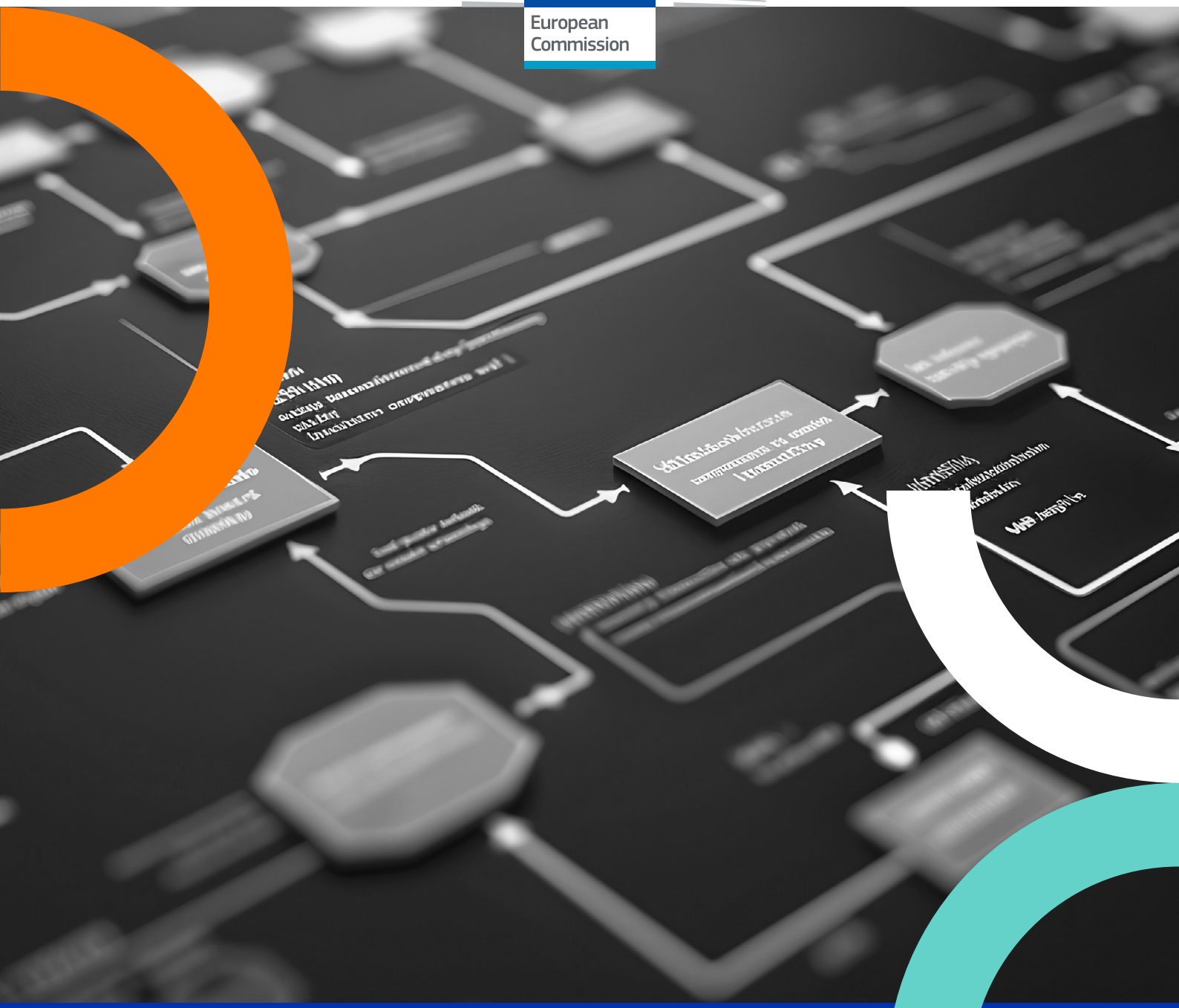
European Commission



European Higher Education Interoperability Framework

EUROPEAN
DIGITAL
EDUCATION
HUB

Education and Training

EUROPEAN
DIGITAL
EDUCATION
HUB

This publication was written by a consortium including the German Academic Exchange Service (DAAD, coordinator), Deloitte Consulting GmbH Germany, Deloitte S.L.U. Spain, Knowledge Innovation Centre (KIC), Stifterverband, SURF and EDEN, in collaboration with the members of the EDEH Higher Education Interoperability Working Group.

The European Digital Education Hub (EDEH) is an online community for practitioners from all sectors of education and training aiming to contribute to improving digital education in Europe. To achieve this goal, EDEH is not only a place for exchange and discussions but also offers a variety of different events and activities. These activities included a dedicated workgroup and a series of squads on higher education interoperability. This document is part of the results of these specific EDEH activities.

EUROPEAN
DIGITAL
EDUCATION
HUB

The European Digital Education Hub (EDEH) is an initiative of the European Commission, funded by the Erasmus+ programme (2021-2027) and operated by a consortium of 13 organisations under a service contract with the European Education and Culture Executive Agency (EACEA).

Luxembourg: Publications Office of the European Union, 2025

Print ISBN 978-92-68-31063-2 doi:10.2766/0459404 NC-01-25-156-EN-C
PDF ISBN 978-92-68-31062-5 doi:10.2766/5588498 NC-01-25-156-EN-N

Executive Summary

The European Higher Education Interoperability Framework (HEIF) was developed as part of the interoperability project within the European Digital Education Hub (EDEH). It addresses the need for seamless digital teaching and learning across Europe as stated in the European Commission's Digital Education Action Plan[1]. HEIF reflects a shared vision and a commitment from both higher education institutions (HEIs) and policy stakeholders. It aims to standardise digital processes to help student mobility across Europe and support virtual interuniversity campuses.

Experts in higher education and interoperability used European University alliances (EU As) to develop the HEIF. They aimed to improve the wider higher education landscape in Europe and support interoperability initiatives.

The EDEH interoperability framework centres on the reference architecture. It details the required components for interoperability in key use cases, covering the whole learner journey.

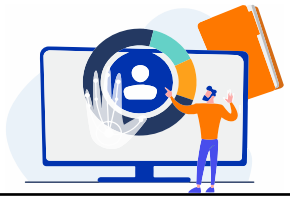
This report combines key elements from different reports. It includes descriptions of the reference architecture, high-level business flow diagrams, and helpful recommendations. These can help to find concrete solutions to address identified gaps.

The main insights and recommendations detailed in the report are as follows:

General recommendations	
Recommendations that have a cross-cutting application to more than one use case.	✔ Agree on the use of controlled vocabularies and ontologies. ✔ Agree on the use of standards. ✔ Minimise data exposure by sharing metadata. ✔ Consider the technical evolution of emerging solutions. ✔ Clearly and concisely define access roles and staff competencies. ✔ Use the latest versions of technical solutions/ frameworks.

[1] European Commission: Directorate-General for Education, Youth, Sport and Culture, Digital education action plan 2021-2027 – Improving the provision of digital skills in education and training, Publications Office of the European Union, 2023, https://data.europa.eu/doi/10.2766/149764.

Use case-specific recommendations

USE CASE 1 **Discover**  Enhancing the visibility and comparability of diverse learning and mobility opportunities across HEIs, emphasising the importance of machine-readable metadata for easy comparison and discovery. CMS (Website) · Course catalogue · Curriculum management	✔ Agree on the use of controlled vocabularies and ontologies. ✔ Align on learning outcome definitions. ✔ Ensure transparency in quality assurance processes. ✔ Improve course information for learners. ✔ Carefully consider the purpose of alliance-wide catalogues.
USE CASE 2 **Apply and get recognition**  Simplifying credit recognition and cross-institutional enrolment, emphasising seamless data exchange to support all forms of learner mobility and academic continuity. Admissions · Recognition	✔ Incorporate micro-credentials into recognition processes. ✔ Streamline recognition agreements. ✔ Foster digital trust and transparency through institutional policies and recognition rules.
USE CASE 3 **Access tools**  Streamlining the management and governance of shared resources among alliance members, covering both physical and virtual assets. Laboratory access · Library systems · Research tool registry	✔ Adopt a common approach and controlled vocabularies for tool discovery. ✔ Minimise data exposure by sharing metadata. ✔ Promote standardised access protocols and centralised tools catalogues.
USE CASE 4 **Manage educational resources**  Promoting the accessibility and mobility of educational materials, fostering a collaborative and accessible educational environment. Content generation · Sharing · Use and re-use	✔ Reduce the exposure of data. ✔ Make use of controlled vocabularies. ✔ Incorporate Open Educational Resources to improve accessibility.

USE CASE 5

Generate data

Establishing a standardised approach for the exchange of learners' activity data to ensure a seamless integration of various virtual learning environments.

Learning Analytics
Student Analytics

- Streamline data scope.
- Share metadata for efficient and lightweight system integration.
- Make clear distinctions between user roles for data management.
- Enable real-time task tracking to enhance visibility into their current status.

USE CASE 6

Earn a credential

The digital management of educational credentials (issuance, verification, revocation), affirming the achievements from diverse learning experiences.

Micro-credentials
Portable credentials

- Adopt up-to-date technologies for credential management.
- Enable selective disclosure.
- Avoid LMSs for issuing and holding credentials.
- Use trusted list for credential issuers verification.

USE CASE 7

User identity

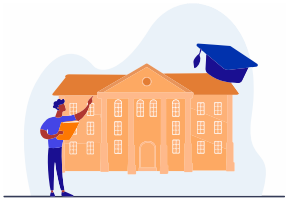
Achieving interoperability for user identities across educational transitions, ensuring consistent identification throughout their academic journey.

Access
Federated identity
Student cards

- Connect to eduGAIN.
- Agree alliance-wide attributes beyond the minimum eduGAIN profile.
- Adhere to existing European services like the European student card initiative.

USE CASE 8

Institutional identity



Developing a cohesive framework for trusted institutional identities, facilitating smoother collaborations and exchanges between HEIs.

Accreditation
Ranking

- Use established European Standard for HEI Identification.
- Monitor and manage institutional identity in European registries.
- Provide transparent information on APIs implemented.
- Provide key information openly.

Table of Content

0 Introduction

The European Higher Education Interoperability Framework (HEIF) was developed as part of the interoperability project within the European Digital Education Hub (EDEH). It addresses the need for seamless digital teaching and learning across Europe as stated in the European Commission's Digital Education Action Plan[2]. HEIF reflects a shared vision and a commitment from both higher education institutions (HEIs) and policy stakeholders. It aims to standardise digital processes to help student mobility across Europe and support virtual interuniversity campuses.

Experts in higher education and interoperability used European University alliances (EU As) to develop the HEIF. They followed their manifesto to improve the wider higher education landscape in Europe and support interoperability initiatives.

The EDEH interoperability framework centres on the reference architecture. It details the required components for interoperability in key use cases, covering the whole learner journey. This architecture acts as a central point of reference. It helps to identify existing gaps to reach full interoperability for priority use cases.

To facilitate uptake and practical use of the reference architecture, there are two further key resources:

- **Implementation resources** for higher education institutions (HEIs) at both strategic and practical levels.
- **A governance model** for policy and decision-makers who govern the overall environment.

The reference architecture is complemented by an **inventory**. It maps the standards and tools used across alliances. It also includes a **synthesis report** that analyses data from over 40 EU-As, generating insights for future decision- and policy making.

The development of the HEIF has been strongly anchored within the EDEH community of experts. The interoperability community adopted an agile and iterative process. They focused on continuous community engagement. Members gathered and shared experiences and established feedback loops. They did this through in-person events, online stock-taking sessions, squad meetings, one-off webinars, and regular satisfaction surveys.

[2] European Commission: Directorate-General for Education, Youth, Sport and Culture, Digital education action plan 2021-2027 – Improving the provision of digital skills in education and training, Publications Office of the European Union, 2023, https://data.europa.eu/doi/10.2766/149764.

This report combines key elements of different reports. It provides an overview of standards and tools. It also includes details about the reference architecture, high-level business flow diagrams, and recommendations. These can help to find concrete solutions to address identified gaps.

The report features dedicated chapters for each individual use case. Each use case is clearly defined and described, followed by its corresponding high-level flows. These high-level flows outline the steps in the business processes, highlighting the key requirements that the architecture must address.

After the high-level flows section, the report introduces the draft architecture, including the definition of its components. The next part builds on this foundation, detailing the reference architecture. The reference architecture presents existing solutions for each use case. It incorporates elements needed for interoperability. Then, the report outlines the capabilities required for interoperability. These represent core capabilities aligned with the reference architecture. Finally, the use case chapter ends with implementation recommendations. These aim to aid decision-making in addressing the topic.

0.1 Overview of use cases and scenarios

The use cases in focus were developed in a series of so-called 'use case squads' from February to October 2024. Each squad focused on one of the selected use cases and ran over a period of three weeks, featuring online meetings with the community of experts.

The online squad meetings attracted more than 80 unique registered participants, with an average of over 30 registered participants per squad. These meetings allowed experts to give technical feedback. This process helped to refine and adjust the draft architectures to meet the specific needs of the identified use cases. The squad meetings helped identify the components required for each use case. As a result, the squads refined the draft reference architectures and iterated on them based on experts' input and insights.

The School of Design Thinking at the Hasso-Plattner-Institute in Potsdam, Germany, guided a Design Thinking workshop. This event refined and challenged the use cases.

In January 2024, the School of Design Thinking at the Hasso-Plattner-Institute in Potsdam, Germany, guided a Design Thinking workshop. This event refined and challenged the use cases.

The first six use cases, as displayed below, define core processes in the learner journey. The remaining two use cases (use cases 7- User identity and 8 - Institutional identity) support the previous ones.

USE CASE 1

Discover

Enhancing the visibility and comparability of diverse learning and mobility opportunities across HEIs, emphasising the importance of machine-readable metadata for easy comparison and discovery.

CMS (Website) | Course catalogue | Curriculum management

USE CASE 2

Apply and get recognition

Simplifying credit recognition and cross-institutional enrolment, emphasising seamless data exchange to support all forms of learner mobility and academic continuity.

Admissions | Recognition

USE CASE 3

Access tools

Streamlining the management and governance of shared resources among alliance members, covering both physical and virtual assets.

Laboratory access | Library systems | Research tool registry

USE CASE 4

Manage educational resources

Promoting the accessibility and mobility of educational materials, fostering a collaborative and accessible educational environment.

Content generation | Sharing | Use and re-use

USE CASE 5

Generate data

Establishing a standardised approach for the exchange of learners' activity data to ensure a seamless integration of various virtual learning environments.

Learning Analytics | Student Analytics

USE CASE 6

Earn a credential

The digital management of educational credentials (issuance, verification, revocation), affirming the achievements from diverse learning experiences.

Micro-credentials | Portable credentials

USE CASE 7

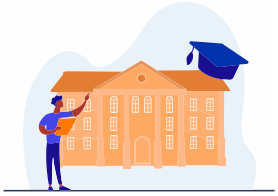
User identity

Achieving interoperability for user identities across educational transitions, ensuring consistent identification throughout their academic journey.

Access | Federated identity | Student cards

USE CASE 8

Institutional identity



Developing a cohesive framework for trusted institutional identities, facilitating smoother collaborations and exchanges between HEIs.

Accreditation | Ranking

0.2 Terminology and diagrams notation

This document shows various diagrams that illustrate high-level business processes and architectures. The different notations used for their representation are listed below:

The simplified architecture diagrams included in this report use the following notation:

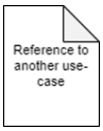
Data standard or model: Guidelines for structuring, describing, and recording data, metadata, and taxonomies.

Business data objects: A business object represents a concept used within a particular business domain[3].

Service: Defines systems required capabilities. Services share or expose data and must be interoperable.

System: Large technology components grouping software applications and physical technologies. Institutions usually have these systems in their ecosystem.

Stakeholder: An actor interacting with the different services and systems.



Reference: Represents a link to another use case describing in detail those components.

To show more detail in architecture, ArchiMate® [4] diagrams are presented. These diagrams help achieve the needed granularity. The structure of ArchiMate's language consists of two primary elements: layers and aspects. These elements collaborate to offer a holistic perspective of the enterprise architecture. The diagrams created in this project are based on the European Interoperability Reference Architecture (EIRA) framework[5]. This framework defines the key building blocks needed to create interoperable solutions.

[3] https://pubs.opengroup.org/architecture/archimate31-doc/chap08.html#_Ref412713032
[4] ArchiMate is a registered trademark of The Open Group. The ArchiMate language is an open and independent modelling language for enterprise architecture: https://www.opengroup.org/archimate-forum
[5] EIRA definition and releases: https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira?f%5B0%5D=solution_content_bundle%3Arelease

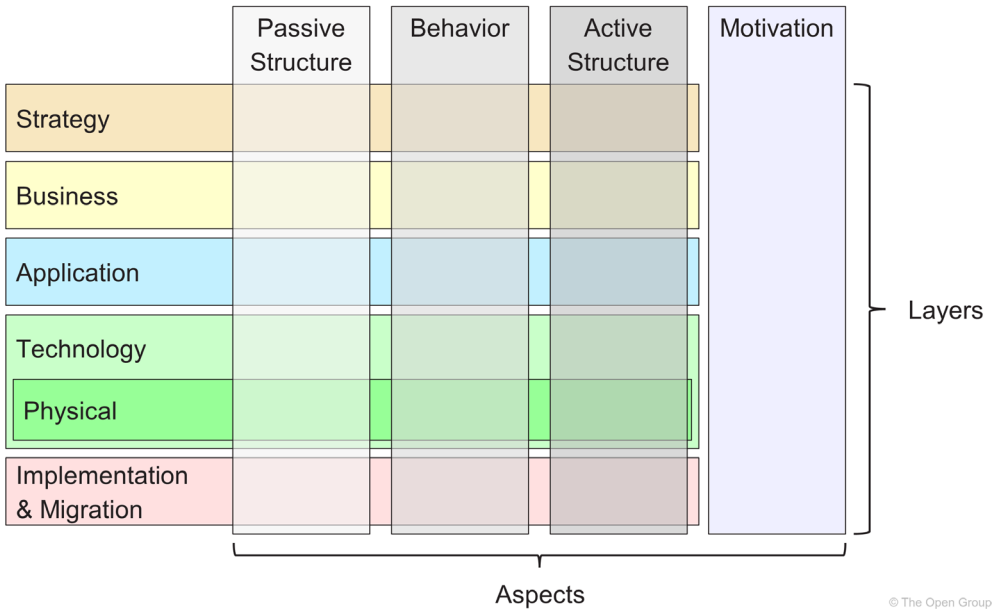


Figure 1 - ArchiMate framework overview.
© The Open Group

Aspects show different views of the enterprise architecture. They give special insights that focus on specific parts of the architecture.

Layers show different levels of abstraction in the architecture. They create a hierarchy that helps organise and distinguish between various domains.

This report focuses on the business and application layers, even though the reference architecture includes basic building blocks for different layers. The business layer (yellow) represents the highest level of abstraction. It focuses on the business aspects of the architecture. The application layer (blue) provides a connection between business processes and technology. The European Interoperability Framework (EIF) defines four layers for interoperability: legal, organisational, semantic, and technical. Three ArchiMate views were created for each use case: one for the semantic layer, one for the organisational layer, and one for the technical layer. These architectures are designed to fit existing solutions, adding the necessary blocks for interoperability.

ArchiMate diagrams models included in this report use the following notation:

Business layer	Application layer	Definition
Business Actor		A business actor is a business entity that is capable of performing behavior.
Business Role		A business role is the responsibility for performing specific behavior, to which an actor can be assigned, or the part an actor plays in a particular action or event.
Business Interaction	Application Interaction	An interaction is a unit of collective behavior performed by (a colaboration of) two or more business roles.
Business Collaboration	Application Collaboration	A collaboration represents an aggregate of two or more internal active structure elements that work together to perform collective behavior.
Business Interface	Application Interface	An interface is a point of access where a service is made avaiable.
Business Event	Application Event	An event signifies a state change, with a potential time attribute indicating when the event occurs.
Business Function	Application Function	A function encompasses behavior based on criteria such as resources, competencies, or location, managed, performed, or implemented as a whole.
Business Service	Application Service	External behavior elements, termed services, embody explicitly defined exposed behavior. A service represents the externally visible behavior of a providing system, emphasizing the value offered to users.
Business Process	Application Process	A process represents a sequence of behaviors that achieves a specific outcome such as a defined set of products or services.
Business Object	Data Object	A data object represents data structured for automated processing
Contract		A contract represents a formal or informal specification of an agreement between a provider and a consumer that specifies the rights and obligations associated with a product and establishes functional and non-functional parameters for interaction.
Representation		A representation represents a perceptible form of the inforrnation carried by a business object.
	Application Component	An application component represents an encapsulation of application functionality aligned to implementation structure, which is modular and replaceable. It encapsulates its behavior and data, exposes services, and makes them available through interfaces.

