{
  "@context" : {
    "ids" : "https://w3id.org/idsa/core/",
          "idsc" : "https://w3id.org/idsa/code/"
  },
  "@type" : "ids:ContractAgreement",
  "@id" : "https://w3id.org/idsa/autogen/contractAgreement/52272512-dcbd-4b15-8f1f-f409327a4a9a",
  "ids:permission" : [ {
    "@type" : "ids:Permission",
    "@id" : "https://w3id.org/idsa/autogen/permission/59b0a20a-11bd-4276-8341-af40c8960e98",
    "ids:target" : {
      "@id" : "https://w3id.org/idsa/autogen/artifact/8e3a5056-1e46-42e1-a1c3-37aa08b2aedd"
    },
    "ids:title" : [ {
      "@value" : "Example Usage Policy",
      "@type" : "http://www.w3.org/2001/XMLSchema#string"
    } ],
    "ids:description" : [ {
      "@value" : "provide-access",
      "@type" : "http://www.w3.org/2001/XMLSchema#string"
    } ],
    "ids:action" : [ {
      "@id" : "idsc:USE"
    } ]
  } ],
  "ids:provider" : {
    "@id" : "https://w3id.org/idsa/autogen/baseConnector/7b934432-a85e-41c5-9f65-669219dde4ea"
  },
  "ids:consumer" : {
    "@id" : "https://w3id.org/idsa/autogen/baseConnector/7b934432-a85e-41c5-9f65-669219dde4ea"
  },
  "ids:contractDate" : {
    "@value" : "2021-02-18T10:15:21.137Z",
    "@type" : "http://www.w3.org/2001/XMLSchema#dateTimeStamp"
  },
  "ids:contractStart" : {
    "@value" : "2021-02-18T10:15:21.137Z",
    "@type" : "http://www.w3.org/2001/XMLSchema#dateTimeStamp"
  },
  "ids:contractEnd" : {
    "@value" : "2022-02-18T10:15:21.137Z",
    "@type" : "http://www.w3.org/2001/XMLSchema#dateTimeStamp"
  }
}
```

If everything works properly, it will create or update the Contract Agreement and return a HTTP 200 OK.

3.1.3.4 Delete a Contract Agreement

This service removes the specified Contract Agreement in the Data Usage Control database.



GET /contractAgreement getAllContractAgreements

POST /contractAgreement addContractAgreement

DELETE /contractAgreement/{contractUuid} deleteContractAgreement

Parameters

Name: contractUuid * required, string (path). Description: contractUuid

Responses

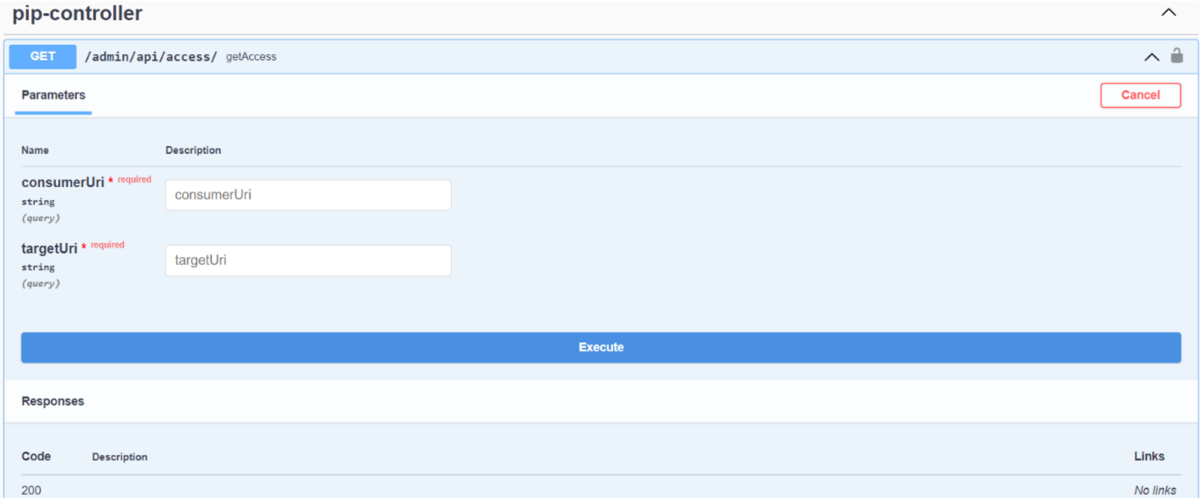
Code: 200. Description: OK. Media type: text/plain. Controls Accept header. Links: No links

Figure 11 – Data Usage Control: Delete Contract Agreement API

Mandatory path parameter is the contract unique identifier {contractUuid} of the Contract Agreement to remove from the database. If everything works properly, it will remove the specified Contract Agreement and return a HTTP 200 OK.

3.1.3.5 PIP endpoint to get number of times a data has been accessed at Consumer side

This service returns the number of times the specified data has been accessed by the specified Consumer Connector. This PIP endpoint is used to apply the "N Times Usage" rule, and its URL will appear in the rule definition.



pip-controller

GET /admin/api/access/ getAccess

Parameters

Name: consumerUri * required, string (query). Description: consumerUri

Name: targetUri * required, string (query). Description: targetUri

Responses

Code: 200. Links: No links

Figure 12 – Data Usage Control: PIP N Times access API

Mandatory parameters are:

- ***targetUri*****:** Id of the dataset. E.g.: https://w3id.org/idsa/autogen/artifact/8e3a5056-1e46-42e1-a1c3-37aa08b2aedd .
- ***consumeruri:*** Id of the Consumer Connector. E.g.: https://w3id.org/idsa/autogen/baseConnector/7b934432-a85e-41c5-9f65-669219dde4ea .

If everything works properly, it will return a number that specifies the number of times the specified data has been accessed by the specified Consumer Connector.

3.2 Data usage control in the ACROSS Personal Data Governance Framework

As already mentioned, the ACROSS personal data government framework strategy is to minimize the service providers adaptation needed to use the framework and it is not realistic to ask public and private services to use IDS connectors for data transfer. Therefore, the ACROSS Personal Data Governance Framework will assume the responsibility of performing data usage policies management and enforcement.

The User Journey Service Engine will call the framework before transferring the personal data to the service to enforce both personal data consents and data usage policies.

Since ACROSS is not going to use IDS connectors for data transfer, the data usage policies are applied only in the data provider side. Therefore, not real “data usage control” can be applied, only a restricted set of IDS policies providing data access rules. Furthermore, the contract negotiation phase is not needed.

In order to be used within the ACROSS data governance framework the Data usage app needs to be adapted by changing the contract format and API. Contracts in IDS represent agreements between companies exchanging data and are defined for specific “artifacts” or data sets. In ACROSS the contract represents agreements between end-users and public/private services for using personal data.

4 ABC framework: DECODE & IRMA

Attribute Based Credentials (ABC) are a form of authentication mechanism that allows to flexibly and selectively authenticate different attributes about an entity without revealing additional information about the entity (zero-knowledge property).