Figure 2 - ArchiMate basic building blocks definition.

0.3 General Recommendations

Throughout the working sessions, the community gathered recommendations and good practices for each stage of the learner's journey. Many of these are technical in nature but also address organisational aspects. The aim of these recommendations is to facilitate and guide the path towards interoperability. However,

they are not the only way to achieve interoperability. Instead, they draw on the experiences and successes of those who have faced and overcome the challenges of this journey.

This section gives basic recommendations that apply across multiple use cases. It helps build a foundation for achieving interoperability.

- **Use standards:** Using agreed data standards facilitates interoperability between entities.
- **Use controlled vocabularies:** Controlled vocabularies help define resources clearly. This makes it easier to filter, classify, identify, and compare them.
- **Share metadata:** Sharing metadata helps you minimise data exposure. This promotes privacy and allows for lighter communications.
- **Define roles clearly:** Clearly defining access roles and staff skills helps professionals in an organisation to use only the systems they need. This reduces errors and simplifies processes.
- **Explore new solutions:** Looking at emerging technologies expands the possibilities for tackling organisational challenges. It also offers fresh chances to adopt innovative solutions together.
- **Use the latest versions:** Using the latest versions of technical solutions or frameworks enhances interoperability. It aligns all entities on the same version, ensuring systems are more robust, secure, and up-to-date.

In specific sections of each use case, some of these recommendations are detailed further as certain cases need special attention.

To enhance the effectiveness of the initiative, it is recommended to adopt a more practical, action-focused approach. This approach should include:

1. **Structured data-sharing protocols:** set-up formal agreements to make data sharing easier and more standardised between institutions.
2. **Capacity-building programs:** Provide accessible pathways for skill development. This equips stakeholders with the tools and knowledge they need to collaborate effectively.
3. **Innovation challenges:** Advance creativity and involvement by holding contests that promote new ideas for common issues.
4. **Long-term sustainability strategies:** Make detailed plans to keep the initiative effective and flexible as time goes on.

In closing this section and looking ahead, it's important to highlight that different use cases come with varying recommendations. This depends on factors like how similar they are to other cases, the feedback received, the depth of the case, or its current progress in the landscape.

PART 1

Use case 1 – Discovery

1 Use case 1 – Discover

USE CASE 1

Discover

Enhancing the visibility and comparability of diverse learning and mobility opportunities across HEIs, emphasising the importance of machine-readable metadata for easy comparison and discovery.

CMS (Website) | Course catalogue | Curriculum management

1.1 Use case definition

The Discovery use case marks the beginning of the learner's journey. This use case focuses on the concept of a course catalogue. Course catalogues are key tools for higher education institutions and EU-As. They give prospective students important information. The broader discovery phase might help learners understand job market demands or use tools to explore their preferences and talents. However, these aspects are not necessarily within the remit EU-As.

The course catalogue is a tool used by institutions, alliances, or other collaborative arrangements between HEIs to manage and offer learning opportunities. Educators create these opportunities by designing activities and assessments, which are then added to the catalogue. Learners use course catalogues to explore available learning opportunities and compare different offerings.

A joint course catalogue created by multiple EU-As improves the visibility and comparison of different learning and mobility opportunities across HEIs. This use case highlights the need for standardised course metadata. Clear and consistent metadata makes it easier to collect, find, and compare learning opportunities.

1.2 High-level flow

The discovery use case is defined by two main processes. First, designing and publishing a learning opportunity. And second, searching for relevant opportunities. This use case involves the following stakeholders:

- **Catalogue user:** A catalogue user is anyone searching for learning opportunities. This could be an educator, a registered learner at an institution, or a potential learner looking for the most suitable course.
- **Publishing institution / HEI:** This is an institution that publishes learning opportunities from its local catalogue. Different stakeholders, like educators and administrative staff, oversee the process.
- **Catalogue operator:** This is an organisation or unit responsible for managing and maintaining a course catalogue. It oversees validation processes and ensures the quality of the catalogue content.
- **Qualification standards body (Economy):** This is an official body that defines the skills needed to practise regulated professions[6].
- **Joint degree consortium:** This is a steering body that handles the organisational tasks for designing, developing, and delivering a joint degree. It usually includes representatives from the participating institutions.

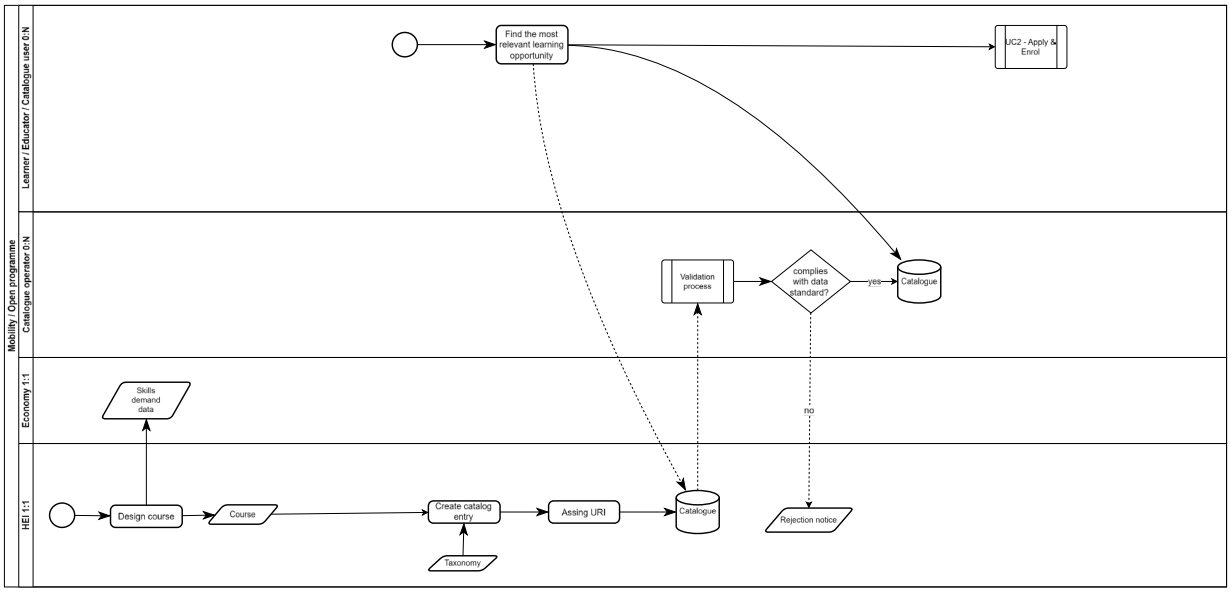


Figure 3 - Design and search of learning opportunities in mobility and open programmes scenarios.
© 2025 European Union

Educators within an institution design learning opportunities based on in-demand skills. This process is kept abstract, as it varies between institutions. The project does not aim to change existing processes but to propose general methods that can be adapted locally.

[6] https://europa.eu/youreurope/citizens/work/professional-qualifications/regulated-professions/index_en.htm

Quality assurance, which is a sensitive and institution-specific process, is outside the scope of this data flow. Once a learning opportunity is designed, it is added to the local catalogue. Many tools can store learning opportunities. Each tool affects how you enter a course into the catalogue and create a uniform resource identifier (URI)[7] to access them. In some cases, the URI will be the outcome of creating the entry in the catalogue.

Once a learning opportunity is included in the local catalogue, it can be published in a central catalogue. However, this step is optional since some approaches do not use a central catalogue. Instead they collect data in real time from multiple local catalogues and present it to users. If a central catalogue is used, all incoming data must go through a validation process. This ensures that the information meets the required format and includes all necessary details before being stored.

The second process focuses on discovering available learning opportunities. This is shown in Figure 3 – Design and Search of Learning Opportunities in Mobility and Open Programmes Scenarios © 2025 European Union. A search may lead a potential learner to apply for an opportunity. Because of this, a link to Use Case 2 – Apply and get recognition has been included at the end of the search process.

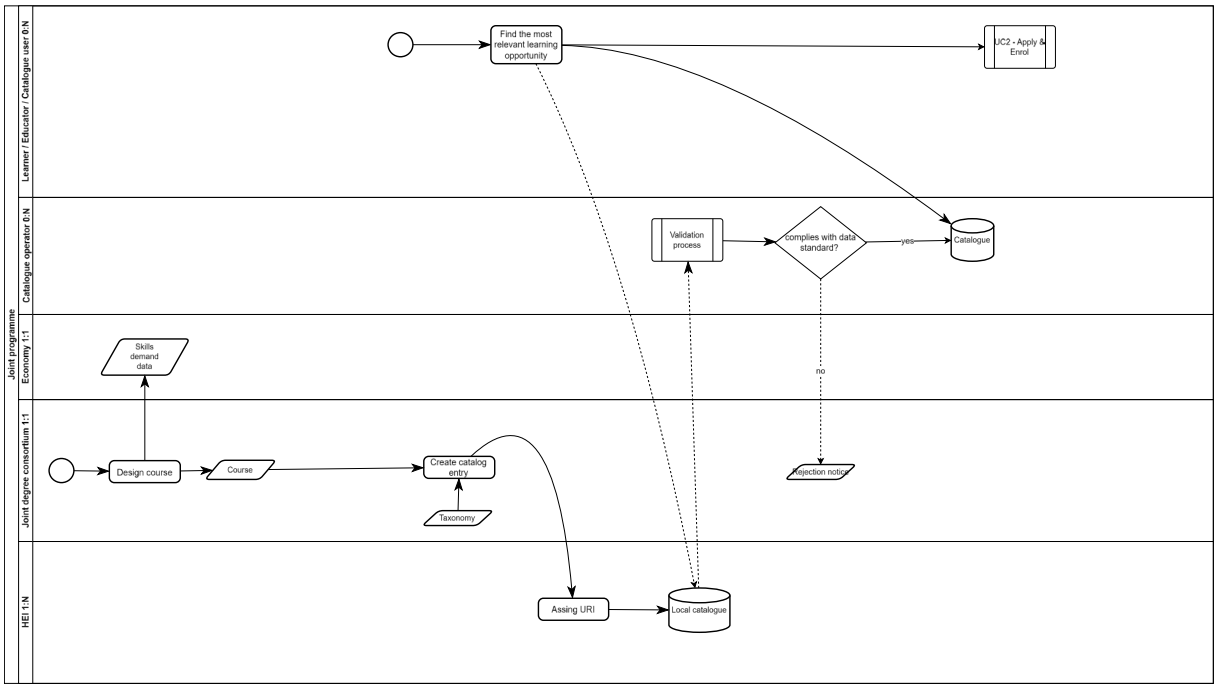


Figure 4 - Design and search of learning opportunities in joint programmes scenario.
© 2025 European Union

[7] RFC 3986: Uniform Resource Identifier (URI): Generic Syntax (rfc-editor.org)

The joint programmes scenario has specific characteristics. Participating institutions work together to design the learning opportunities they offer. In this case, the specification must follow a shared format that can later be added to local catalogues. This presents the first technical challenge in achieving interoperability.

After the specification is added to local catalogues, the institution in charge of a learning opportunity includes it in its local catalogue. Then, it publishes the information in the central catalogue with its unique URI. The rest of the process remains unchanged, and no further adjustments are needed.

1.3 Draft architecture

The original draft architecture was challenged and revised during the squad sessions, resulting in the diagrams below. The three scenarios outlined previously all impact the reference architecture of this use case. They share the same basic components, outlined in „Figure 3 - Design and search of learning opportunities in mobility and open programmes scenarios“. The joint programme and mobility diagrams also include additional components needed to cope with the nuances of their respective scenarios.

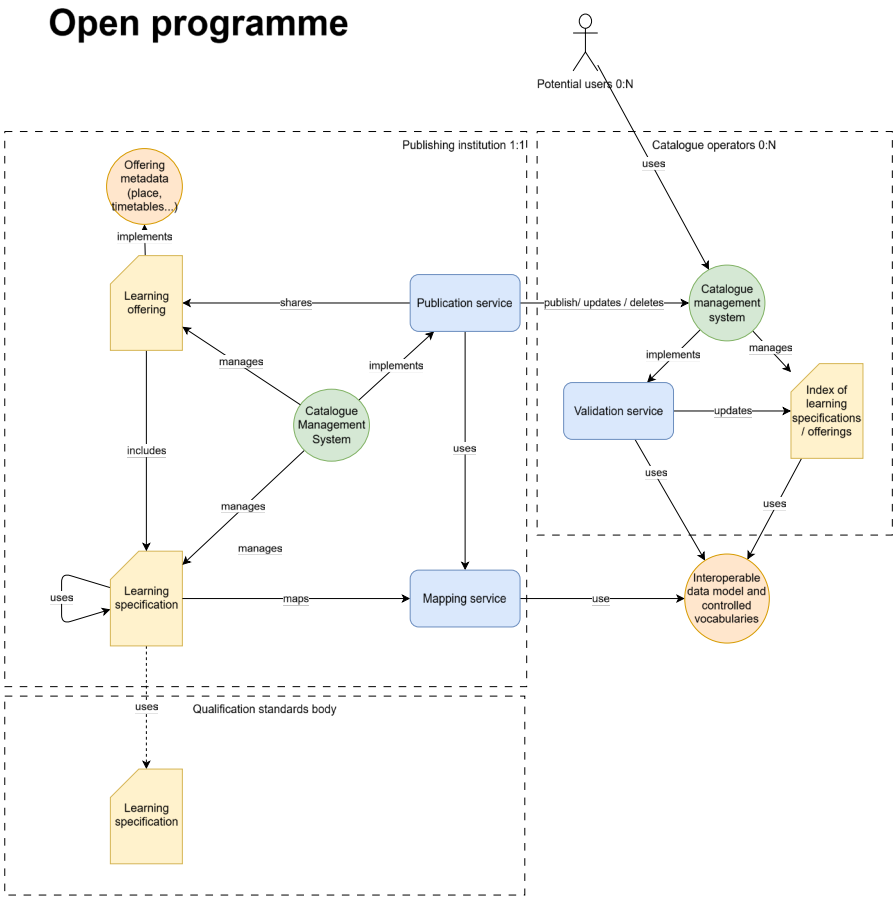


Figure 5 - Main components required to manage a central catalogue of learning opportunities.
© 2025 European Union

Main components inherent to this use case are:

Business objects

- **Learning specification:** This is a definition of a learning opportunity. It includes details about the learning activities, enrolment requirements, assessments, and outcomes after completion.
- **Learning offering:** A specific instance of a learning specification, taking place at a specific time in an academic calendar, with its scheduling details. The European Learning Model (ELM)[8] standard does not separate learning specifications from offerings. However, most alliances' management systems do make this distinction. This is reflected in the architecture to support the existing systems already in place. Throughout this report, we will use the terms ‚specifications' and ‚offerings' to refer to learning opportunities.

Services

- **Mapping service:** Service to translate between different data models and standards. Mapping services are widely used to enable interoperability between systems exposing a data model that differs from the receiving system. In this use case mapping services play a key role to enable seamless communication with the catalogue.
- **Harvester:** A service that collects information from management systems that don't have publishing or exporting options. Harvesters collect data from exiting systems and ready it for the central catalogue. They can also collect and merge information from various services. This helps mapping between different data models or standards.
- **Publication service:** This service sends information from a local catalogue to the central one. It uses the same communication protocol as the catalogue ingesting service.
- **Validation service:** A service that checks received data against data standards and ensures it meets agreed minimal required fields. It does not interfere or overlap with quality assurance processes and focuses exclusively on compliance with data structures.

Systems

- Catalogue management system: A system for managing the catalogue of learning opportunities.

[8] https://europa.eu/europass/elm-browser/index.html

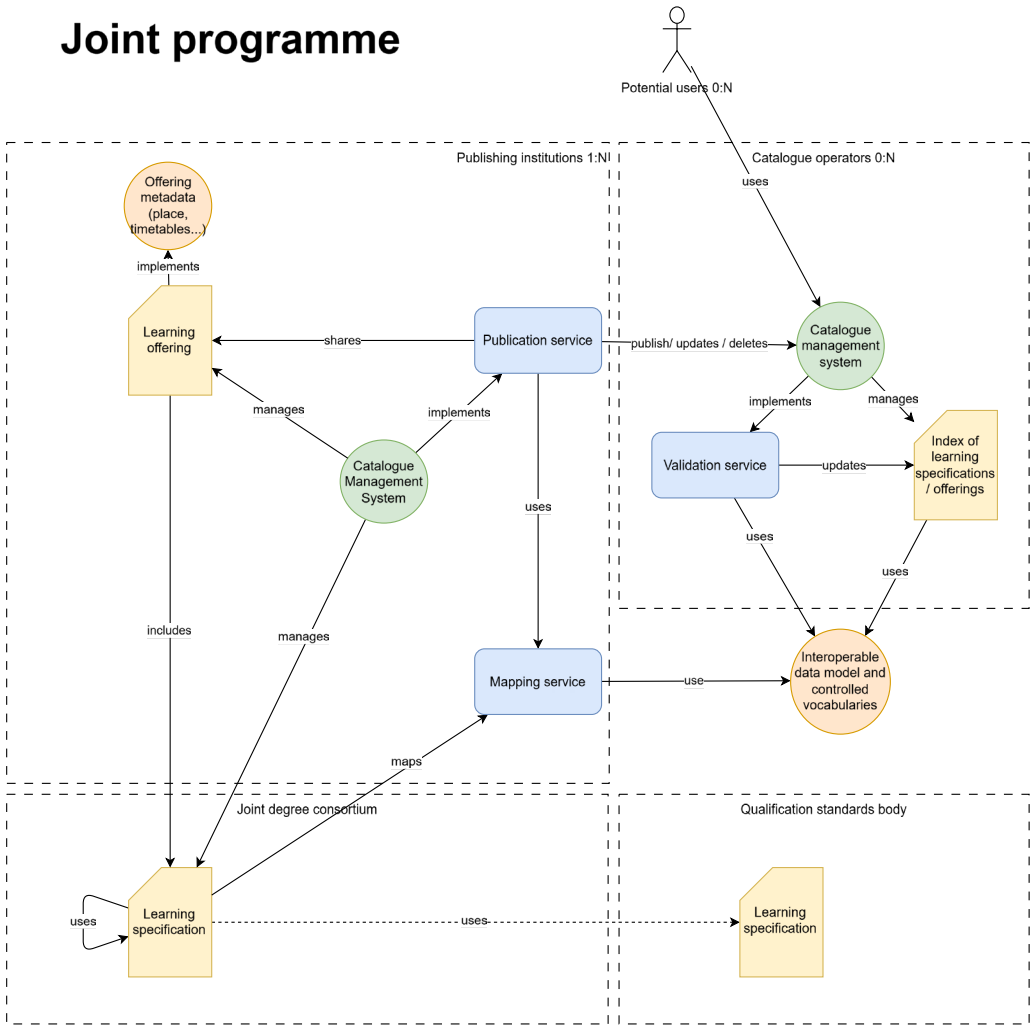


Figure 6 - Specific components required to work with a central catalogue managing opportunities belonging to a joint programme.
© 2025 European Union

This scenario focuses on the learning opportunities provided by joint programmes. The institutions involved design the curriculum, which is then delivered. This leads to a shared learning specification that may or may not be compatible with the different local data models. To overcome this challenge, the mapping service can be used to translate the specifications into the local models. Learning specifications can be saved in each local catalogue run by an institution in the joint programme. However, offerings are handled by the local catalogue of the institution providing that specific opportunity. The rest of the process stays the same. The components work as shown in „Figure 5 - Main components required to manage a central catalogue of learning opportunities."

Mobility

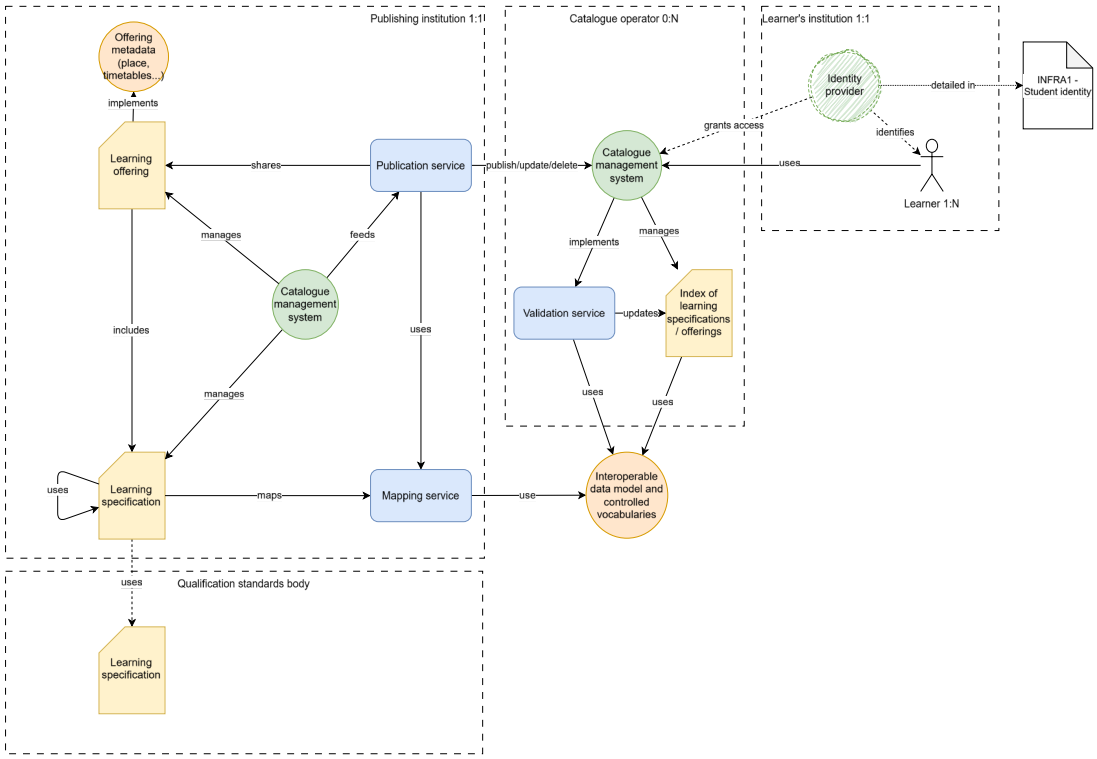


Figure 7 - Optional identity provider to filter opportunities available for a mobility.
© 2025 European Union

In a mobility scenario, an identity provider is an option to be included. This helps filter learning offerings for the learner based on past agreements.

1.4 Reference architecture

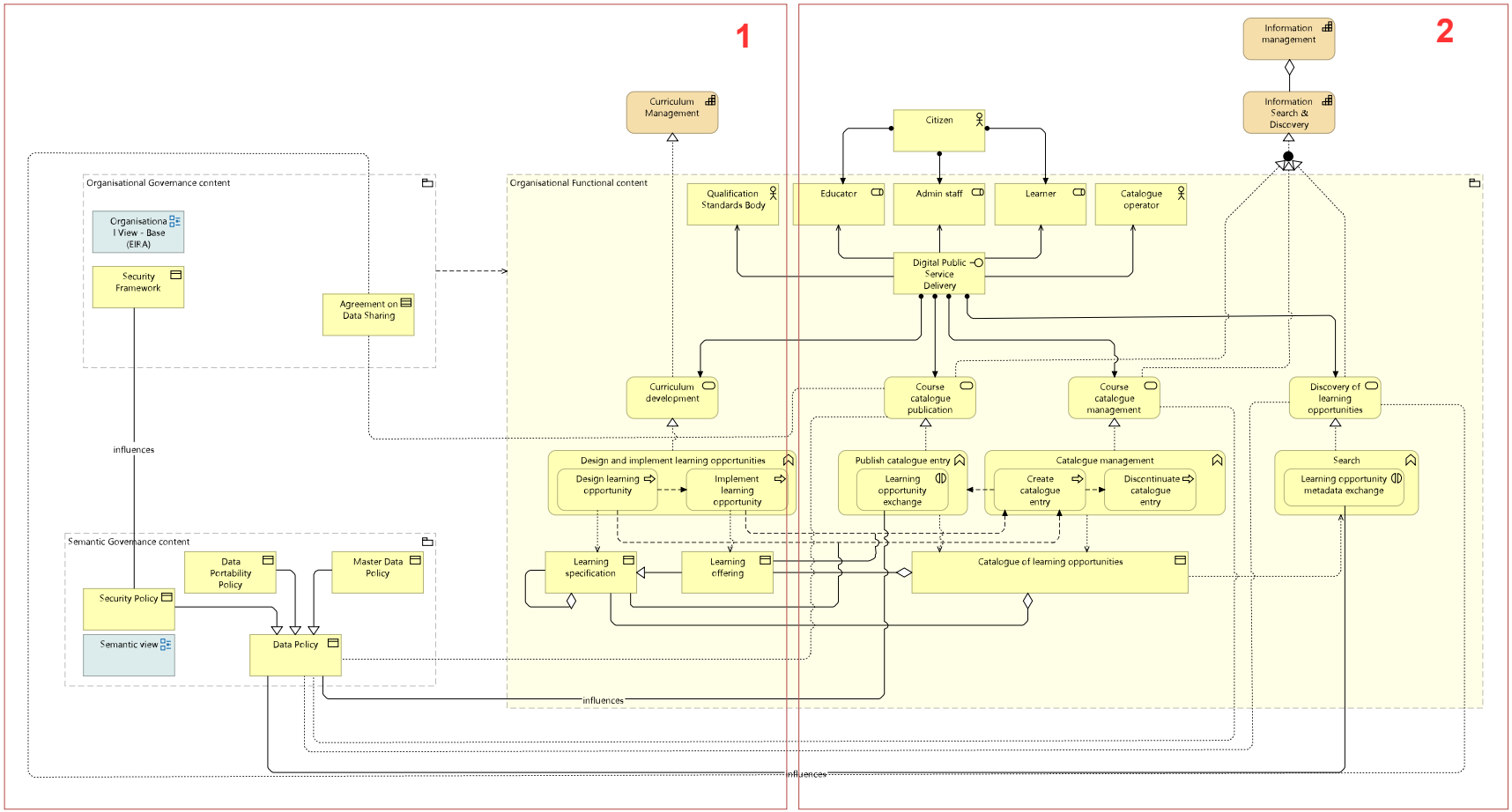


Figure 8 - Use case 1 (Discover) – organisational view.

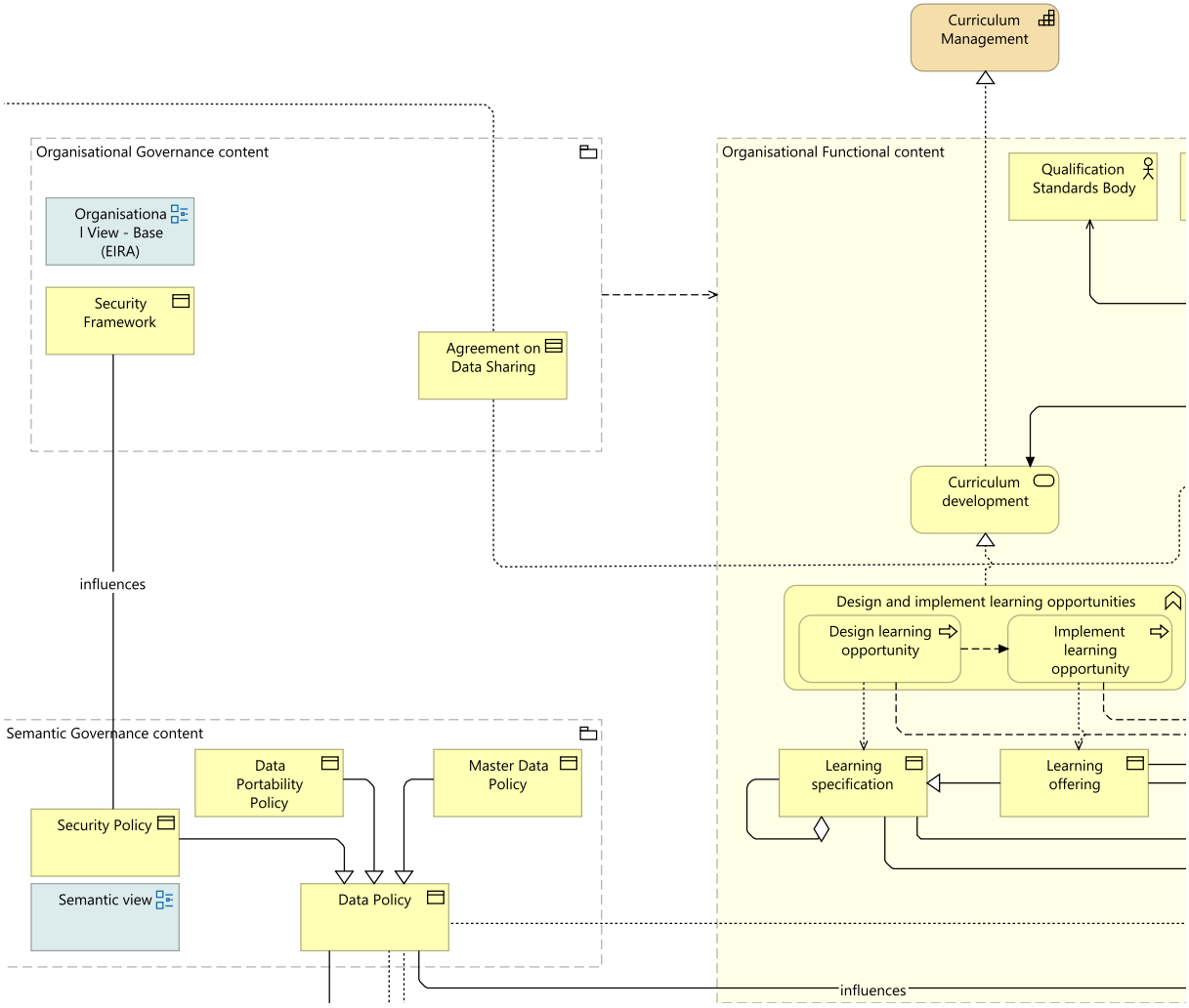


Figure 9 - Use case 1 (Discover) – organisational view - part 1.
© 2025 European Union

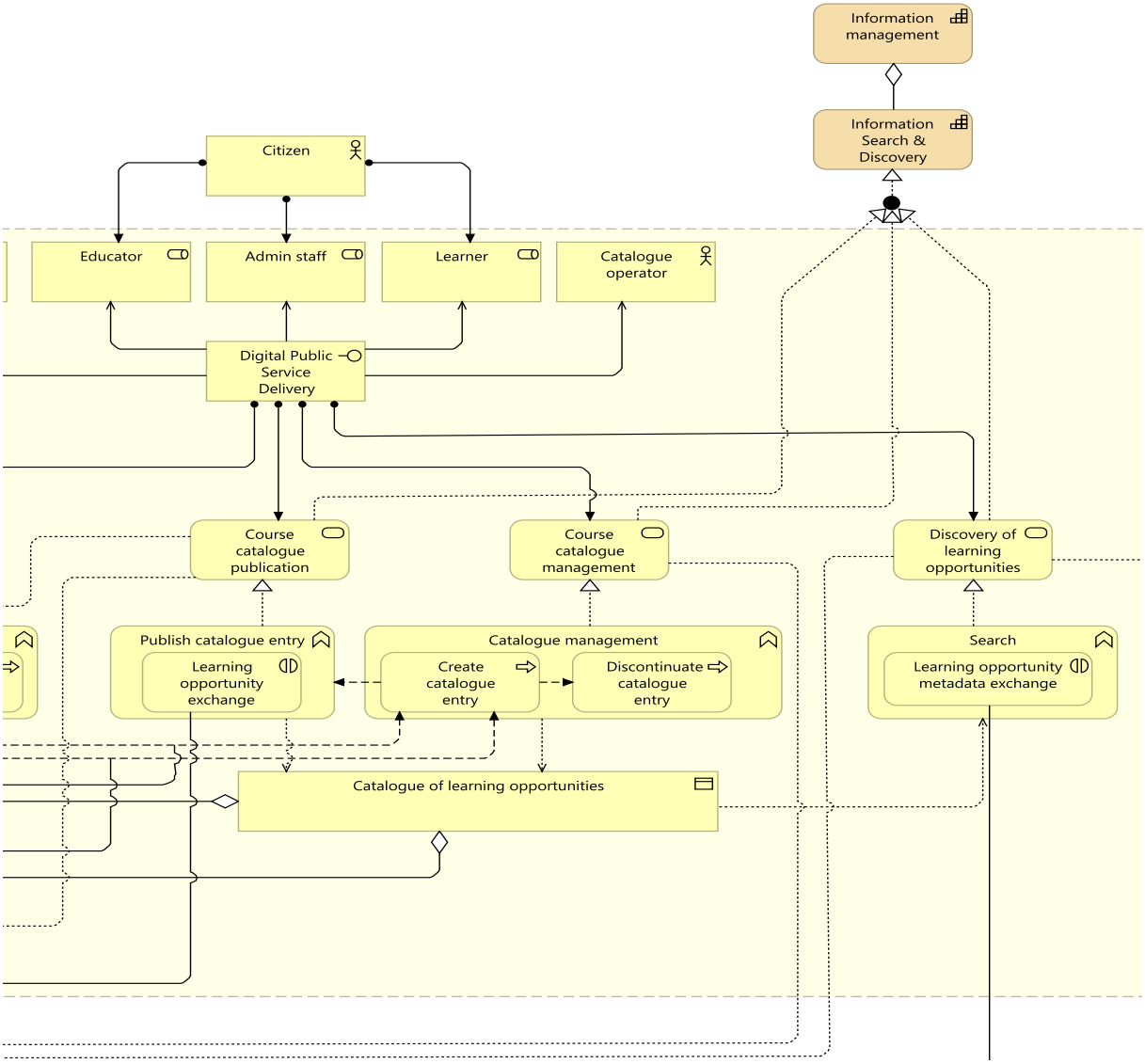


Figure 10 - Use case 1 (Discover) – organisational view - part 2.
© 2025 European Union

The organisational view diagrams show the key capabilities needed for this use case, including curriculum management and the search and discovery of information. The four main services are: 1. curriculum development; 2. course catalogue publication; 3. course catalogue management; and 4. discovery of learning opportunities. These services provide the required capabilities. Each service is further defined by its functions and processes, which are shaped by data policies and agreements.

The following table describes the most significant building blocks refined during the first squad series.

Building block	Type	Description
Curriculum management	Capability	The curriculum management creates or finds structured learning activities such as courses, subjects, and units. This ensures the institution can deliver them effectively.
Information search and discovery	Capability	The information search and discovery provide tools, catalogues, and services to help people locate and access information.
Agreement on data sharing	Contract	A data sharing agreement is a contract. It outlines the information needs, syntax rules, protocols, and semantic artefacts for data exchange.
Data portability policy	Business object	A data portability policy regulates data reuse and data transference between public administrations.
Learning specification	Business object	A learning specification includes information of a learning opportunity. It includes the requisites, learning activities, assessments and learning outcomes.
Learning offering	Business object	A learning offering is an instance of a learning specification in an academic period. It includes scheduling information.
Catalogue of learning opportunities	Business object	Collection of learning opportunities offered by one or multiple institutions.
Design learning opportunity	Business process	A design learning opportunity produces complete specifications of structured learning opportunities.
Implement learning opportunity	Business process	A implement learning opportunity delivers educational products.
Security framework	Business object	A security framework helps protect data, information, and knowledge assets, along with the organisational resources that manage them.

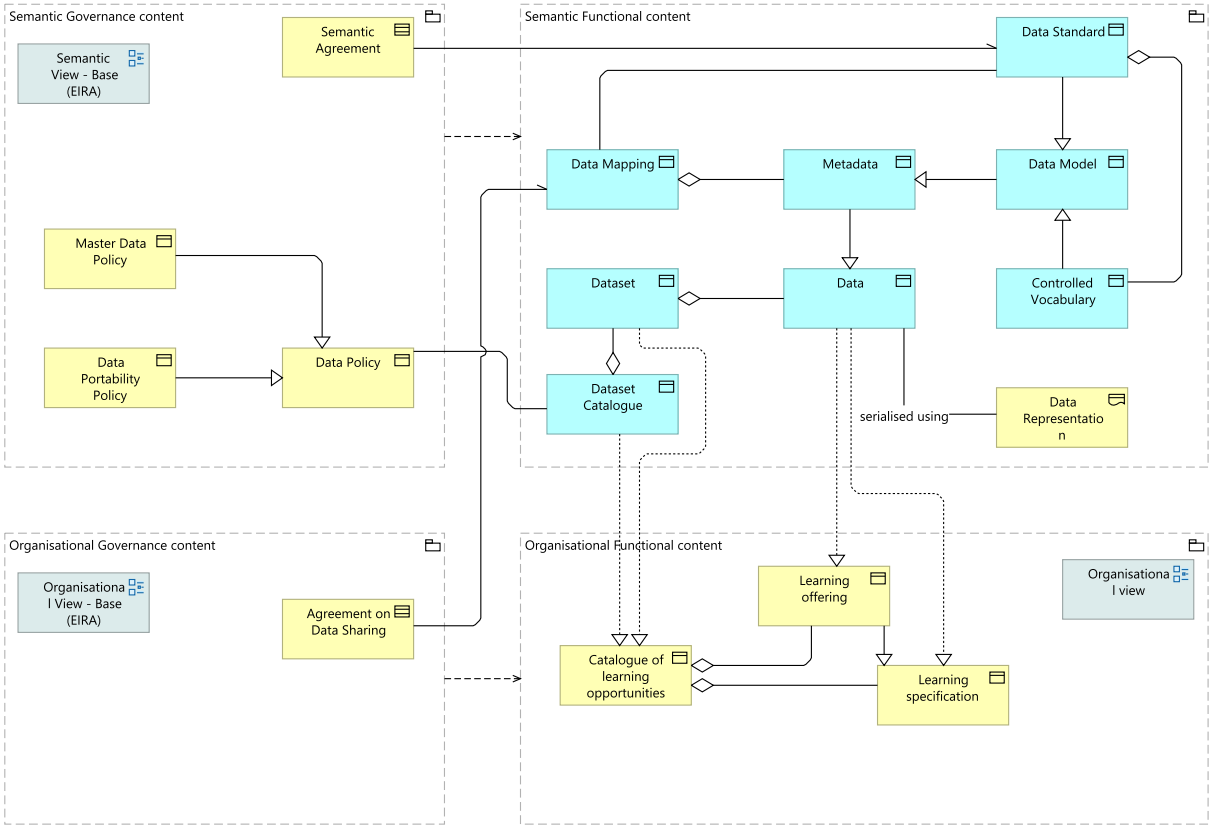


Figure 11 Use case 1 (Discover) – semantic view.
© 2025 European Union

The previous ArchiMate view corresponds to the semantic view. In this view, building blocks from both the business and technical layers are combined to represent the flow of mapping non-standardised data to standardised data. Semantic agreements help with standardisation. Their use is shown through the relationship between the ArchiMate Building Block (ABB) Semantic Agreement and the technical ABB Data Standard. As in the previous view, the most important ABBs are:

Building block	Type	Description
Semantic agreement	Contract	A semantic agreement formalises an agreement from a peer to the common ontology. This ontology results from a matching or mapping process used to resolve semantic discrepancies. The combination matching process includes a linguistic base and compares internal and external structures. The outcome of this matching process will help create an agreement unit, which is a key component of the agreement.

Dataset catalogue	Data object	A dataset catalogue indexes a collection of datasets in a systematic way.
Dataset	Data object	A dataset is a collection of related data, organised, and presented in a structured format.
Data	Data object	Data stores digital or non-digital information. This information is collected, stored, or processed by a computer system or other tech infrastructure. This information comes in many forms, such as text, numbers, images, video, audio, and more.
Data standard	Data object	A data standard guides the organisation, integration, and management of data. This includes data models, formats, protocols, and technical specs. They help ensure data consistency, interoperability, and efficient exchange.
Controlled vocabulary	Data object	A controlled vocabulary ABB is a data object. It offers a set of chosen terms to describe concepts or objects in a specific field. It is a standardised list of terms. It ensures consistency and accuracy in indexing, searching, and retrieving information.
Data representation	Representation	Data Representation representation ABB refers to theis a method or mechanism by which data is encoded and stored in a computer system. It involves transforming data from its original form into a format that can be processed and manipulated by a computer.