Attribute based credentials (ABCs) are a technology that could potentially be applied to enable privacy, granular control, and data minimisation in ACROSS. Put simply, ABCs are ‘a way to have a trusted party 'vouch' for you in a situation where you don’t want to give away any more information than is absolutely necessary’[21]. ABC is ‘a form of authentication mechanism that allows to flexibly and selectively authenticate different attributes about an entity without revealing additional information about the entity (zero-knowledge property).’

4.1 DECODE

DECODE[22] project aims at creating tools that will give people ownership of their data. These tools combine blockchain technology with attribute-based cryptography to give the data owner control of how their data is accessed and used.

Two pilots from the DECODE project were developed and tested in the Netherlands that make use of *attribute-based credentials* to help people have more control over the data they share.

With 'Claim Verification 18+', the City of Amsterdam prototyped a passport box and mobile web app that allow users to upload passport data from the RFID-chip (inside the physical passport) onto their phone. A physical box scans the passport’s chip, and then creates a QR code that the phone can scan using the DECODE web app. Once scanned, the app allows the user to share certain credentials without sharing personal data—as is the case in the example above, a user can generate and share a valid credential based on their passport data, proving they are over 18, for example, without sharing their actual age or date of birth. In addition to age, this proof of concept can also verify a person’s name and gender.

DECODE partners are working to enable their users to have granular control over the data they share on the site by integrating IRMA (a platform that supports the use of attribute-based credentials) into a website.

[21] https://waag.org/en/article/experimenting-attribute-based-credentials
[22] https://decodeproject.eu/

4.2 IRMA[23]

IRMA stands for *I Reveal My Attributes*. IRMA empowers the user to disclose online, via your mobile phone, certain attributes of yourself ("over 18"), but at the same time hide other attributes (like your name, or phone number). IRMA protects privacy in this way. This privacy-protection is intrinsic to the system, which is called *privacy by design*. In the most recent European data protection regulation such privacy by design is legally required for new ICT-systems.

IRMA is a set of free and open source software projects implementing the Idemix attribute-based credential scheme, allowing users to safely and securely authenticate themselves as privacy-preserving as the situation permits. Users receive digitally signed attributes from trusted issuer, storing them in their IRMA app, after which the user can selectively disclose attributes to others. Schematically:

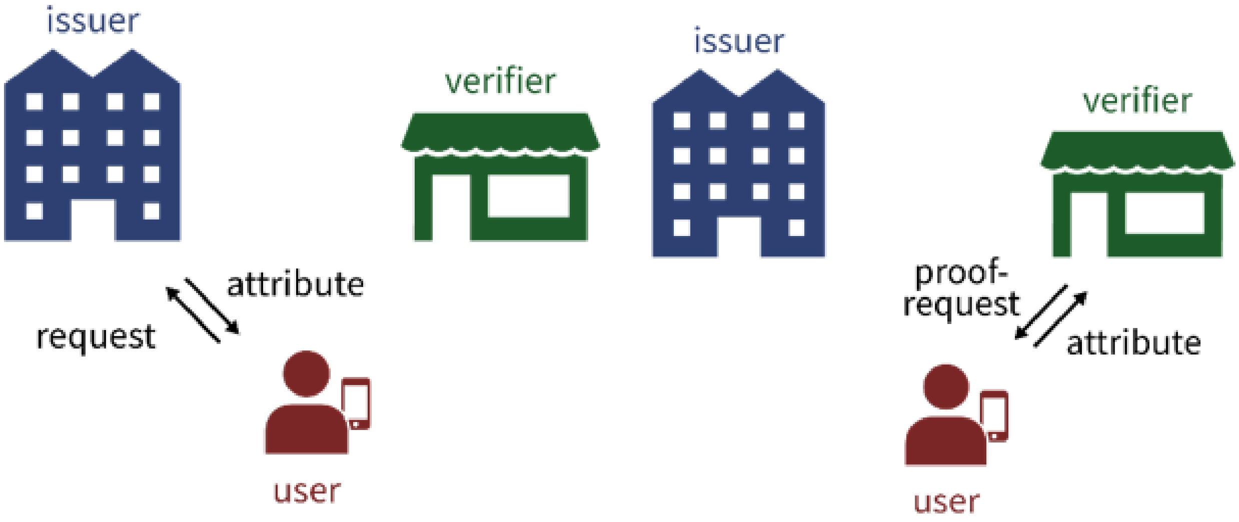


Figure 13 Issuing and verifying attributes with IRMA

Using the issuer's digital signature over the attributes the verifier can verify that the attributes were given to the user in the past, and that they have not been modified since.

[23] https://privacybydesign.foundation/irma-en

4.2.1 IRMA session flow

A typical IRMA session is depicted schematically below.

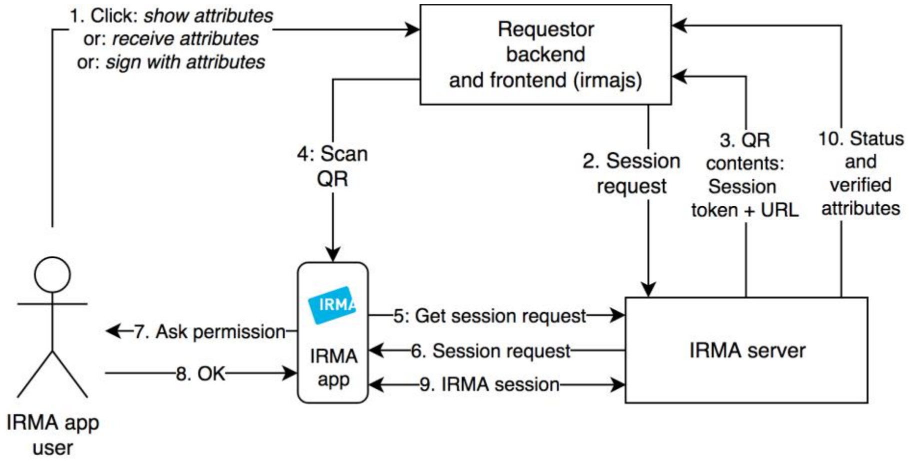


Figure 14 IRMA session flow and applications

In the session flow, three applications are involved:

- ***Requestor backend and frontend***: Generally, the requestor runs a website with a (JavaScript) frontend in the user's browser, and a backend server. During an IRMA session the frontend displays the IRMA QR that the IRMA app scans. All frontend tasks depicted in the diagram are supported by irma-frontend.
- ***IRMA server***: Handles IRMA protocol with the IRMA app for the requestor.
- ***IRMA mobile app***: Personal wallet (Android, iOS)

According to the IRMA documentation[24], this is the explanation of the steps:

1. Usually the **session starts by the user performing some action on the website** (e.g. clicking on "Log in with IRMA").
2. The requestor sends its session request (containing the attributes to be disclosed or issued, or message to be signed) to the IRMA server. Depending on its configuration, the IRMA server accepts the session request only if the session request is authentic from an authorized requestor.
3. The IRMA server accepts the request and assigns a session token (a random string) to it. It returns the contents of the QR code that the frontend must display: the URL to itself and the session token.
4. The IRMA frontend receives and displays the QR code, which is **scanned by the IRMA app**.

[24] https://irma.app/docs/what-is-irma/

5. The IRMA app requests the session request from step 1, receiving the attributes to be disclosed or issued, or message to be signed.