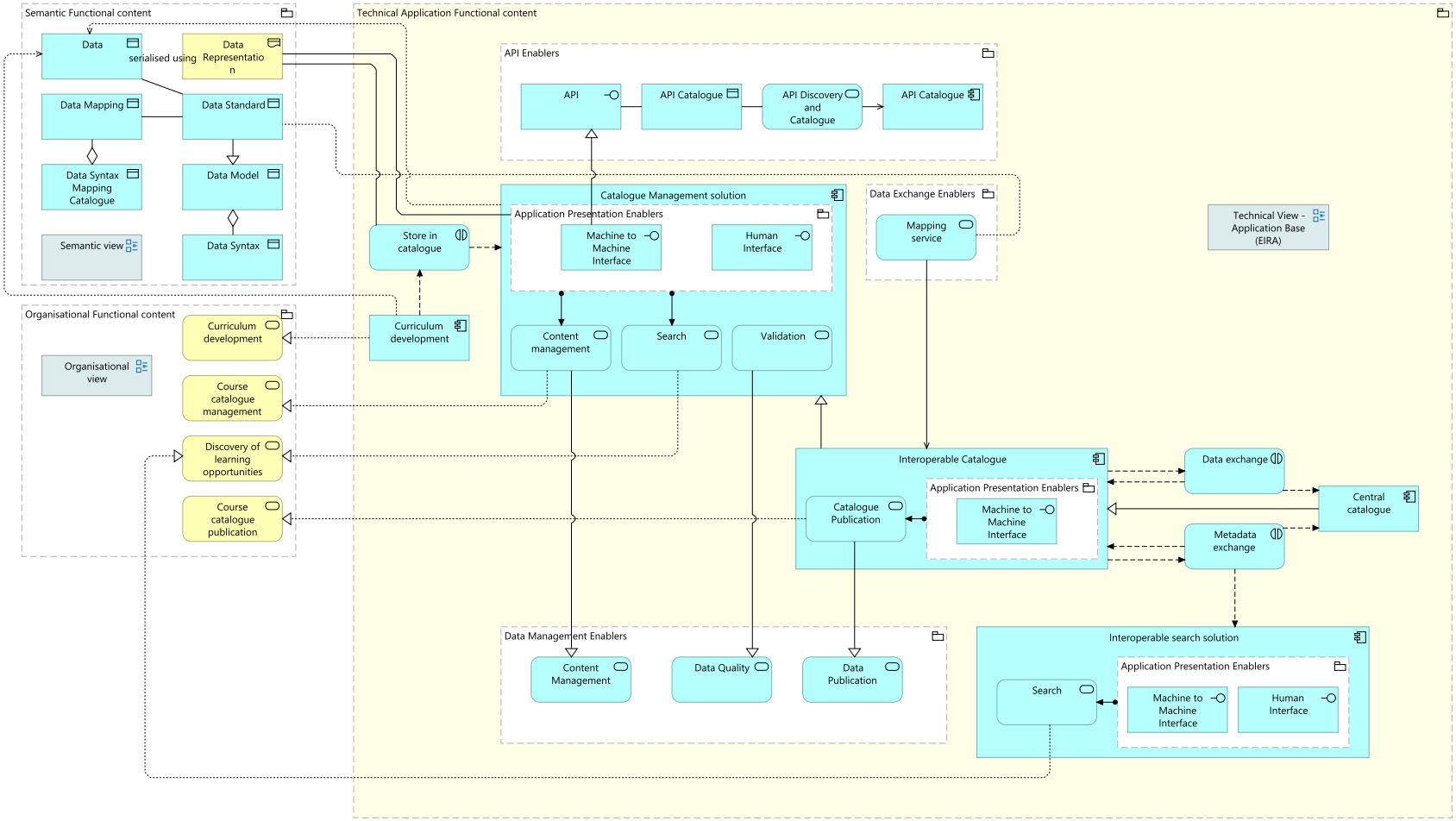


Figure 12 - Use case 1 (Discover) - technical view.

The final view in this architecture for use case 1 shows the technical layer. This view includes not only the target interoperable solutions but also the current solutions institutions have implemented. It shows these as active parts of the architecture and explains how non-interoperable and interoperable components relate. This gives a view of coexistence that can help move towards interoperability. The interoperable solutions rely on using standardised metadata through a mapping service. This is supported by the semantic agreements defined in the semantic layer.

Building block	Type	Description
Data syntax mapping catalogue	Data object	A data syntax mapping catalogue bridges the differences between two systems or data models. It ensures that data stays accurate and usable as it moves from a source to a destination.
Curriculum development	Application component	A curriculum development ABB is an application service. It produces complete specifications of structured learning opportunities, such as courses or programmes, through enabled processes.
API catalogue	Application component	The API catalogue defines the functionalities of (open) software interfaces. These functionalities align with the implementation structure of digital services.
API discovery and catalogue	Application service	The catalogue management handles data storage, validation, publication, and retrieval in a catalogue. It helps users discover data easily.
Catalogue management solution	Application component	The catalogue management handles data storage, validation, publication, and retrieval in a catalogue. It helps users discover data easily.
Mapping service	Application service	A mapping service ABB is a service that enables the translatesion between data models, standards, or controlled vocabularies
Catalogue publication	Application service	The catalogue publication makes learning opportunities, assets, and educational resources accessible and reusable.

Interoperable catalogue	Application component	An interoperable catalogue is a specialisation of the catalogue management solution. It represents the interoperable variant of the proposed solution.
Interoperable search solution	Application component	The interoperable search solution ABB is an application component that enables the search for standardised metadata from an interoperable catalogue through a service.

For more about the ArchiMate building blocks in this diagram, review the blueprint reference architecture report. It has all the details you need about these schemes.

1.5 Interoperability required capabilities

Adapting to the proposed approaches requires interoperability capabilities. A strong data standard brings together learning opportunities from different institutions into one catalogue. This makes it easier to discover new options. However, the varied vocabulary used by different HEIs can complicate this process. Therefore, a standard vocabulary is essential for consistency. The absence of a common standard necessitates an intermediary. A mapping service can help standardise different HEI learning opportunities.

For more information about the interoperability capabilities of this use case, please see the comprehensive final mapping report for details.

1.6 Recommendations – use case 1

A significant amount of feedback has been received from the community through various sources regarding use case 1. To achieve interoperability, a series of recommendations have been outlined:

- **Use of agreed ontologies and controlled vocabularies:** Using controlled vocabularies is crucial for ensuring consistency and alignment of courses across different institutions. They provide a standardised set of terms and definitions. This helps eliminate ambiguities when institutions exchange information about courses and learning outcomes. Uniformity is essential for learning agreements. It enables clear articulation of course content, skills, and competencies. Using common terms for course descriptions and outcomes helps institutions map and compare courses. This makes academic collaborations and credit transfers across borders easier.
- **Standardise learning outcome descriptions:** Standardised learning outcome descriptions are essential for improving institutional collaboration. They enable easier assessment, comparison, and mapping of courses across different institutions and education systems. This standardisation

helps universities see students' learning achievements from partner institutions. It also supports flexibility and mobility in study programmes. Standardising learning outcomes helps higher education institutions set clear expectations. This promotes transparency and builds trust among learners. One way to standardise descriptions is by using classifications such as ESCO.

- **Improving course information for learners:** Institutions must provide clear and structured course information to help learners create effective study plans. This includes detailed descriptions of learning outcomes, course content, prerequisites, workload, credits, mode of delivery, and other relevant details. The ECTS Users Guide provides a benchmark for the information needed. Clear course listings help learners plan their academic paths, especially when studying abroad or at different institutions. Also, using a standard format for course information allows institutions to organise courses into catalogues better. This makes it easier for learners to find and compare options that meet their needs.
- **Carefully consider the purpose of alliance-wide catalogues:** Most European university alliances aim to create an alliance-wide catalogue of learning opportunities for their virtual inter-university campus. However, the specific goals will vary. Therefore, it is important to carefully consider the purpose and scope of the joint catalogue before starting this project and making design choices. This includes questions like what core content should be included and which learning opportunities to feature.
- **Start with a pilot or proof of concept:** Creating a joint catalogue that gathers information from all institutions in an alliance is complex. In particular when aiming for automated information flows. It is best to start with a pilot, demonstrator, or proof of concept. This can be a simpler manual or low complexity setup or testing a technical solution to collect learning opportunity data from some alliance members. When designing this pilot, consider how it can be scaled to include all offerings across the alliance.
- **Transparency in quality assurance processes:** Institutions should be transparent about their quality assurance processes. This includes external audits and internal reviews or certifications that confirm the quality of their courses and learning outcomes. By sharing how courses are evaluated and certified, institutions can build trust with potential partners. This transparency boosts confidence in academic standards, which is essential for new learning agreements. Showing a commitment to quality assurance also improves the institution's reputation. This, in turn, encourages future collaborations with universities, both locally and internationally.

These recommendations focusing on use case 1, aim to improve collaboration among higher educational institutions by promoting standardisation, transparency, and trust. These elements are key to establishing effective learning agreements. By standardising terminology and clarifying course offerings, institutions can uphold high quality standards. This helps facilitate student mobility and strengthens global academic partnerships.

PART 2

Use case 2 – Apply and get recognition

2 Use case 2 - Apply and get recognition

USE CASE 2

Apply and get recognition

Simplifying credit recognition and cross-institutional enrolment, emphasising seamless data exchange to support all forms of learner mobility and academic continuity.

Admissions Recognition

© 2024 Freepik

2.1 Use case definition

Use case 2, apply and get recognition, focuses on enrolling in a learning opportunity and creating an online learning agreement. Getting recognition involves assessing the learner's previous credentials, which is essential for admission decisions. This use case aims to simplify credit recognition and cross-institutional enrolment. It emphasises smooth data exchange to support all types of learner mobility and academic continuity.

2.2 High-level flow

This use case is a step further in the learner journey from the discovery use case. After identifying the most relevant learning opportunities in a catalogue, learners apply to selected opportunities. This second use case has two main steps. First, there is the application, which involves identity validation. Then, there is the evaluation of the application. This step may require some necessary validation and signing an agreement.

This use case has the following stakeholders involved:

- **Learner:** An individual who may enrol in a higher education program. Learners pursue various degrees, such as bachelor's, master's, or doctoral degrees. They engage in academic studies, research, and skill development. In this flow, the learner is an individual interested in a course for that they have discovered.
- **Application portal:** Any type of interface that lets the learner send their application form. It may be presented as a web or mobile application.

- **Sending / Receiving HEI:** A Higher Education Institutions involved in a mobility programme and either sending or receiving learners
- **Designated registrar:** The designated registrar is part of a joint programme or consortium. It can also be an extra unit or body, like one at the alliance level. This role coordinates the admission and enrolment processes.
- **Alliance:** Described by the European Commission, the European Universities alliances (EUAs) are 'transnational alliances that will become the universities of the future, promoting European values and identity, and revolutionising the quality and competitiveness of European higher education'. On the joint programme scenario, they are the ones which evaluate the application.
- **Alliance member:** A High Education Institution (HEI) that belongs to an alliance. They can be N per each alliance. On the joint programme scenario are the ones that handle application.

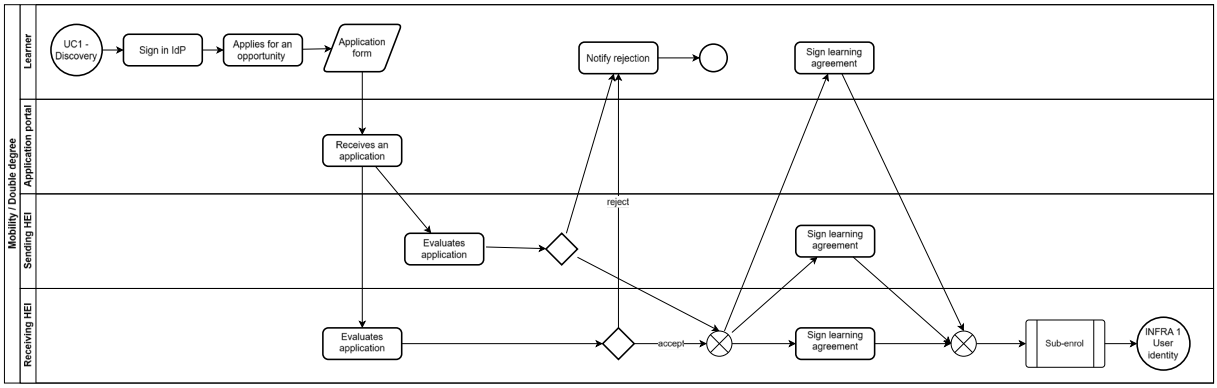


Figure 13 - High-level data objects, steps, and responsibilities to evaluate an application in a mobility scenario.
© 2025 European Union

Mobility scenarios have some particularities inherited from the Erasmus+ programme. Learners are registered with their sending institution. The sending institution, the receiving institution, and the learner sign a learning agreement. This agreement details the programme of studies at the receiving institution. It also guarantees that the learner will receive automatic recognition for all credits earned from successfully achieved learning outcomes during the mobility[9]. If any institution rejects the learner's application at any point in the flow, the application process is terminated. This is because all parties involved must agree for the flow to proceed.

[9] Mobility and learning agreements | Erasmus+ (europa.eu)

In the joint programme scenario, there is no individual learning agreement since the learner enrols in a standard programme that is offered jointly. They are enrolled in all participating institutions.

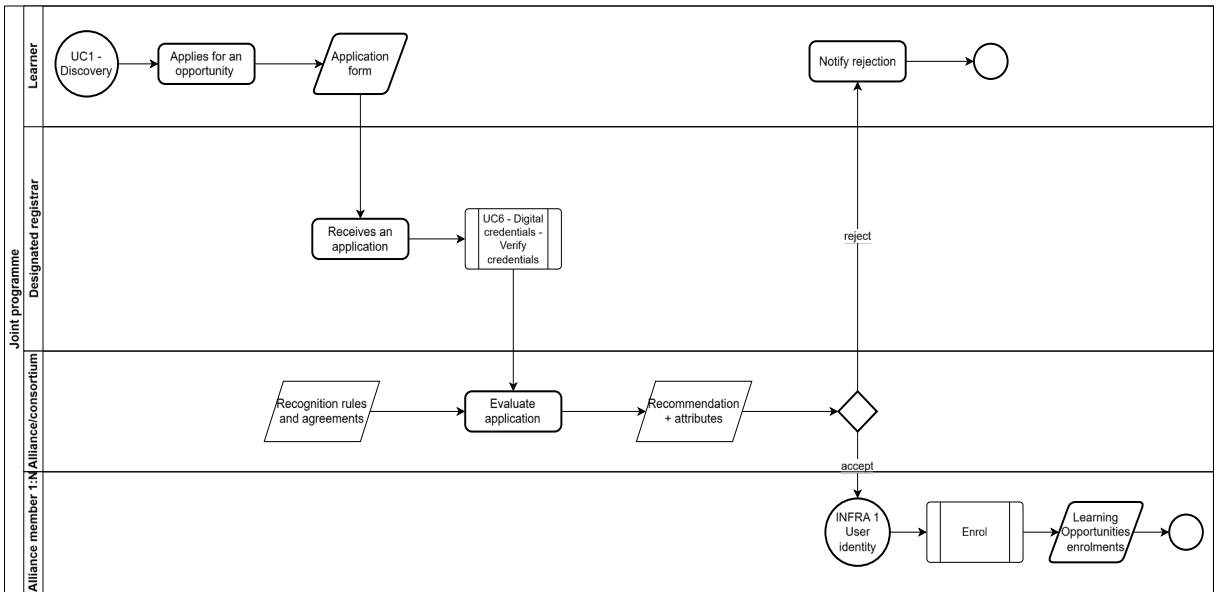


Figure 14 - High-level data objects, steps, and responsibilities to evaluate an application in a joint programme scenario.
© 2025 European Union

2.3 Draft architecture

This use case requires the following main components:

Business objects

- **Identity attributes:** The attributes required to verify the identity of a learner. Identity attributes will be explained in more detail in the use case 7 focused on user identity.
- **Credentials:** Credentials are physical or digital certificates. They confirm a learner's past achievements or claims.
- **Application:** The required data to validate and verify a learner's eligibility to participate in a learning opportunity.
- **Recognition rules and agreements:** An interoperability agreement that sets the rules for recognising a learner's past achievements.
- **Learning offering:** A specific learning plan that occurs in a set academic term, with details on scheduling.
- **Learning specification:** This outlines a learning opportunity. It includes various activities, enrolment requirements, assessments, and the outcomes you achieve after completion.

Services

- **Validation service:** Service to validate the information from an application.
- **Requisite compliance check service:** This service checks if a learner's past achievements meet the skills needed to enrol in an opportunity. It also considers the scheduling limits of a specific offering when needed.

Systems

- **Identity provider:** A system that manages learner identity, described in more detail in the use case focused on user identity. It handles learner identification and manages the identity details needed to verify and allow access to the right systems.
- **Catalogue management system:** A system that manages the catalogue of learning opportunities.

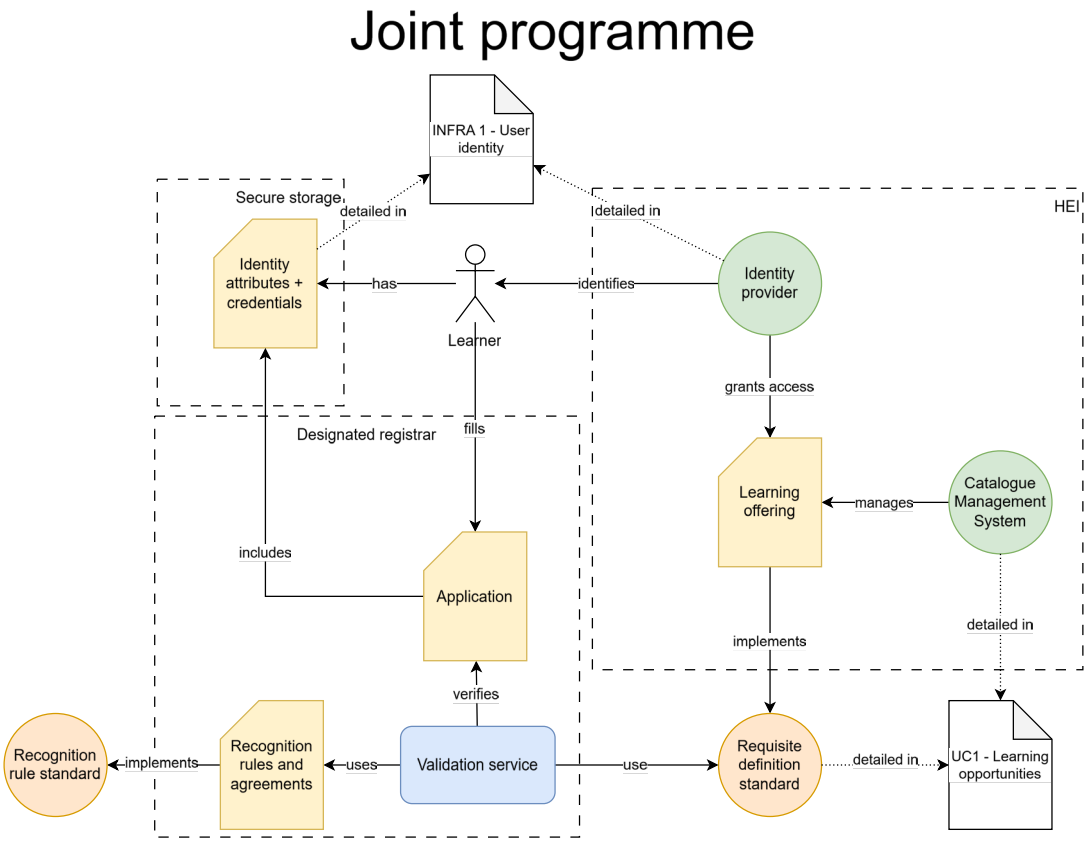


Figure 15 - Main components required to evaluate an application in a joint programme scenario.
© 2025 European Union

The mobility scenario is heavily influenced by the existing Erasmus+ process. Here, learners are registered at their home institution and have a unique identifier. Both institutions have checked each other's quality requirements before. Exam committees have verified the assessment policies, and there is an inter-institution agreement in place.

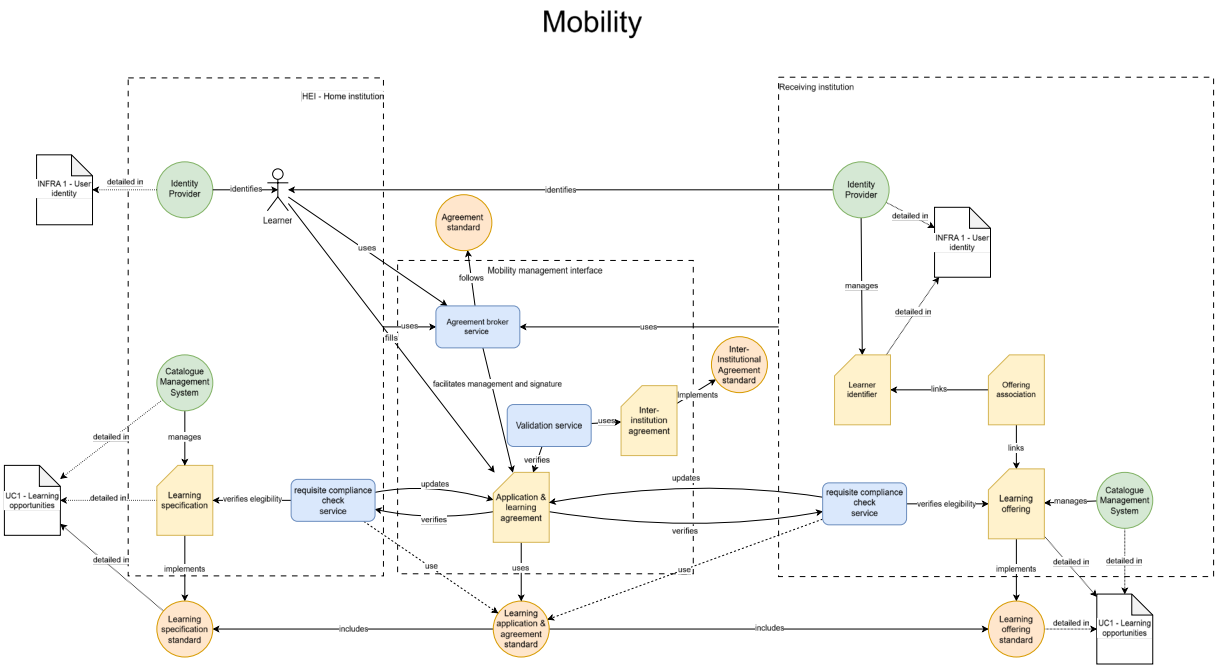


Figure 16 - Main components required to share learner data in a mobility scenario.
© 2025 European Union

The process begins with learners filling out an application form. This form includes the learning offerings they wish to take at the receiving institution. It also lists the learning specifications they will be recognised for after successful completion. The application must be validated by both institutions. To make this validation process work smoothly, learning agreements should follow a data standard that allows for an efficient compliance check. There are three main things to verify:

- The application meets the inter-institutional agreement.
- The home institution checks if the learner can enrol in the course. This means they match the requirements with what the learner has already achieved.
- The receiving institution checks if the incoming learner can enrol in the specific offering. This includes reviewing the schedule and confirming they meet the requirements.

Once the application is approved, all parties sign a learning agreement: the learner, the sending institution, and the receiving institution. The agreement broker facilitates the signing process and is out of the scope of this project. The learner's identity is then transferred to the receiving institution to facilitate the local enrolment process.

This use case relies on three use cases:

- **User identity** to transfer identity attributes.
- **Discovery** to find the offering in the receiving institution.
- **Earn a credentials** to verify eligibility and get the credits recognised once the mobility has successfully finalised.

2.4 Reference architecture

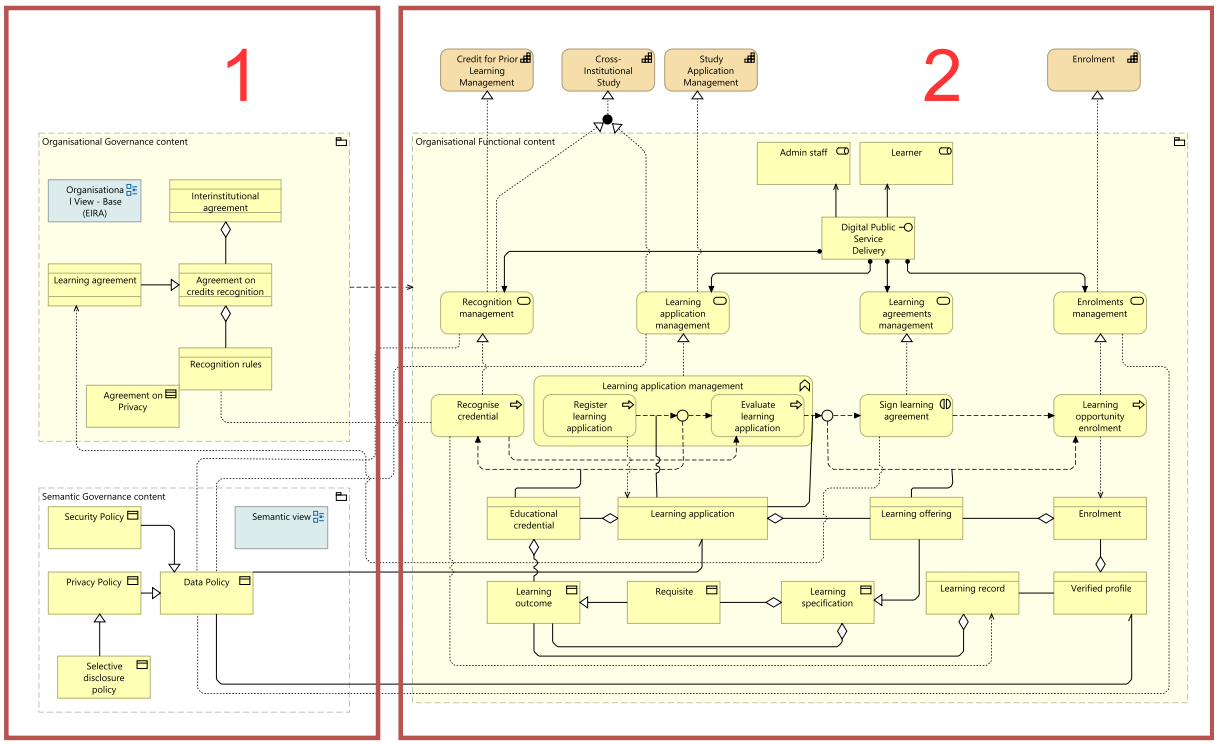


Figure 17 use case 2 (Apply and get recognition) - organisational view.
© 2025 European Union.

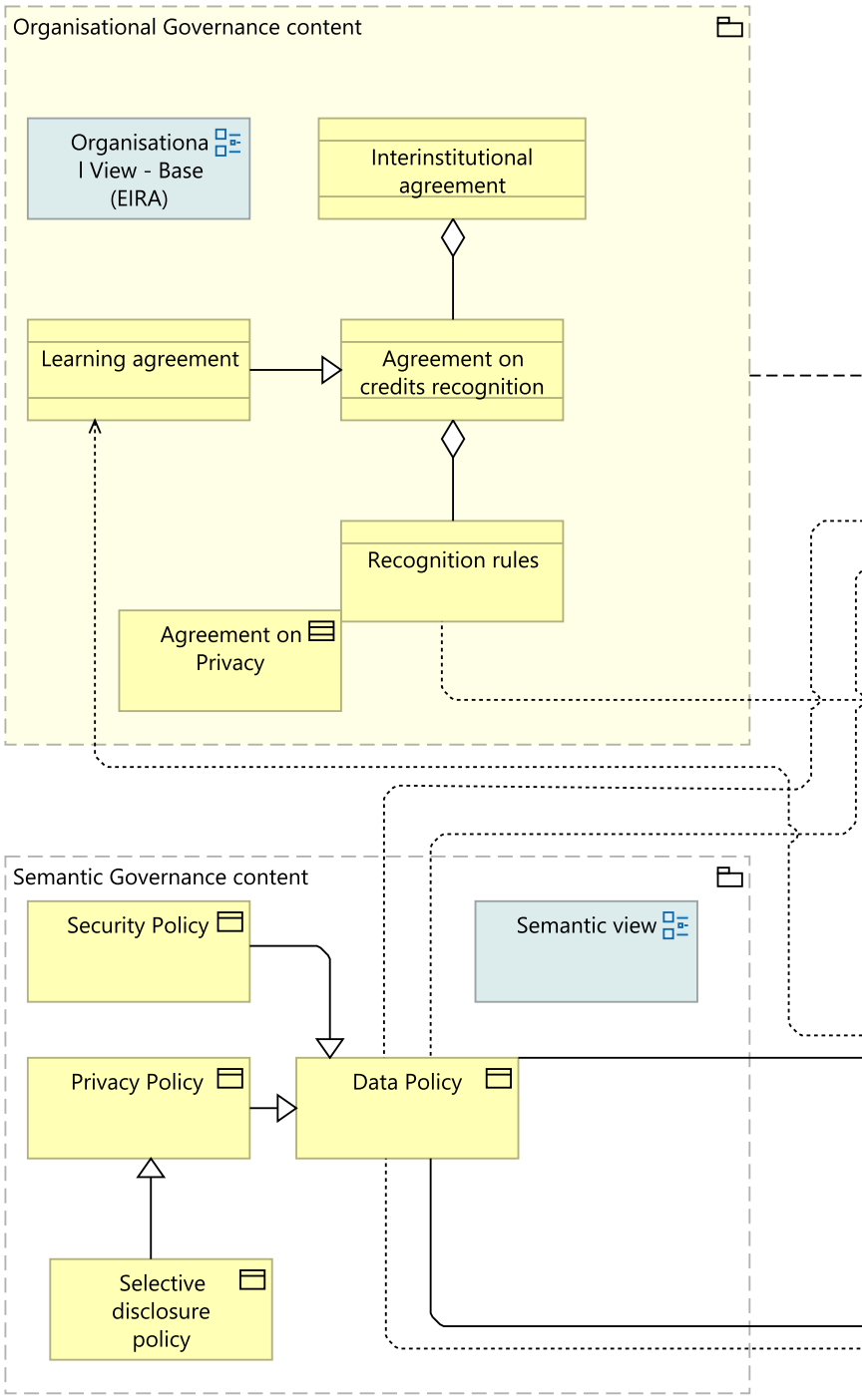


Figure 18 use case 2 (Apply and get recognition) - organisational view - part 1.
© 2025 European Union.

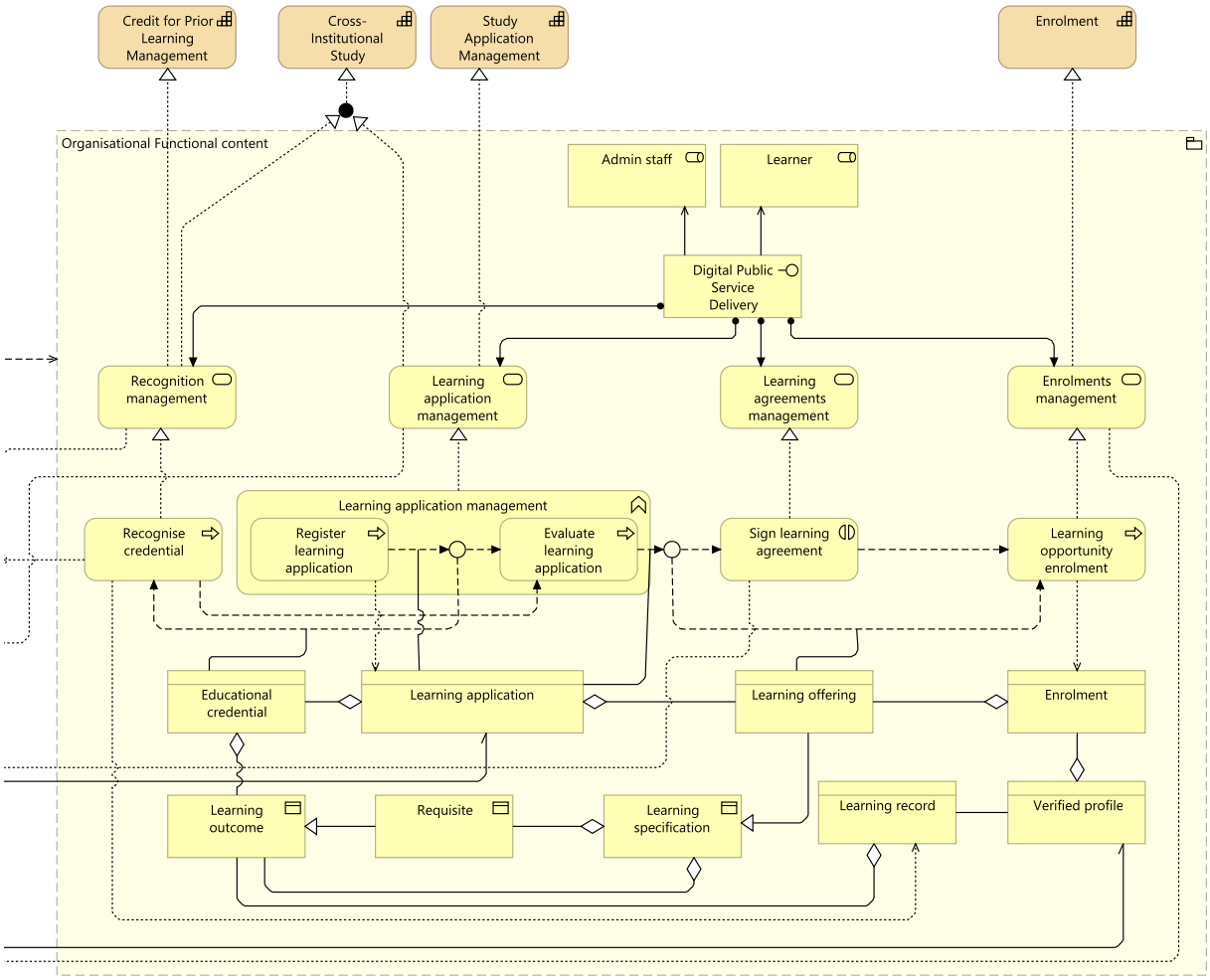


Figure 19 use case 2 (Apply and get recognition) - organisational view - part 2.
© 2025 European Union.

For this use case, aligning with the draft architecture, four main capabilities are identified: 1. credit for prior learning management; 2. cross-institutional study; 3. study application management; and 4. enrolment. All these capabilities relate to enrolling learners across various institutions. This includes recognising credits from other institutions. The previous diagram shows the organisational layer, where related services implement these capabilities through an interface.

Key elements and potential pain points involve the agreements between institutions during enrolment and the credit recognition process. Both can be challenging. They depend on trust between institutions and the possible lack of uniformity in learning outcomes.

In the following table, the most prominent building blocks are described.

Building block	Type	Description
Credit for prior learning management	Capability	The credit for prior learning management receives, assesses, and responds to applications for credit, recognising equivalent prior study or experience.
Cross-institutional study	Capability	The cross-institutional study manages formal study away from the home institution.
Study application management	Capability	The study application management receives, assesses, and responds to applications to study.
Enrolment	Capability	Enrolment manages students' formal registration in curriculum elements.
Recognition rules	Business object	Recognition rules are used for the recognition of credits from institutions other than the one where the student originates.
Agreement on credits recognition	Contract	The agreement on credits recognition aggregates recognition rules. This contract represents the agreements between institutions regarding the recognition of specific credits.
Interinstitutional agreement	Contract	The interinstitutional agreement aggregates agreements on credit recognition. This contract outlines agreements between institutions for recognising credits in joint programmes.
Agreement on privacy	Contract	The agreement on privacy sets rules for how public administrations collect, process, and transfer personal data of individuals.
Recognise credential	Business process	The recognise credential determines whether an education credential of previous learning activities meet the requirements to be recognised by the institution.
Learning application management	Business function	The learning application management involves two key business processes: 1. registering a learning application and 2. evaluating it. These processes work with credential recognition. They are the first step before a learner can enrol.

Sign learning agreement	Business interaction	The sign learning agreement implements the learning agreements management service. This business interaction happens before the learner enrols. It includes signing interinstitutional agreements.
Learning opportunity enrolment	Business process	The learning opportunity enrolment is the last step in a learner's enrolment. This process updates the enrolment business object. The verified profile business object then aggregates this, representing the learner.
Educational credential	Business object	An educational credential is an attestation, evidence or proof of qualification, activities, assessments, or entitlements.
Learning outcome	Business object	A learning outcome is a statement about what a learner knows and can do after finishing a learning process. This includes their knowledge, skills, responsibilities, and independence.
Selective disclosure	Business object	The selective disclosure policy regulates the access to personal data of any actor interacting with the systems. Each business process that needs access to personal data must include the minimum required attributes. Based on EIF: Recommendation 13. Users should be asked to provide only the information that is absolutely necessary to obtain a given public service.

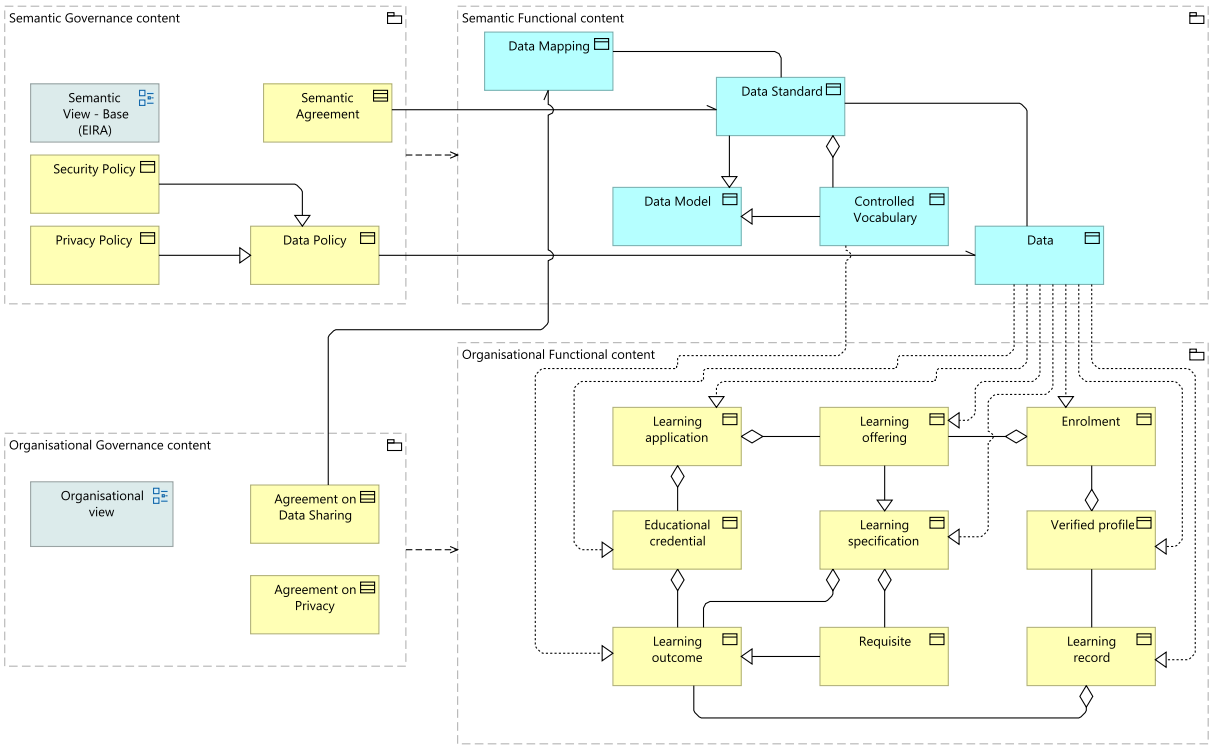


Figure 20 use case 2 (Apply and get recognition) - semantic view.
© 2025 European Union.

For Use Case 2, the view of the semantic layer highlights the agreements on the standards used to define learning outcomes, learning offerings, and learning specifications. A pain point in this architecture is that agreements require well-defined and interoperable learning outcomes, which can be challenging to achieve when different institutions need to reach consensus. The recommendations section provides more details on making learning outcomes more interoperable.

In the following table, the most prominent building blocks refined during the first squad series are described.

Building block	Type	Description
Semantic agreement	Contract	A semantic agreement formalises an agreement from a peer to the common ontology. This ontology results from a matching or mapping process used to resolve semantic discrepancies. The combination matching process includes a linguistic base and compares internal and external structures. The outcome of this matching process will help create an agreement unit, which is a key component of the agreement.
Data standard	Data object	A data standard guides the organization, integration, and management of data. It includes data models, formats, protocols, and other technical specifications. These ensure data consistency, interoperability, and efficient data exchange.
Agreement on data sharing	Contract	An agreement on data sharing outlines the information needs, syntax rules, protocols, and semantic artefacts for data exchange.
Agreement on privacy	Contract	The agreement on privacy sets rules for how public administrations collect, process, and transfer personal data of individuals.
Controlled vocabulary	Data object	A controlled vocabulary offers a set of chosen terms to describe concepts or objects in a specific field. It is a standardised list of terms. It ensures consistency and accuracy in indexing, searching, and retrieving information.