6. The IRMA server returns the session request.
7. The IRMA app displays the attributes to be disclosed or issued, or message to be signed, and asks the user if she wants to proceed.
8. **The user accepts.**
9. The IRMA server performs the IRMA protocol with the IRMA app, issuing new attributes to the user, or receiving and verifying attributes from the user's IRMA app, or receiving and verifying an attribute-based signature made by the user's app.
10. The session status (DONE, CANCELLED, TIMEOUT), along with disclosed and verified attributes or signature depending on the session type, are returned to the requestor.

4.3 Other alternatives from EU funded projects

There are several EU projects designing and implementing Personal wallet and ABC related technologies in different contexts. One of these projects is especially interesting for ACROSS since it pursues the same final objective.

The EU-funded mGov4EU[25] project aims to design, implement and evaluate an open ecosystem for secure mobile government services to be used across Europe and beyond.

The novel framework will take advantage of security features of modern smartphones (such as hardware-backed secure elements) and integrated convenience elements (such as biometric sensors) with the aim of meeting both the security needs and data-protection expectations placed on public services. Moreover, mGov4EU will address the usability issues that arise when accessing complex services via mobile devices.

One of the objectives of mGovEU is to design and implement a European personal wallet platform. ACROSS and mGovEU have started collaborating with the aim of analysing how to integrate the digital wallet that is being designed by mGovEU with the ACROSS platform and use cases.

[25] https://www.mgov4.eu/

4.4 Personal wallet integration with ACROSS Personal data governance framework and workflow engine.

To use the personal wallet authentication, attribute-based credentials data minimization, and personal data transfer functionalities the service providers should implement a specific credentials API and became verifiable credentials issuers and verifiers.

In the case of the Attribute Based Credentials technology, the support of the European Commission and its initiatives regarding Self Sovereign Identity and Blockchain makes Personal wallet one of the most promising technologies for the future.

Two approaches for using the personal wallet have been identified:

The first ACROSS approach regarding the integration of a personal wallet as the secure storage for the end user is depicted in the next figure. ACROSS plays the role of trusted intermediary between the personal wallet and the services, both issuers and verifiers, interacting with the personal wallet, getting the credentials from the issuers and sending the credentials to the services.

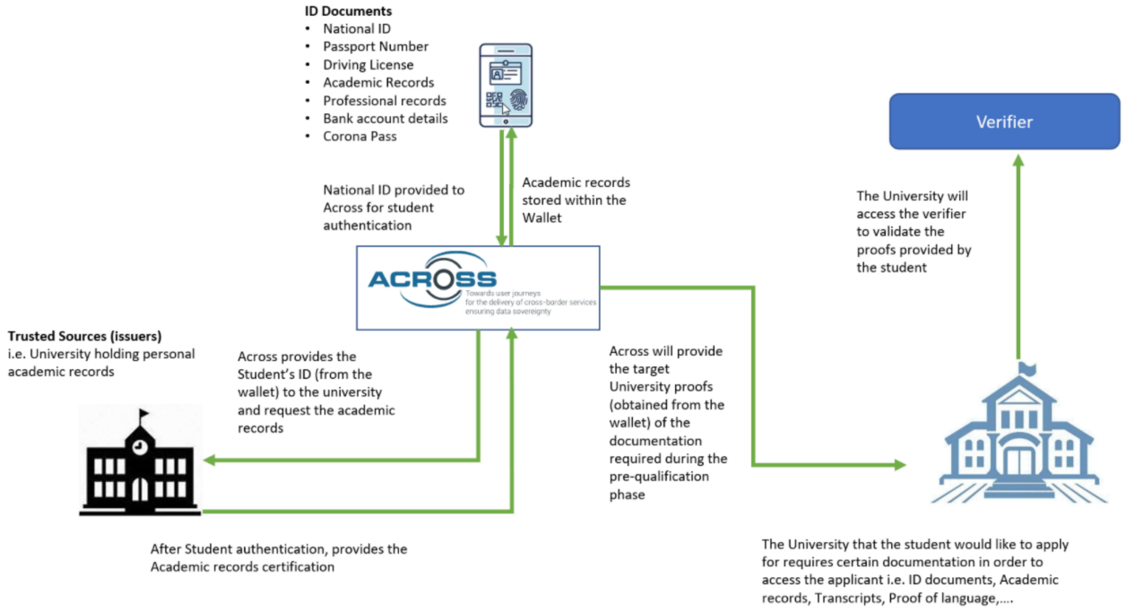

ID Documents
National ID
Passport Number
Driving License
Academic Records
Professional records
Bank account details
Corona Pass
Verifier
National ID provided to Across for student authentication
Academic records stored within the Wallet
The University will access the verifier to validate the proofs provided by the student
ACROSS
Towards user journeys for the delivery of cross-border services ensuring data sovereignty
Trusted Sources (issuers)
i.e. University holding personal academic records
Across provides the Student's ID (from the wallet) to the university and request the academic records
Across will provide the target University proofs (obtained from the wallet) of the documentation required during the pre-qualification phase
After Student authentication, provides the Academic records certification
The University that the student would like to apply for requires certain documentation in order to access the applicant i.e. ID documents, Academic records, Transcripts, Proof of language,....

Figure 15 ACROSS approach for the personal wallet

Another approach is implementing the personal wallet based data transfer to service providers as another channel to interact with a service, provided that the service is integrated with the personal wallet workflow and implements its protocol.

In this case the user journey workflow engine should ask the user to perform all que steps in the personal wallet workflow, e.g. starting the IRMA session, reading the QR code, and accepting the disclosure of the attributes.

This approach can be valid for any other Personal wallet implementation.

5 ACROSS Personal data governance framework implementation

5.1 ACROSS Personal data governance framework Architecture

The ACROSS Personal Data Governance Framework is part of the so-called ACROSS platform, useful in the context of cross-border public/private services for the citizens. However, it has been designed to be an independent framework useful also for the individuals to manage their personal data according to the GDPR in any other context. Furthermore, it will extend the MyData operator concept with Data usage policies enforcement and data minimization techniques will be also integrated.

The following figure provides the overall view of the main components of the Data Governance Framework as an independent framework.