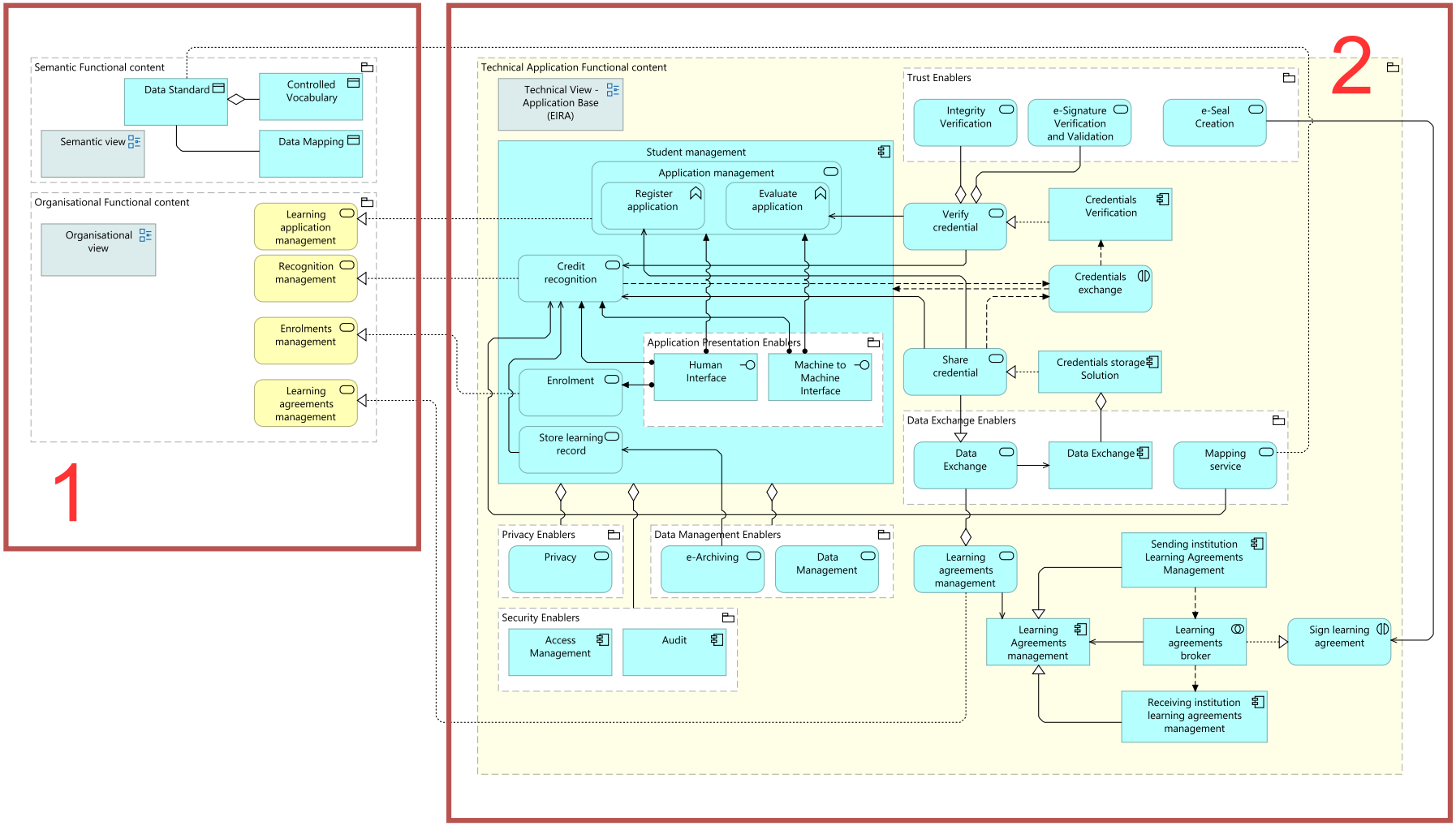


Figure 21 use case 2 (Apply and get recognition) - technical view.
© 2025 European Union.

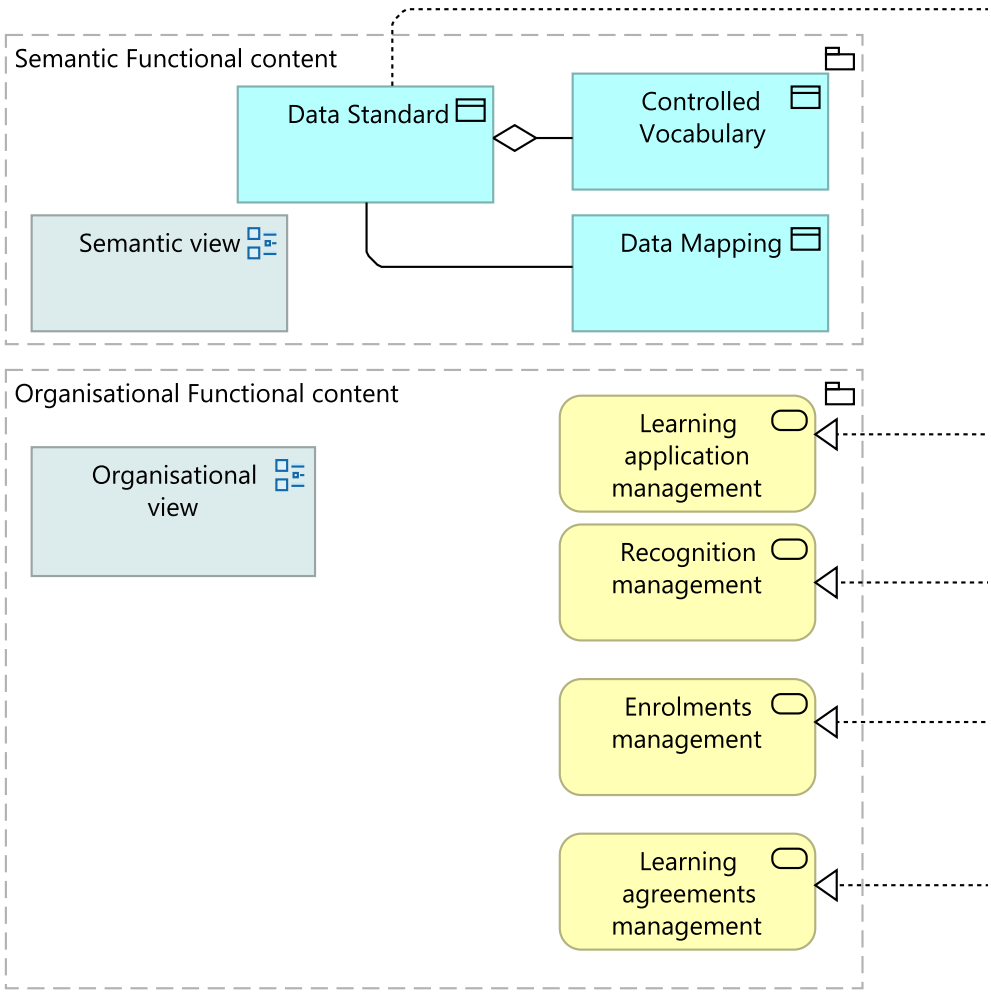


Figure 21 use case 2 (Apply and get recognition) - technical view.

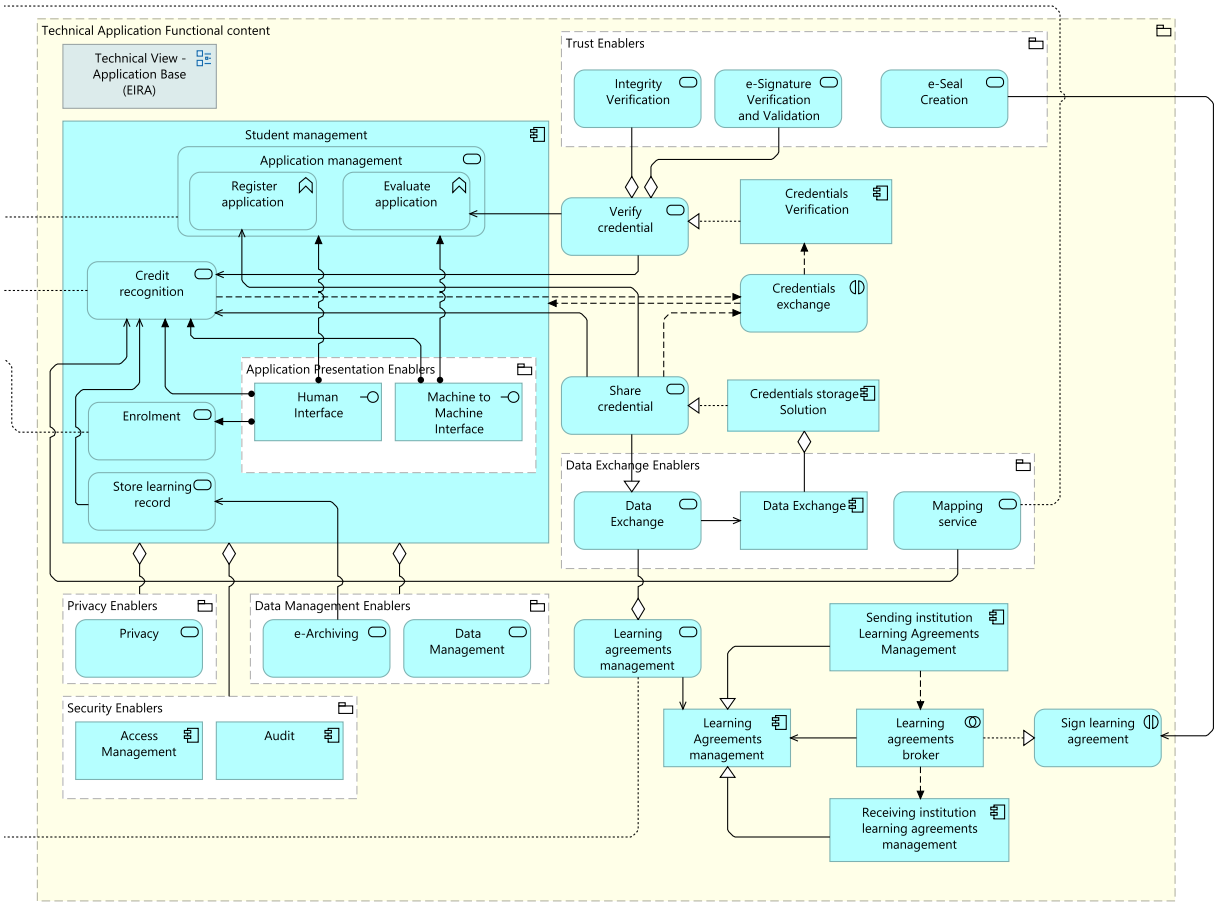


Figure 23 use case 2 (Apply and get recognition) - technical view - part 2.
© 2025 European Union.

In the application view of use case 2, several groupings can be distinguished by their function. Multiple types of enablers are defined according to their field: those related to trust management, data exchange, privacy, security, and data management. Besides these enablers, there is the student management block. It has services for enrolment and credit recognition, which are shown through interfaces. These application ABBs are also linked to their counterparts in the business layer.

The following table describes the most prominent building blocks refined during the first squad series.

Building block	Type	Description
Trust enablers	Grouping	Trust enablers help secure cross-border transactions and interactions.

Integrity verification	Application service	The integrity verification ensures that information remains unaltered since creation, transmission, or storage.
E-signature verification and validation	Application service	The e-signature verification and validation verifies and confirms the validity of electronic signatures or seals.
E-seal creation	Application service	The e-seal creation enables signing data in electronic forms on behalf of a legal entity.
Verify credential	Application service	The verify credential ensures the claims in a credential are valid.
Credentials verification	Application component	The credentials verification ABB verifies user credentials during the evaluation process. It uses the verify credentials service for this task.
Credentials exchange	Application interaction	The credentials exchange ABB is an application interaction that describes how credentials are shared and recognised in the learner's application.
Credentials storage solution	Application component	A credentials storage solution provides a secure way to store credentials, whether they are conventional or wallet-type.
Data exchange enablers	Grouping	Digital exchange enablers ABB are tools or components that facilitate data exchange between systems or applications.
Data exchange	Application service	A data exchange enables secure exchange of messages, records, forms, and other data between individuals, organisations, or systems. It includes data routing but excludes endpoint discovery.
Learning agreements broker	Application collaboration	The learning agreements broker is an application collaboration that synchronises the agreements among all parties involved in the learner's application process.
Sign learning agreement	Application interaction	The sign learning agreement is conducted by the learning agreement broker. This interaction involves the signing of agreements by all parties involved in the learner's application process.
Privacy enablers	Grouping	Privacy enablers are components and services that support privacy-related functionality within applications or systems.
Security enablers	Grouping	Security enablers are components help implement and manage security controls, protecting digital assets and information from cyber threats.

Data management enablers	Grouping	Data management enablers are components and services that support effective data management practices and procedures.
Student management	Application component	The student management implements services related to the learner's application workflow, accessible through various interfaces.
Application presentation enablers	Grouping	Application presentation enablers support the creation of visually appealing and interactive user interfaces for software applications.

For more information about the ArchiMate building blocks in this diagram, refer to the blueprint reference architecture report. It contains all the relevant details regarding these schemes.

2.5 Interoperability required capabilities

Adapting to the above proposed approaches requires certain interoperability capabilities. To start, all data objects requiring standardisation will be defined.

Data standards play a major role in semantic interoperability. The chosen data standard should meet a set of metadata and attribute requirements that facilitate communication between systems. Each data object contains a minimum set of relevant data identified as key values that the selected standard should include.

One of the main data objects, part of the process of application and getting recognition, is the application itself. The application must have at least a standard on the learner's attributes to be mapped with the requisites of the learning offering.

To validate the application and check compliance with learning offering prerequisites, you need their standards and a set of recognition rules and agreements. These recognition rules and agreements must follow their own standards to ensure both institutions in a joint programme scenario follow the same criteria.

For more information on the interoperability capabilities of this use case, please refer to the comprehensive final mapping report.

2.6 Recommendations – use case 2

Within the learner's path flows included in use case 2, several pain points have been identified and highlighted throughout this chapter. Based on the feedback collected thus far, a set of recommendations will be defined to address these. These recommendations aim to improve the processes in alignment with the interoperability goals of the institutions involved, tackling the challenges.

One of the most important challenges identified for this use case is credit recognition. This is because different institutions do not trust each other, due to some institutions being unclear about their internal processes. Moreover, there is no standard definition for learning outcomes. Here are a few recommendations to help tackle the problem:

- **Use a common ontology and controlled vocabulary**, as suggested for use case 1. This will help align key data goals, such as credentials, applications, and recognition rules. This will also support use case 2 by promoting consistent use of shared tools across processes related to applying for and recognising learning achievements.
- **Introduce micro-credentials into recognition processes** to validate prior learning and skills flexibly. Institutions should issue micro-credentials that align with European standards like Europass and EQF. This will ensure portability and interoperability. These credentials must fit into the credit recognition workflow. They should provide clear and verifiable evidence of skills and achievements. This evidence will support decisions about mobility and admissions.
- **Streamline recognition agreements** by adopting standardised frameworks and formats. This approach will reduce administrative barriers and foster trust between institutions.
- **Establish digital trust and transparency through institutional policies and recognition rules**, as this is key to building trust. Institutions should focus on secure digital credentials and e-signatures. These tools help verify shared data and ensure it is authentic, streamlining processes and build confidence in credit recognition decisions.
- **Pilot and scale interoperability methods** to find more challenges. Refine processes and help scale successful models across institutions and alliances. This ensures effective and efficient implementation.

This is not a strict recommendation, but it is worth considering when developing this use case. It can help institutions boost their visibility to students from other places.

In 2018, the **Single Digital Gateway (SDG)** regulation was approved to facilitate online access to information. The SDG is an EU initiative that offers a central online platform. This platform helps citizens and businesses access information, complete procedures, and get assistance in EU member states. It works with **Your Europe**, a website that provides practical guidance on rights, rules, and processes for living, studying, working, or doing business in the EU. For universities, these tools are vital for improving accessibility and efficiency, especially for international applicants. Through **Your Europe**, potential students can easily find information on course requirements, application steps, and qualification recognition across EU countries. The **SDG** makes tasks like submitting documents or verifying credentials simpler, ensuring a smoother experience for students applying to study abroad.

By reducing barriers and streamlining processes, the SDG and **Your Europe** promote mobility. They make it easier for students to explore educational opportunities in Europe, while helping universities attract a diverse and talented student body.

PART 3

Use case 3 – Access tools

3 Use case 3 – Access tools

USE CASE 3

Access tools

Streamlining the management and governance of shared resources among alliance members, covering both physical and virtual assets.

Laboratory access | Library systems | Research tool registry

3.1 Use case definition

The ability to access tools is fundamental to learning. The 'access tools' use case is closely tied to traditional IT Service Management (ITSM). Its goal is to simplify how alliance members procure, manage, and govern shared resources. This includes both physical and virtual resources. This use case heavily relies on use case 7 - User identity.

So far, findings revealed that discoverability is not a priority for alliances at present, as the number of requests is still manageable through local and manual processes. As alliances work on interoperability, sharing tools will become more common. This is especially true in joint programme scenarios. Moreover, being able to expose assets can be crucial for institutions and alliances focused on research as part of their institutional identity.

3.2 High-level flow

This use case focuses on the mechanisms for sharing and accessing resources. To fully define it, we must outline the processes for managing the catalogue of available resources and the steps required to discover and access them.

The scenarios described earlier in this document affect the steps needed to manage user access. This includes users with specific roles or those enrolled in learning opportunities that require particular tools for learning

activities. However, access rights management is covered in **use case 7 – user identity**. As a result, high-level flows and reference architecture diagrams do not detail these scenarios but instead refer to **use case 7**.

There are two main approaches: First, a **central catalogue approach**. A central catalogue stores metadata about the tools shared by each institution. A **catalogue operator** manages this information, but institutions remain responsible for handling requests and granting access rights to users. Second, a **decentralised approach**. This approach requires additional steps to make tools searchable. The discovery service must send requests to all institutions sharing resources, collect the responses, and merge them before presenting the results to the user.

As the architecture section will show, both solutions have their strengths and weaknesses.

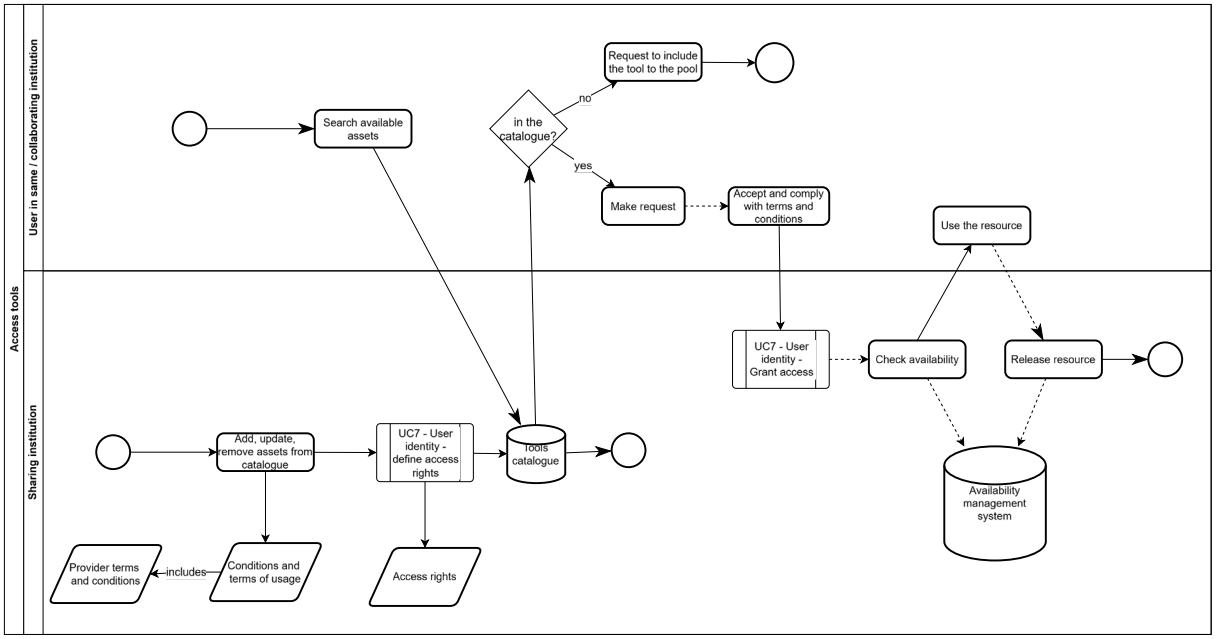


Figure 24 - Steps required to share and manage access to shared resources.
© 2025 European Union

The first step is defining the process for making a resource available. Institutions sharing resources may choose a subset of tools to share. These tools typically have licences that outline their terms and conditions of use. In addition, sharing institutions may apply specific access rules. Defining access rights is a key part of sharing a resource. Once a resource is fully described, it can be added to the tools catalogue. If the selected approach includes a central catalogue, the sharing institution sends the tool description for publication. Otherwise, once the tool is listed in the local catalogue, it will appear in future searches.

Users searching for tools or assets use a discovery service, which either queries local catalogues or accesses the central one, depending on the chosen approach. This process should remain transparent for the user. A new tool can also be added through a local request process. Since this process is managed within each institution and does not introduce interoperability challenges, it falls outside the scope of this project.

Once a user finds a tool, the sharing institution manages the request and grants access. At this stage, different scenarios may apply: Some cases require individual evaluation. For example, an educator may request access to test a tool before integrating it into a learning opportunity. Other cases do not need individual evaluation and can be automated. For instance, software tools available to all registered users or learning specifications that require a particular tool for a specific role. Learners enrolled in a programme linked to such a specification must be granted access to the necessary tools. The specifics of managing user permissions and roles are detailed in use case 7.

Availability management and related processes are handled locally and do not require seamless communication. However, these steps are included in the diagram to emphasise that some tools may involve additional local procedures when access is granted, such as quota restrictions.

3.3 Draft architecture

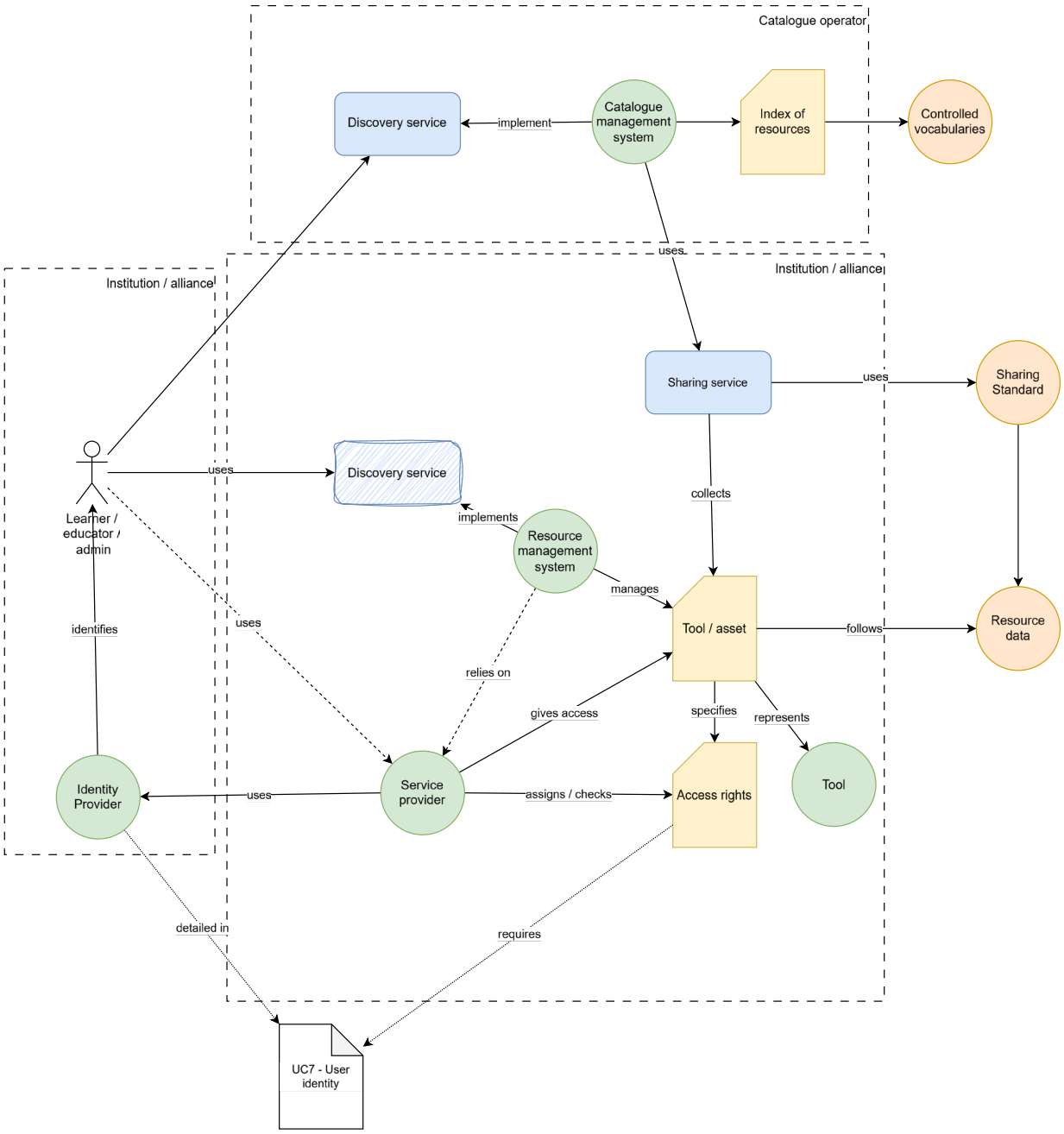


Figure 25 - Overview of components required to manage a repository of discoverable and shareable assets.
© 2025 European Union

Data objects:

- **Tool / asset:** A tool, software package, laboratory equipment, or any other physical or virtual asset available within an institution.
- **Access rights:** A set of permissions required to use a tool. Different users may need different access rights depending on their role. Administrators may require special permissions to manage requests or modify configurations. Students may need read-only access to certain tools. Details on access rights and their management are covered in use case 7.
- **Index of resources:** A collection of assets available for sharing. It includes details about each tool and how to access it.

A sharing service collects data from assets and makes it available according to the sharing standard. This process can be complex, as some tools have built-in management systems, while others rely on manual processes, leading to customised approaches.

As mentioned earlier, alliances take different approaches to managing resources. A **centralised approach** incorporates a central catalogue that stores standardised information. A **catalogue management system** maintains an index of available tools and providing a **discovery service** for search. The **decentralised approach** requires each institution to maintain its own local catalogue and discovery service. At present, no formal discovery services exist. Educators work based on past experiences and collaborations with colleagues from other institutions.

Requesting access to a tool follows a local process and is not included in the reference architecture. The process for granting access depends on the type of asset and its management system. **Physical resources** may require users to obtain an access card from a service desk at the institution. **Virtual or digital assets** can integrate with the identity management system described in use case 7 to assign access rights.

3.4 Reference architecture

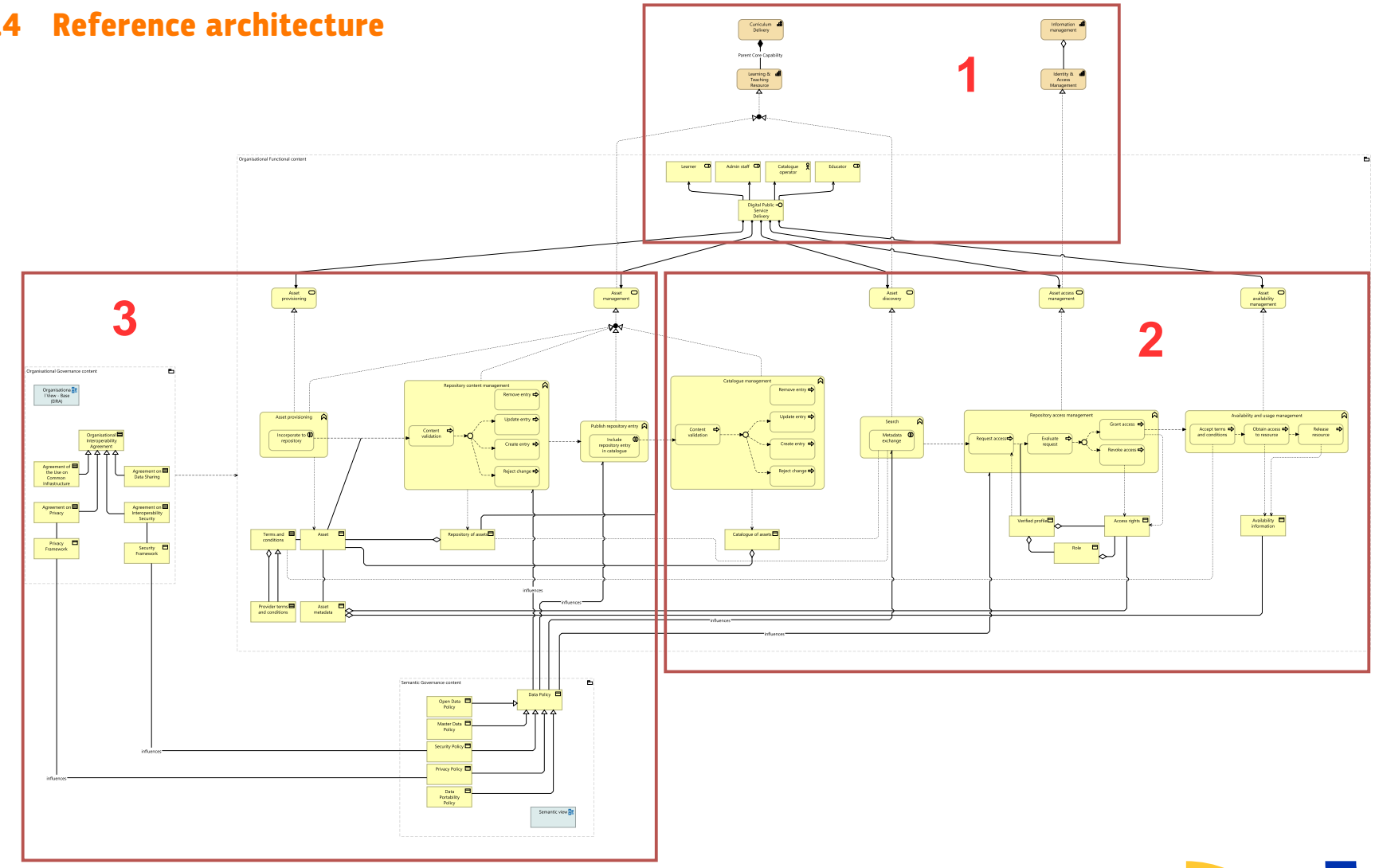


Figure 26 use case 3 (Access tools) - organisational view overview.

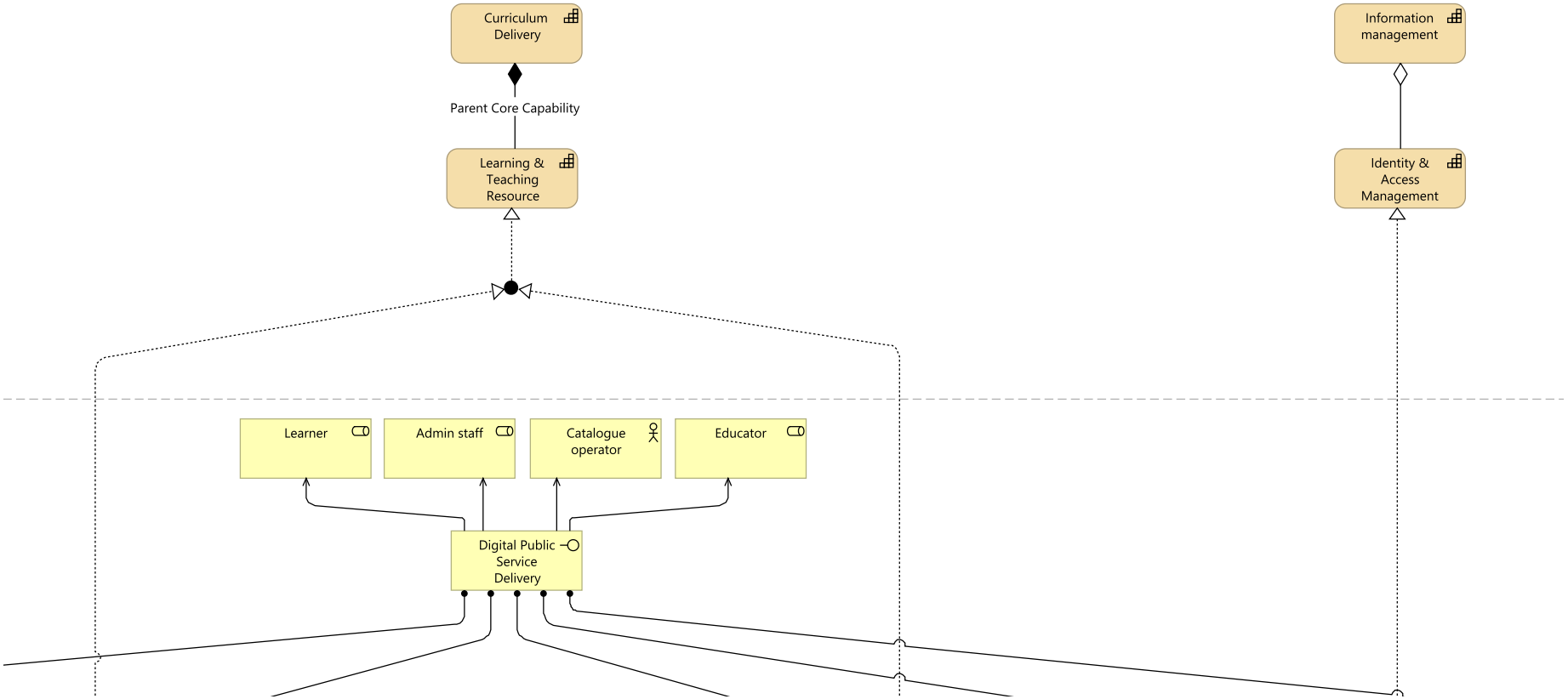


Figure 27 use case 3 (Access tools) - organisational view - part 1.

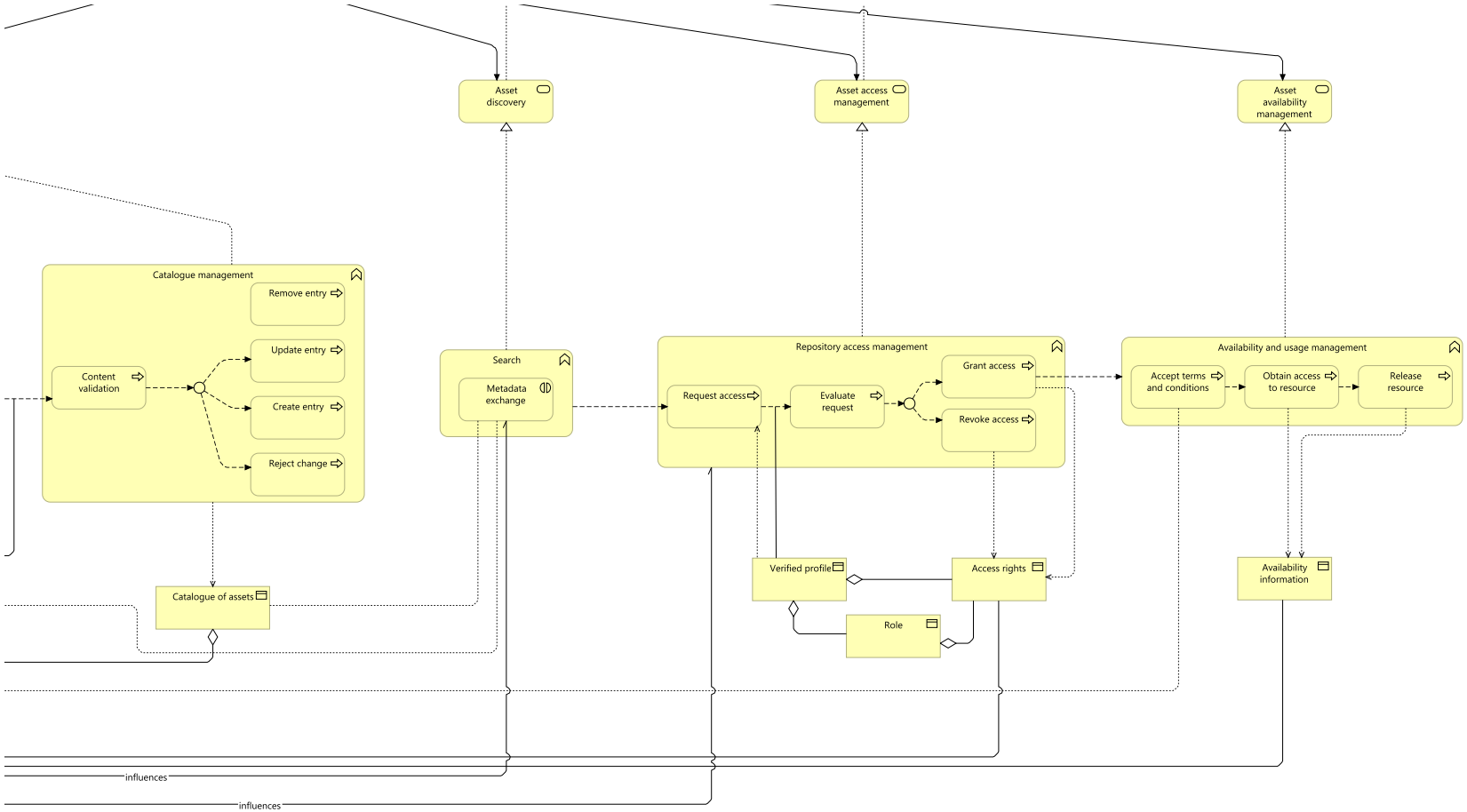


Figure 28 use case 3 (Access tools) - organisational view - part 2.

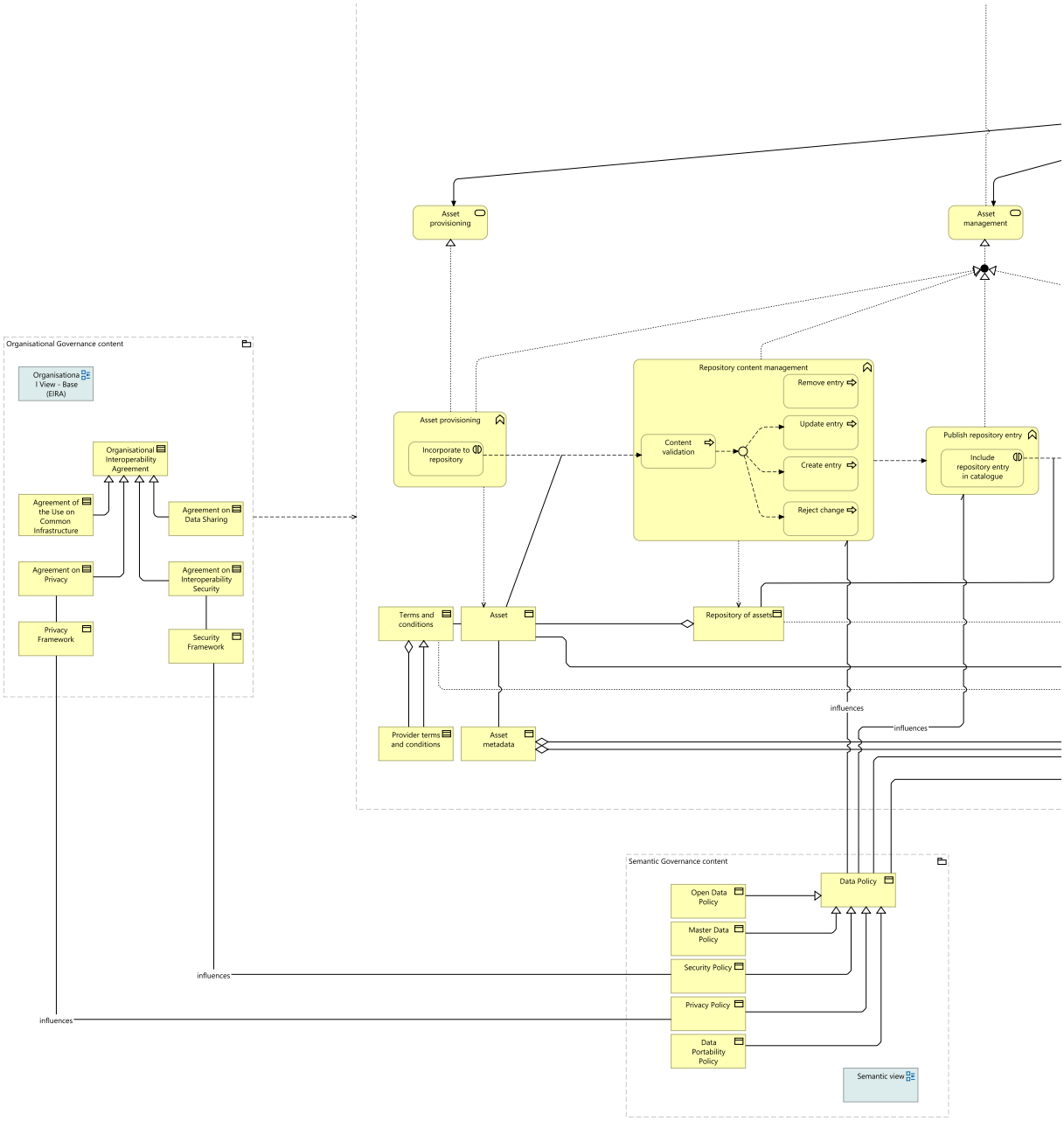


Figure 29 use case 3 (Access tools) - organisational view - part 3.
© 2025 European Union

In the organisational view diagram, the necessary capabilities for this use case can be identified. A key element is the learning and teaching resource, which is part of ***curriculum delivery***.