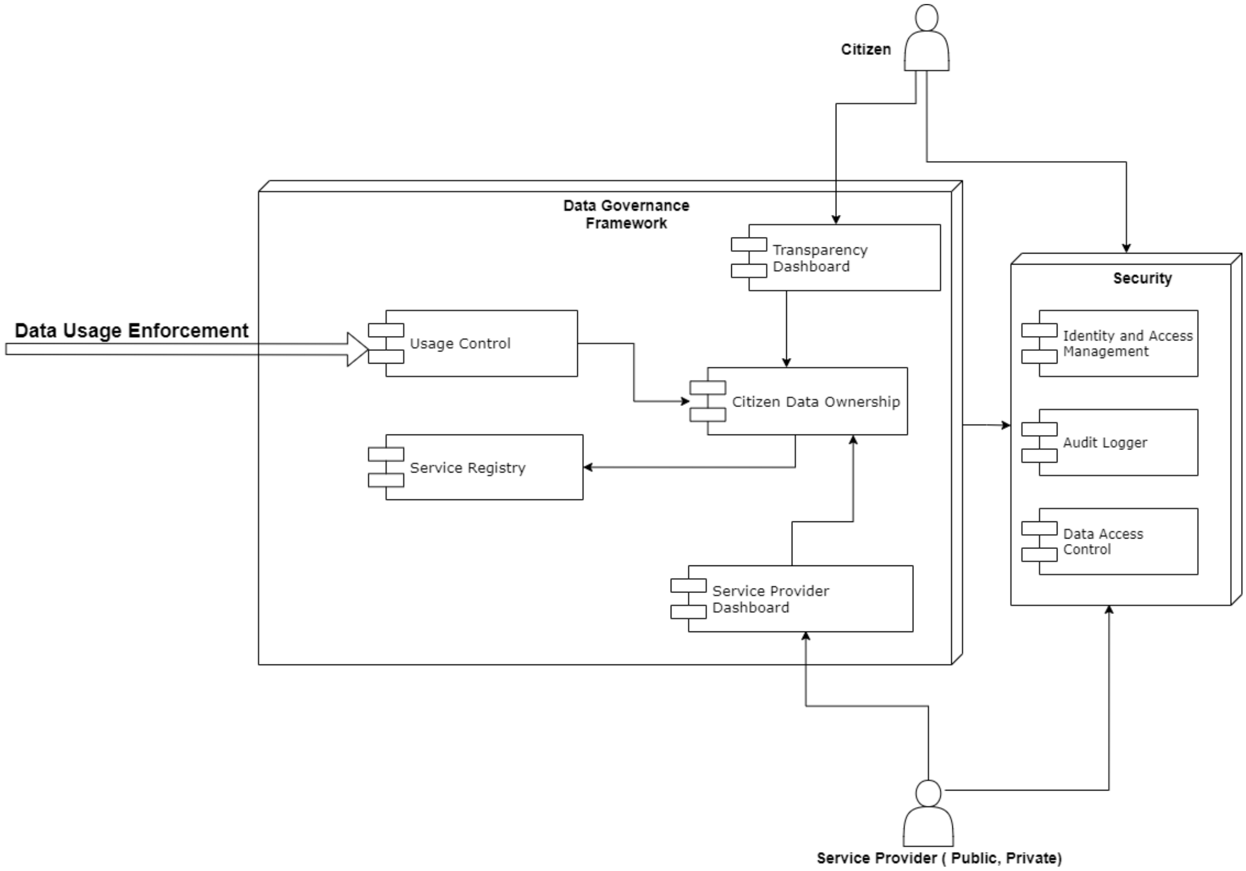


Figure 16 Component View of Data Governance Framework

The Data Governance Framework will allow citizens / users to register in a series of services (Service Registry) and allow the use of their data based on consents that should be approved by them. To carry out this transfer of information in a secure way, the Usage Control module will be used. This module will be able to check the legal base of a service to use personal data and will allow the usage of data based on previously defined usage policies.

The components in the Security layer will be used by all the components in the Data Governance Framework. This layer provides all the security features needed for a citizen and a service provider to be authenticated and authorized, and for logging all the interactions among all components of the framework.

Next figure shows the integrated view of the whole ACROSS platform, including the interaction between the User Journey Services Engine and the ACROSS Personal Data framework with the Usage Control module.

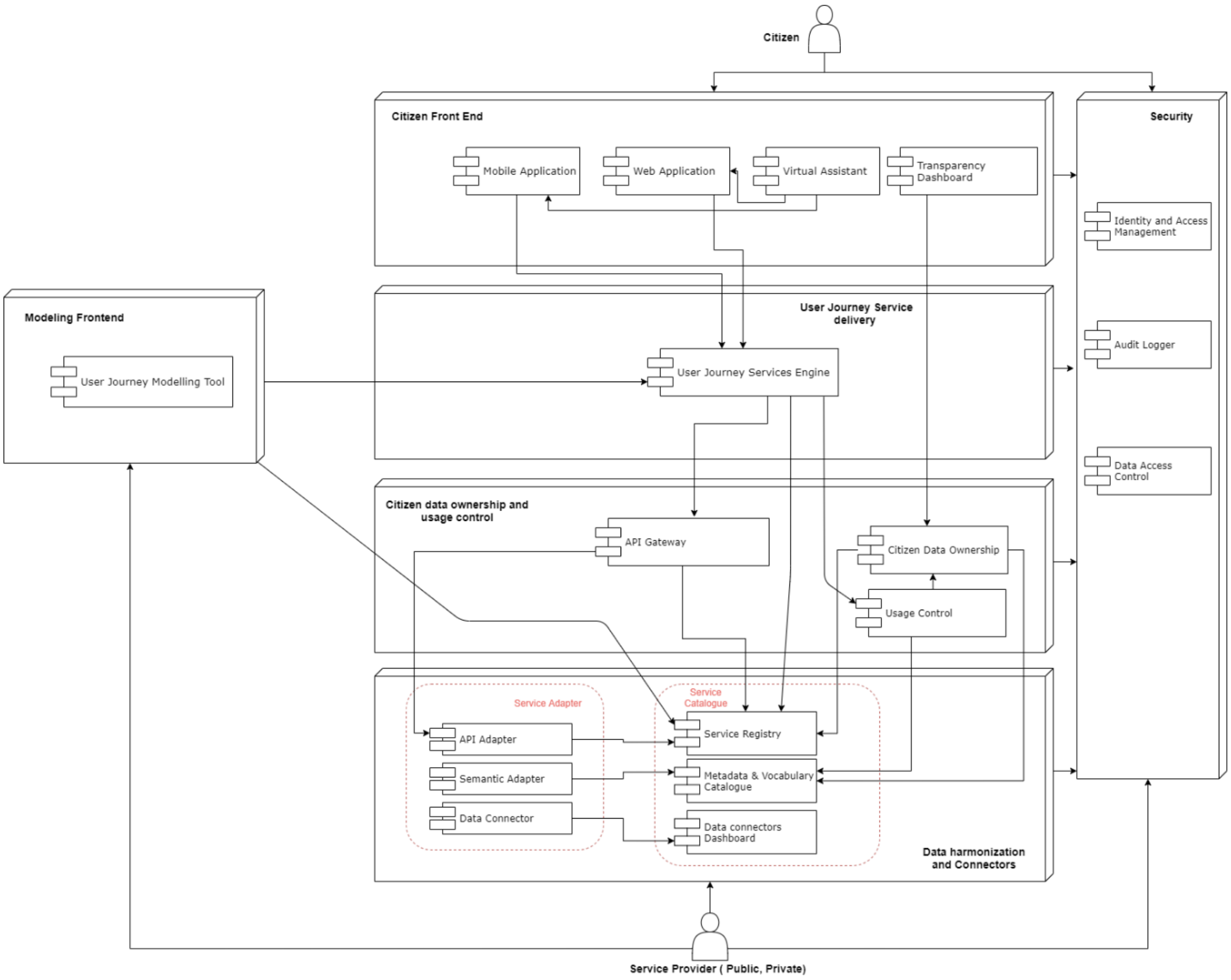


Figure 17 ACROSS platform architecture integrated view

5.1.1 Citizen Data Ownership

This component allows the citizens to manage their personal data and allows the organizations/services to fulfil the requirements in line with the GDPR. It will expose several interfaces for the Transparency Dashboard, so that the individuals can grant and withdraw their consents, manage data usage policies and receive notifications about how their data is being used.

5.1.2 Usage Control

This component provides the enforcement mechanism to apply usage policies according to previously defined consents. The available formats of data usage policies include GDPR consents and IDS data policies enforcement. On the other hand, it will expose several interfaces for the services, so that they can be informed about the consents of the citizens, and they can send notifications about the data that is being used.

5.1.3 Service Registry

This component provides human and machine-readable description of services that will be available in ACROSS platform for user journey services provisioning. The registry enables the storage and publishing of service by providing general, technical and data processing information based on standard models (e.g. ISA[2]).

The component provides the following functionalities:

- Publishing, searching, and retrieving of an already available service in the platform
- Service Description versioning
- API for programmatically interaction with the registry

5.1.4 Transparency Dashboard

This module is a web application that uses a human centric approach to liberate the potential of personal data and to facilitate its controlled flow from multiple data sources to applications and services. Citizens must be able to opt-in and out from the use of their personal data, in line with the requirements of the GDPR. The main objective is to give the individual control of their own data.

The component provides the following functionalities:

- Monitor which data are available and how they are used or how it can be accessed. It provides individual's linked services, and data use related policies and consents.
- Notify users about realised data processing at services.
- Give users control over their data allowing them to add as well as delete or modify information.

5.1.5 Service Provider Dashboard

This module is a web application that allows the service providers to:

- manage the Semantic Descriptions and registrations of its own provided Services, so that it is available for the citizens through the Transparency Dashboard.
- view and manage the Consents status given by all the Users of its registered services.

5.1.6 APIs

5.1.6.1 Citizen Data Ownership

The Citizen Data Ownership module will expose the following interfaces:

- SearchConsent: Search consents by different criteria.
- ModifyConsent: Modify consent status (e.g.: withdraw), enable or disable specific data to which consent applies, change organizations to which data is shared.
- ViewLogs: Show information about the events that have happened related to the linked services and the consents given/withdrawn.
- SearchServices: Search services by different criteria.
- LinkUserToService: Link a user to a service, so that he can manage the consents given to that service.

5.1.6.2 Usage Control

The Citizen Data Ownership module will expose the following interface:

- UsageControlEnforcement: Apply usage policies and enforce personal data consents so that data is used accordingly.

5.1.6.3 Service registry

The Service Registry module will expose the following interfaces:

- Store/delete: Storing or delete a service description.
- Search: Search a service description according to several metadata in accordance to the adopted service model.
- Publish: The service description is active and available and searchable.

5.2 ACROSS Personal data governance framework initial version mock-up

This section includes the specification and design of a first version of the ACROSS Personal Data Management Framework covering the basic set of functionalities, the so-called minimum viable product. This initial version will be extended along the project to produce the final implementation of the ACROSS Data Governance framework for data sovereignty.

This version of the ACROSS personal data governance framework will be implemented from scratch, without using the base technologies identified.

The next figure shows the scenario and steps covered by this first version. The numbers in **red** corresponds to the steps in the CaPe workflow:

1. **Service description and registration**
2. Service Linking → This step is not needed in ACROSS.
3. **Consent Request**
4. Data Request, Notification and Activity Logs. **Consent enforcement**
5. **Consent Management** & User Data Usage Control

Keycloak will be used for Identity and Access Management instead of the SSI Authentication included in the figure.

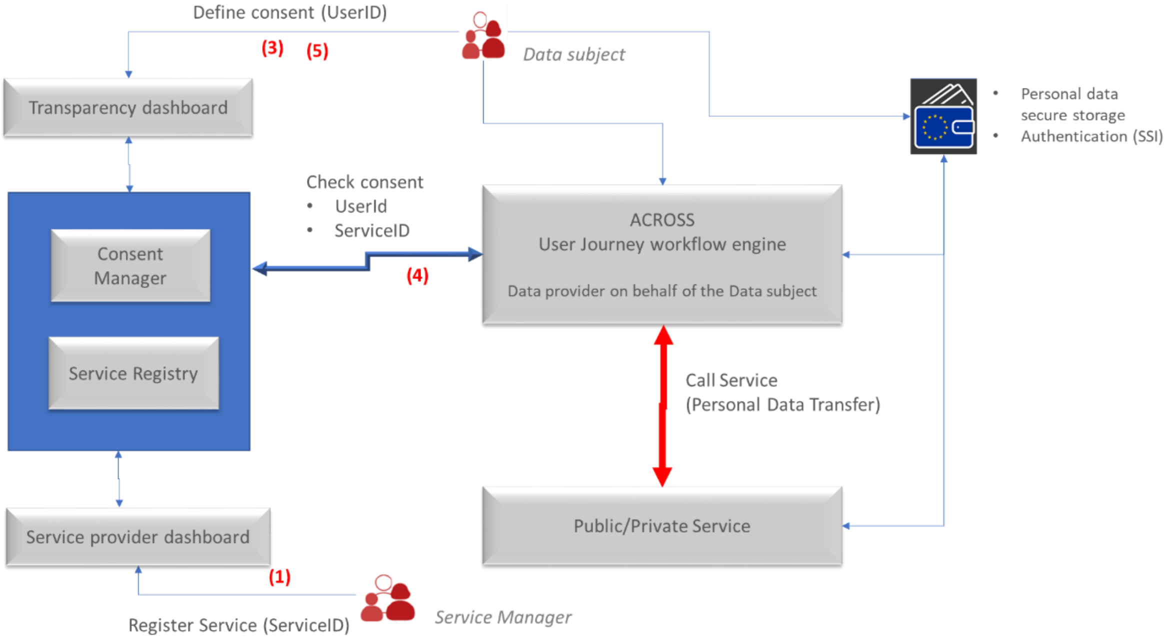


Figure 18 ACROSS Personal data governance framework scenario

Next, the ACROSS Personal data governance framework requirements are presented along with the description of the functionalities to be included in the first version.

5.2.1 Users management

The data Governance Framework must allow an end user to create a new account or to remove it. The first time a user enters the framework, the end user will have the opportunity to create an account in the framework. At least three types of user are envisaged: Administrator, End User (Citizen) and Service provider.

The basic database structure needed to store the information about users will be implemented. However, the front-end will not be covered in the first version.

5.2.2 Personal Data catalogue management

When defining a new Service, apart from providing its description, the description of the type and structure of the set of personal data processed by the Service must be also provided. Each dataset will be associated to a specific use purpose and specific processing ways e.g.:

- Dataset A contains: Name, Last name, gender, nationality.
- Dataset B contains: Gender, date of birth, nationality, address, phone.

Each of these datasets is used by the service for a specific purpose, is shared with specific organizations and is processed in a specific way. However, the definition of the data sets used by different services could use different models.

In order to homogenise the personal data models, the ACROSS Personal Data Framework will implement a Data catalogue functionality to provide a common way to describe personal data. The data model will be based on DPV Personal Data Category[26] taxonomy and classes.

DPV provides broad top-level personal data categories adapted from the taxonomy contributed by EnterPrivacy[27]. The top-level concepts in this taxonomy refer to the nature of information (financial, social, tracking) and to its inherent source (internal, external). Each top-level concept is represented in the DPV vocabulary as a Class and is further elaborated by subclasses for referring to specific categories of information - such as preferences or demographics.

[26] https://w3c.github.io/dpv/dpv/#vocab-personal-data-categories

[27] https://enterprivacy.com/wp-content/uploads/2018/09/Categories-of-Personal-Information.pdf

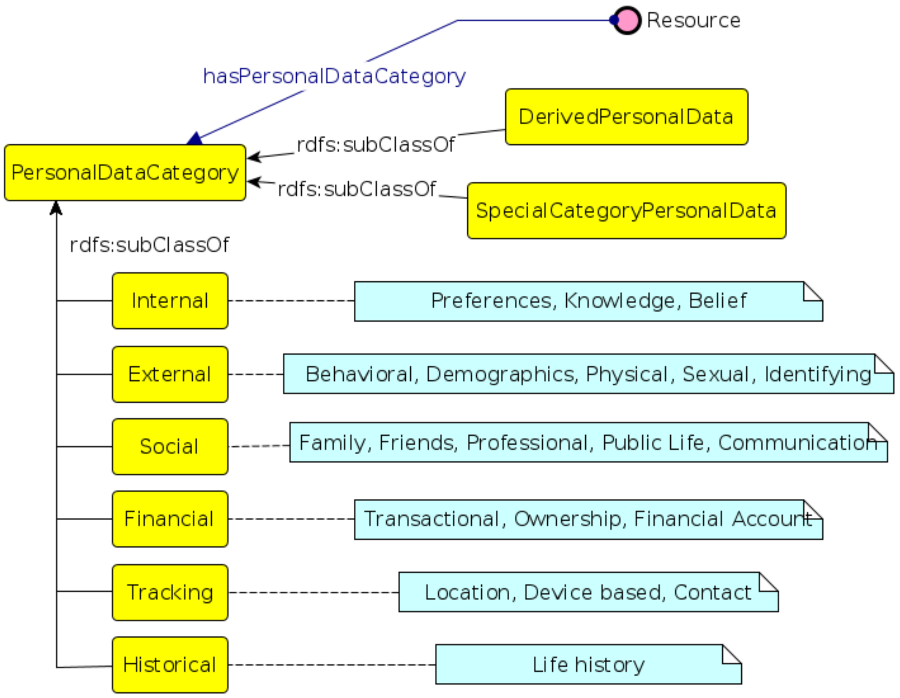

Resource
hasPersonalDataCategory
DerivedPersonalData
rdfs:subClassOf
PersonalDataCategory
rdfs:subClassOf
SpecialCategoryPersonalData
rdfs:subClassOf
Internal
Preferences, Knowledge, Belief
External
Behavioral, Demographics, Physical, Sexual, Identifying
Social
Family, Friends, Professional, Public Life, Communication
Financial
Transactional, Ownership, Financial Account
Tracking
Location, Device based, Contact
Historical
Life history

Figure 19 DPV taxonomy for personal data28

The framework will give the service provider a way to map its specific data model with the DPV Personal Data Categories data model. In this way, it would be possible to have a vision of where each type of data is being used in different services.

The model will be implemented but the frontend to define the mapping and the frontend for the end user are not included.

5.2.3 Service management

A service provider will be able to:

- Create and Edit all descriptions of Services that will be integrated with the framework, according to the Service Description Data Model defined
- Get an overview and manage the lifecycle of Services Descriptions (Create, Import, Export, Register, DeRegister, Delete and so on).
- Get an overview and details of the Consents that End Users have given at corresponding registered Services, in particular:

[28] https://enterprivacy.com/wp-content/uploads/2018/09/Categories-of-Personal-Information.pdf

    - Processing and Purpose details.
    - Consents history.
    - Consents raw data (JSON).

In this first implementation only the registration of a new service by importing a JSON file will be available.

5.2.4 Service consent management

The end user will be able to:

- Get an overview of his personal data being processed by the Services he is linked to.
- Get an overview of previously registered Services by Service Providers, and ready to be linked to his account, and of already linked Services.
- Link his account to an available Service.
- Disabling a linked Service. This will put all its active Consents (if any) in Disabled state
- Get an overview of given or pending Consents, where the following information will be provided:
    - Processed personal data
    - With which Organization data can be shared
    - Other info
- Manage the lifecycle of given Consents by changing its status:
    - Disable: disable the Consent
    - Activate: enables the previously disabled Consent or pending Consent.
    - Withdraw: revoke the Consent, a new one must be given.

  The aforementioned actions will involve the creation/modification/removal of the policy rules that will describe how the personal data should be used by the service.

- Enable or disable each single Data Concept contained in the Resource Set regulated by that Consent (e.g.: his age). This action will involve the modification of the corresponding data usage control policy rule.

In this first implementation only the registration of a new consent by importing a JSON file will be available.

5.2.5 External APIs

The framework will expose a set of APIs to be used by the Data provider that are going to be integrated in the framework. This API will allow the data provider to check the service linking status, the consents associated to end users and to inform the framework the usage of personal data.

In ACROSS, the data provider will be the ACROSS user journey workflow engine.

Only the checkConsent (UserID, ServiceID) functionality will be included and the result will be just yes/no answer.

This functionality is a first version of the UsageControlEnforcement API that allows to apply usage policies and enforce personal data consents so that data is used accordingly.

6 Conclusions and next steps

This report includes the analysis of the applicability of a concrete set of technologies/products:

1. **MyData model for human-centered personal data management and processing**: CaPe open source implementation of the MyData Operator concept.
2. **Attribute-Based Credentials techniques**: DECODE project and IRMA.
3. **IDSA data sovereignty concept and *data usage policies* enforcement**: Data usage application implementation by TECNALIA.

One of the main conclusions of the analysis is that, in order to use the three technologies, the public and private services involved in the workflows have to be adapted.

- In order to interact with CaPe the service providers should implement the CaPe SDK/APIs infrastructure.
- To make use of the full functionality of IDS data usage control, IDS connectors must be used both by the ACROSS User Journey Service Engine and by the public/private services.
- To use the personal wallet authentication, attribute-based credentials data minimization, and personal data transfer functionalities the service providers should implement a specific credentials API and became verifiable credentials issuers and verifiers.

However, the ACROSS personal data government framework strategy is to minimize the service providers adaptation needed to use the framework since it is not realistic to ask public and private services to use IDS connectors for data transfer or to adapt their current implementations to CaPe. Therefore, only the User Journey Services Engine will interact with the ACROSS Personal Data Governance framework before transferring the personal data to the public/private services.

Resulting from this analysis, some extensions or adaptations have been identified.

- Data Usage Control will be implemented as an adaptation of the Data usage app integrated with the IDS connector but with very limited functionality since ACROSS will not use IDS connectors for data transfer. Only a small set of data access rules will be applied.
- Some CaPe modules could be adapted to be used by the ACROSS Personal data governance framework by providing a new API or relaxing some constraints.

In the case of the Attribute Based Credentials technology, the support of the European Commission and its initiatives regarding Self Sovereign Identity and Blockchain makes Personal wallet one of the most promising technologies for the future. Two approaches for using the personal wallet have been identified:

Define ACROSS as a trusted intermediary between the personal wallet and the services or to define a new channel for interacting with the services, like using a web page or email.

Finally, the document includes the specification and design of a first version of the ACROSS Personal Data Management Framework covering the basic set of functionalities, the so-called minimum viable product. It will not include the data usage control functionality nor the personal wallet integration.

This version of the ACROSS personal data governance framework will be implemented from scratch, without using the base technologies identified. This initial version will be extended along the project to produce the final implementation of the ACROSS Data Governance framework for data sovereignty.

7 References

[1] Data governance act: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

[3] Understanding MyData Operators https://mydata.org/wp-content/uploads/sites/5/2020/04/Understanding-Mydata-Operators-pages.pdf

[4] TechDispatch #3/2020 - Personal Information Management Systems, 6 January 2021, from the European Data Protection Supervisor; see https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-32020-personal-information_en

[5] Opinion 9/2016 - EDPS Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data; see https://edps.europa.eu/sites/default/files/publication/16-10-20_pims_opinion_en.pdf

[6] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

8 Annex I: Across Baseline Technologies

This section contains information about three baseline technologies and its applicability in the context of the Personal Data Governance Framework:

- MyData operator
- Attribute Based Credentials (ABC)
- IDS Data usage control

The information about the technologies in this section has been gathered from the original sources.

8.1 MyData

8.1.1 ACROSS project and/or pilots as MyData operators

A Mydata operator can be an organization that manages and utilizes open data, develops APIs and communicates with other organizations that also create and use data and APIs for their own operation. It can also exchange data with them as well as with individuals. To achieve this in a simple and sustainable way a Mydata operator must:

- Create and maintain the Data Standards and enforce that application and data source developers comply with them.
- Provide documentation for the API that grants access to the data.
- Develop login portals for the developers and the end users, using secure authentication and authorization protocols.

Data source developers maintain the data source and register it via the developer portal.

Application developers can then find the registered data sources and explore the given options in the API documentation.

End users can access the online applications, where they receive authorization to access the data.

MyData specification does not cover all the functionality included in the ACROSS Personal data governance framework:

- Data usage policies definition and enforcement
- Attribute based credentials to comply with data minimization principle
- Some of the GDPR user rights are not included in MyData strategy.

8.1.2 MyData operator

MyData Operators Thematic Group which is part of the MyData Global organisation has produced the whitepaper "Understanding MyData Operators" [3] which focuses on practical aspects of technology and governance to make the operation of infrastructures for personal data easier and more human-centric, with the goal of establishing full interoperability between operators.

According to the whitepaper, a MyData operator is an actor that provides infrastructure for human-centric personal data management and governance. In the paper the initial minimum requirements to be considered a MyData operator are presented.

One of the central ideas of the MyData operator model is that there will be a large number of actors providing personal data management services, and that those services should be interoperable and substitutable as well as technology agnostic as far as possible.

In the paper, four dimensions of the MyData Operator concept are considered:

- **Reference model**: The MyData operator reference model provides a structure within which to analyse operators' offerings and characterise their **functional elements**. The reference model creates a baseline for expectations for an operator from individuals, other operators, and other actors in the ecosystem.
- **Interoperability**: Interoperability is key to realising the many benefits of the MyData vision. The paper describes different aspects of interoperability, indicating the role that MyData can play in enhancing human-centric interoperability as ecosystems mature.
- **Governance**: The governance of human-centric data sharing ecosystems is discussed in the contexts of legal and voluntary frameworks. The paper considers how governance should be formulated and enacted, taking into account transparency, the responsibilities of operators towards individuals, and how the nature of who controls an operator impacts this relationship.
- **Business models:** The paper studies parameters of the business models options available to and currently used by some proto-operators, covering fundamental design criteria from the perspectives of human-centricity and financial sustainability.

The purpose of this section is to describe the functional requirements covered by a MyData operator comparing them with the ACROSS Personal Data Governance framework requirements.

The MyData operator reference model describes nine core functional elements of operators. These elements affect how easy it is to utilise personal data, how transparent and human-centric the utilisation of personal data is, and how well the infrastructure supports open competition.

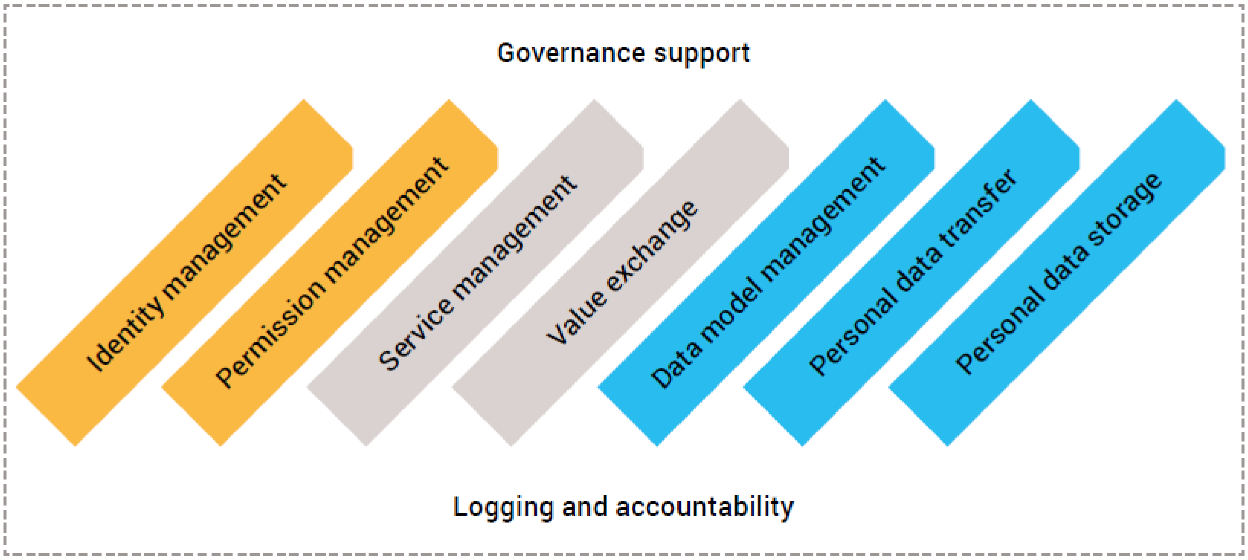


Figure 20 Functional elements of a MyData operator.

The first two (yellow) pillars mediate data transactions in terms of participants and permissions.

The middle two (grey) pillars describe what services are enabled in the ecosystem and how value can be exchanged between ecosystem participants.

The right-hand three (blue) pillars manage data, its meaning, its exchange, and its storage.

‘Governance support’ and ‘Logging and accountability’ provide context for the other functional elements and are critical for transparency and trust in the ecosystem.

Next, more information about the pillars are included along with a first mapping with the functional modules of the ACROSS personal data governance framework.

Identity management handles authentication and authorisation of individuals and organisations in different, linked identity domains and links identities to permissions. This module is also included in the ACROSS data governance framework and it is a common module used also by the ACROSS platform.

Permission management enables people to manage and have an overview of data transactions and connections and to execute their legal rights. It includes maintaining records (notices, consents, permissions, mandates, legal bases, purposes, preferences etc.) on data exchange. This is one of main ACROSS data governance framework modules along with the Service management and the Data model management module. The users of this module are the individuals in charge of managing their own personal data records.

Service management uses connection and relationship management tools to link operators, data sources, and data using services. Data can be available from different sources and can be used by multiple data using services.

Value exchange facilitates accounting and capturing value (monetary or other forms of credits or reputation) created in the exchange of data. The value exchange functionality is not within the scope of ACROSS.

Data model management is about managing the semantics (meaning) of data, including conversion from one data model to another. ACROSS data governance framework will use a "personal data model" to classify the personal data and to link the user permissions to the specific personal data categories.

Personal data transfer implements the interfaces (e.g. APIs) to enable data exchange between the ecosystem participants in a standardised and secure manner. This functionality is not covered by the ACROSS data governance framework, but it will be provided by the ACROSS platform to transfer data from the personal data storage to the Public/private services included in the defined user journeys.

Personal data storage allows data to be integrated from multiple sources (including data created by a person) in personal data storage (PDS) under the individuals' control. The personal data storage is an important functionality, but in ACROSS we will rely on existing solutions.

Governance support enables compliance with the underlying governance frameworks to establish trustworthy relationships between individuals and organisations.

Logging and accountability entails keeping track of all information exchanges taking place and creating transparency about who accessed what and when. ACROSS also provides this functionality.

Next a more detailed analysis about the two main functional elements and their implementation in the ACROSS data governance framework.

8.1.2.1 Permission management

According to MyData, permission management covers the technical functionalities required for human-centric *control* of personal data, such as the user interfaces and underlying data structures for individuals to view, understand, grant, revoke, and modify different kinds of permissions related to data flows.

The term 'permission' is used in a broad sense to cover the means that the individual has to take control of data flows. These means can be based on legislation (executing legal rights) or go beyond that. Part of the permission management functionality is that the operator only allows execution of such data transactions where the permission is valid.

ACROSS data governance framework will focus on permission management, providing a way for people to orchestrate the specific data that can be shared (or disclosed) between parties, for which purposes, and for how long. Furthermore, it will go beyond basic permission management including the following functionalities:

- IDS data usage policies for more fine-grained usage control
- Facilitate the GDPR minimization principle using Attribute Based Credentials or defining data transformation filters as a data usage policy.
- Provide the technical means to exercise the GDRP user rights, even after the data has been transferred.

8.1.2.2 Service management

MyData operators live in an ecosystem with data sources and data using services. Navigating this ecosystem requires the linking of actors through an operator: this is the purpose of the service management functionality. The human-centric manifestation of service management is the possibility for individuals to manage the relationships and connections to different data sources and data using services in the ecosystem.

Service management enables dynamic linking of data sources and data using services (permissioned by the individual) so that data can be available at different sources and can be used by multiple data using services.

In a multi-operator environment, it is a significant decision whether the operators use a shared service registry (potentially still distributed) or if each operator manages services separately. This is a topic that will evolve in future work; currently, there is limited standardisation or convergence in this field.

Service management encompasses both access control and technical connection management. However, the delivery of these functionalities is largely determined by the data sources. Operators may support these to a greater or less extent through, for example, key management services.

The ACROSS data governance framework will provide the service management functionality by designing and implementing a Graphical User Interface and providing a set of APIs to interact with the services.

The Graphical User Interface will allow the service providers to define the service metadata, including its characteristics from the point of view of personal data usage. On the other hand, the data governance framework APIs will provide the means to inform the services any change in the users´ consent or to exercise the GDRP user rights like data rectification or data portability.

8.1.2.3 ACROSS Data Governance Framework vs MyData operator: gap analysis

After a first analysis of the MyData operator requirements the conclusion is that ACROSS Data Governance Framework will share its main capabilities regarding permission and service management and it could be considered a proto-operator.

The main differences are:

- ACROSS data governance framework does not include data storage, data transfer and value exchange capabilities.
- ACROSS data governance extends the concept or permission with IDS data usage policies
- ACROSS will facilitates the GDPR minimization principle by leveraging the ABC technology (to be analysed)

8.2 Attribute Based Credentials (ABC)

Attribute based credentials (ABCs) are a technology that could potentially be applied to enable privacy, granular control, and data minimisation in ACROSS. Put simply, ABCs are ‘a way to have a trusted party 'vouch' for you in a situation where you don’t want to give away any more information than is absolutely necessary’ (Waag). PrivacyPatterns.org describes them as ‘a form of authentication mechanism that allows to flexibly and selectively authenticate different attributes about an entity without revealing additional information about the entity (zero-knowledge property).’

The DECODE pilot in Amsterdam (in which Waag was a partner) developed a proof-of-concept to enable ABC in certain city services. One of the pilot’s applications allowed people to generate a credential to prove they are over 18 without disclosing all of the other information shown in the passport, including that person’s specific age and date of birth. Further information on the ABC pilots in DECODE can be found at https://decodeproject.eu/publications/deployment-pilots-amsterdam.html .

There are a number of potential ways in which ABCs could potentially be applied to cross border services. At present, people moving across borders have to share a lot of information with a lot of different parties, ranging from public to private. One can imagine many examples where a person would want to exercise more granular control to minimise the amount of data they share – for example, a person may want to prove that they are an EU resident without disclosing their home address; or may want to prove they are eligible for an apartment without disclosing their income and employer; etc.

8.2.1 Applicability of ABC in ACROSS

Developments over the coming months will inform ACROSS partners as to whether and how ABCs may be a viable implementation in our own project. These developments include the completion of a preliminary gap analysis; the initial co-creation of the ACROSS governance framework; the development of specified use case scenarios; and a technical evaluation which considers this report, among others.

8.3 Applicability of IDS Data Usage Control in ACROSS

IDS Data usage control aims at exchanging of information between business partners and it does not explicitly cover personal/private data issues. However, some of the usage policies defined by IDS are also applicable to personal data transfers, giving the individual the possibility to control the way in which personal data is used in more fine-grained manner.

An IDS policy could be used to constraint the location in which data is used, to enforce the deletion of the personal data after a specific period or to modify the personal during the data transfer process.

In fact, some of the defined data usage policies can be used to enforce the some GDPR rights and principles. For example, the rule that allows to modify the data in transit could be used to ensure the data minimization principle.

However, in IDS, the policy enforcement functionality is performed by the IDS connectors and some of the rules can only be applied by the consumer connector, so it can be used only if the services (both public and private services) deploy the IDS connectors technology for data transfer.

ACROSS personal data framework will provide IDS policy enforcement capabilities without the use of IDS connectors as an added value functionality, as part of the Usage control module.