From a business logic perspective, the main interface for this use case is a digital public service delivery, which must implement the following business services: *Asset provisioning, asset management, asset discovery, asset access management and asset availability management*.

These services are carried out through their related functions and processes. They are shaped by the required data policies and agreements.

In the following table, the most prominent building blocks are described.

Building block	Type	Description
Curriculum management	Capability	The curriculum management manages and operates an institution's curricula.
Learning and teaching resource preparation	Capability	The learning and teaching resource preparation acquires, assembles, or creates learning materials resources. This includes artefacts such as books and excerpts, documents, X-Reality experiences, 3D models and prints, and video presentations, and so forth.
Asset	Business object	An asset is a physical or digital resource managed by an institution.
Access rights	Business object	Access rights govern who can view, edit, or delete data, ensuring confidentiality, integrity, and availability.
Availability information	Business object	Availability information indicate whether or not an asset is available
Verified profile	Business object	A verified profile is a representation of a learner, educator or administrative staff related to an institution.
Terms and conditions	Contract	Terms and conditions are a legal agreement between an institution and the end user of an asset. Provides a set of conditions to make use of an asset.
Provider terms and conditions	Contract	The provider terms and conditions are a legal agreement between an institution and the end user of an asset. Provides a set of conditions to make use of an asset.
Metadata exchange	Business interaction	The metadata exchange facilitates system communication for searching across repositories.

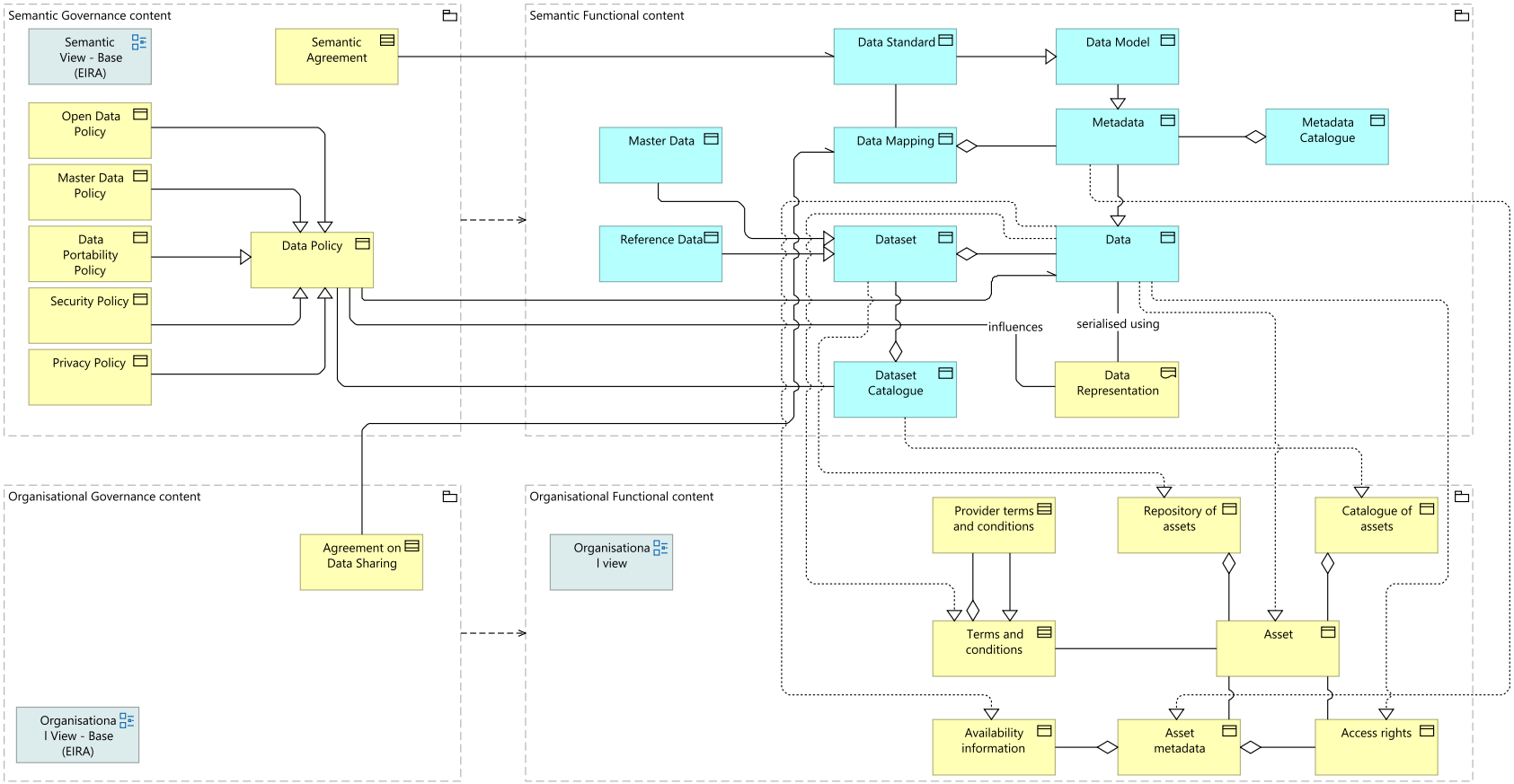


Figure 30 use case 3 (Access tools) - semantic view.

As highlighted in use case 2, agreements play a key role in the semantic layer of use case 3. A key issue in this architecture is managing terms and conditions. This use case focuses on tools and sharing, so it is important to find a collective and interoperable solution.

In the following table, the most prominent building blocks are described.

Semantic agreement	Type	Description
Semantic agreement	Contract	A semantic agreement is a contract between a peer and the common ontology, resulting from a matching or mapping process that resolves their semantic discrepancies. This process combines linguistic base, internal and external structure comparison. The resulting match is used to develop an agreement unit, a component of the agreement. The agreement rests on some key assumptions. First, everyone must use the same language for the schema, ontology, labels, and meanings. Also, there should not be personal views in the shared ontology.
Data model	Data object	A data model is a collection of entities, their properties, and how they relate. It aims to represent a domain, a concept, or something in the real world.
Data standard	Data object	A data standard is a predefined structure that guides the organization, integration, and management of data. It includes data models, formats, protocols, and other technical specs. These ensure data stays consistent, works well together, and exchanges efficiently.
Metadata	Data object	Metadata provide information about one or more aspects of the data.

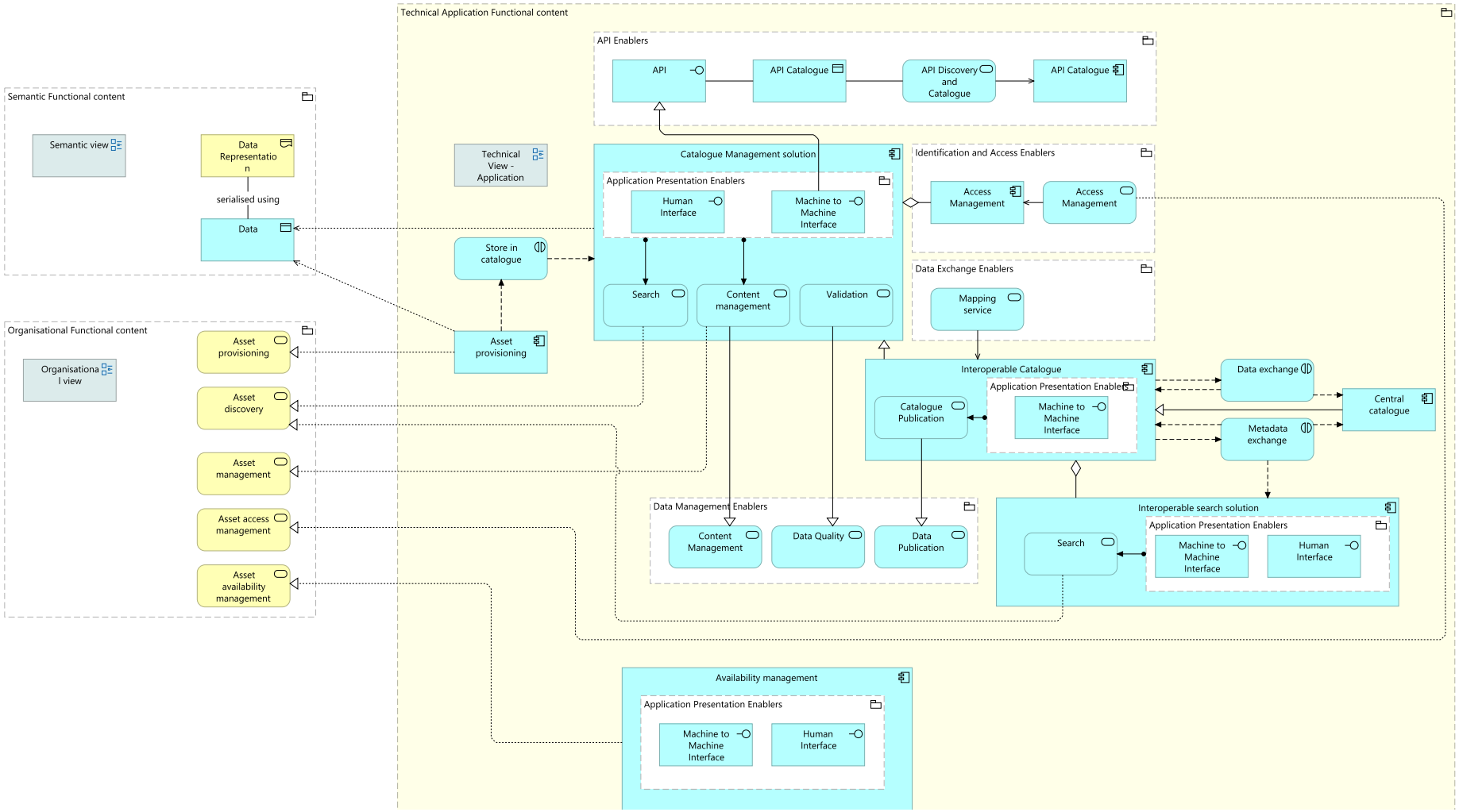


Figure 31 use case 3 (Access tools) - technical view.

Since this use case is primarily understood as a catalogue of tools, the key focus is searching and usage. This is where standards and metadata play a crucial role. The essential building blocks for the technical layer will be detailed below.

Building block	Type	Description
Catalogue management solution	Application component	The catalogue management solution helps manage data in a catalogue. It handles storage, validation, publication, and retrieval. This makes it easier to discover data.
Interoperable catalogue	Application component	The interoperable catalogue supports the exchange of data between different catalogues.
Data exchange	Application component	The data exchange enables the transfer of data between interoperable catalogues. This includes data such as courses and assets.
Metadata exchange	Application interaction	The metadata exchange enables validation and search functionality through metadata sharing.
Catalogue publication	Application service	The catalogue publication makes learning opportunities, assets, and educational resources accessible and reusable.
Search	Application service	Search enables users to discover, filter, and organise learning opportunities and assets.
Validation	Application service	Validation ensures data accuracy, completeness, and consistency before publication.

For further details on ArchiMate building blocks, please refer to the blueprint reference architecture report.

3.5 Interoperability required capabilities

To make tools searchable, they must be characterised. Alliances have emphasised the need for a common data standard. Without a standard, institutions must rely on agreements defining the data model to be used.

Beyond data models, a sharing standard is also needed so users understand how to request access. A common inventory of tools across institutions would help. This could avoid having too many licences for a tool, unlike other cases where the required quota barely covers the expected number of uses. From the Alliance's perspective, it is also interesting to showcase the full potential that can be offered to researchers and learners.

For more information on the interoperability capabilities of this use case, please refer to the comprehensive final mapping report.

3.6 Recommendations – use case 3

- **Adopt a common approach and controlled vocabularies for tool discovery:** Using controlled vocabularies makes tool search and filtering simpler. Standardising terminology improves discoverability across alliances. Beyond technical alignment, a cultural shift is necessary. Institutions should agree collectively on and adopt common standards. This allows tools to be shared beyond the traditional boundaries of a Higher Education Institution (HEI).
- **Minimise data exposure by sharing metadata:** When implementing systems to manage shared tools, it is essential to prioritise metadata sharing over full datasets. This approach reduces security risks and improves system performance. It also ensures that licensing and data protection policies are followed. This helps institutions keep control over sensitive information. At the same time, it allows for effective discovery and access.
- **Promote standardised access protocols and centralised tools catalogues:** Institutions and alliances should adopt standardised protocols for granting access to shared tools. Ensure end users have a seamless experience. Consider creating centralised tool catalogues to aggregate metadata, improve accessibility, and reduce redundancy. A centralised approach should be scalable, allowing institutions to share efficiently while optimising resources. It should also encourage institutions to share responsibility and be mutually accountable.

PART 4

Use case 4 – Manage educational resources

4 Use case 4 - Manage educational resources

USE CASE 4

Manage educational resources

Promoting the accessibility and mobility of educational materials, fostering a collaborative and accessible educational environment.

Content generation | Sharing | Use and re-use

4.1 Use case definition

It is crucial that educational resources can be easily presented on various platforms. Therefore, decoupling the resource from the platform is valuable. This use case concentrates on the ability to co-create a resource and then access and share these educational materials. This fosters collaborative and accessible educational environments. Typically, a learning management system has the capability to create and/or export educational resources.

4.2 High-level flow

This use case builds on use case 3 (access tools). Educational resources are designed to work with a specific tool. Before creating the content, educators or learners co-creating it select the tool. The specific steps for creating content are not shown in the high-level flow, as they vary between institutions.

Once the educational resource is created, it needs to be classified and characterized with metadata to make it searchable. Controlled vocabularies and sharing standards are crucial in this process. Educational resources registries, called content pools in the diagrams, use a specific data model. They can hold data created long ago and follow various methods to classify and describe educational resources. This raises an interoperability issue, as harmonizing existing methodologies can be complicated.

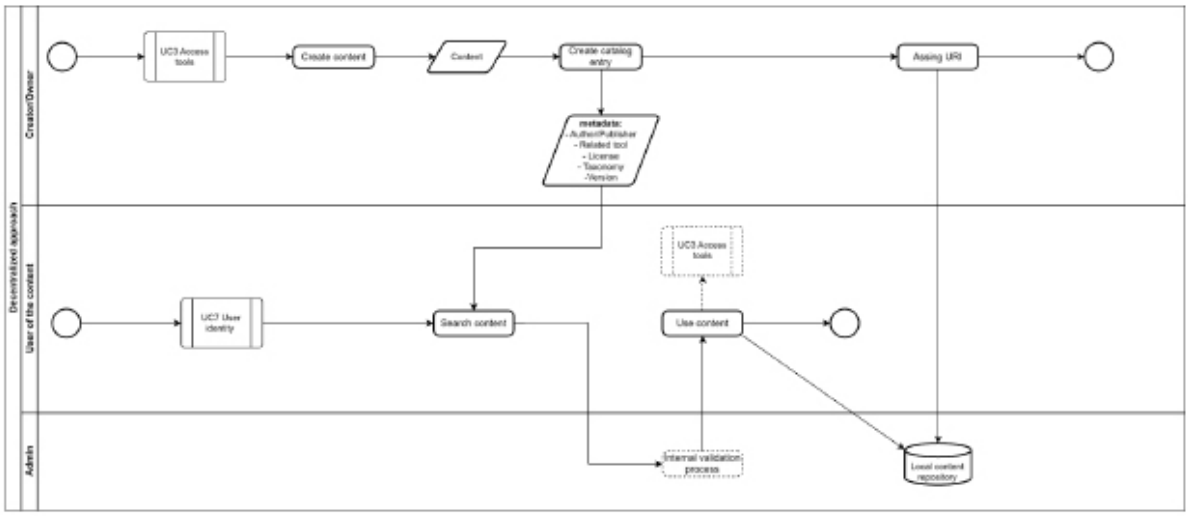


Figure 32 - Overview of the steps required to share and discover educational resources following a decentralised approach.
© 2025 European Union

If the alliance adopts a decentralised approach, sharing educational resources begins once the catalogue entry is created and the content is added to the registry. This approach complicates the discovery phase. Users must gather information from various systems. Alternatively, alliances can create a discovery service to collect and streamline data before showing it to users. After searching for the content, the user's request to use it goes through each institution's internal processes, which determine whether access to the resource is granted or not.

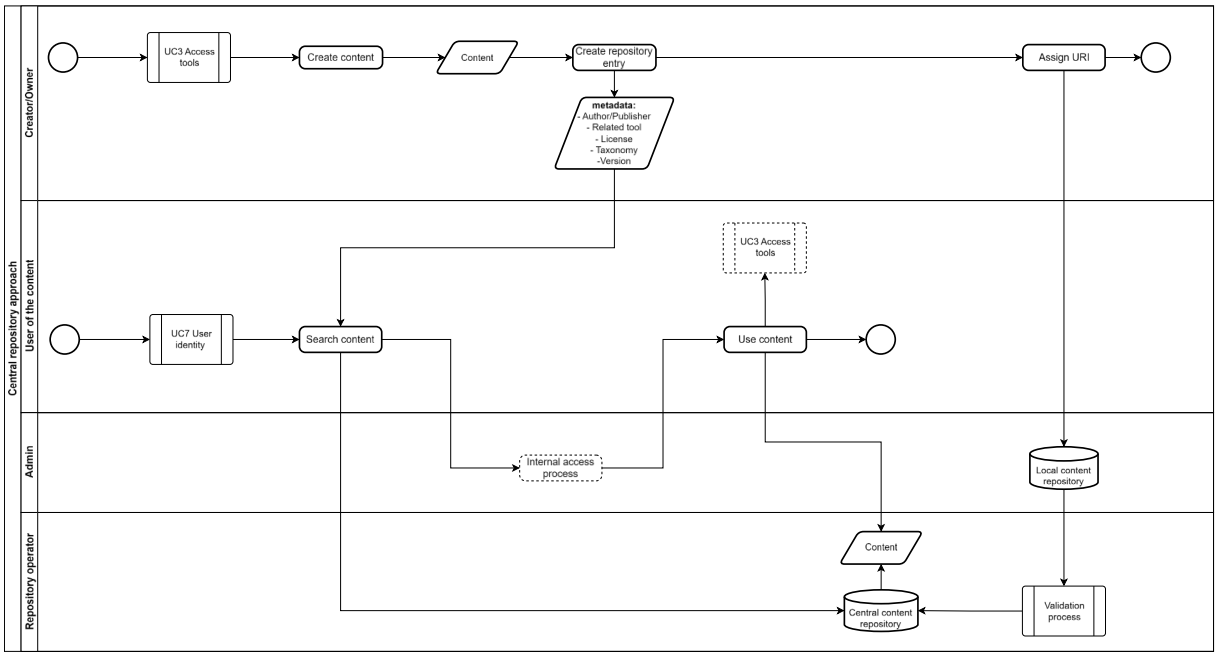


Figure 33 - Overview of the steps required to share educational resources following the central catalogue approach.
© 2025 European Union

Institutions using the centralised approach must make their educational resources available on the central catalogue. This involves translating from their local model into the shared standard vocabularies.

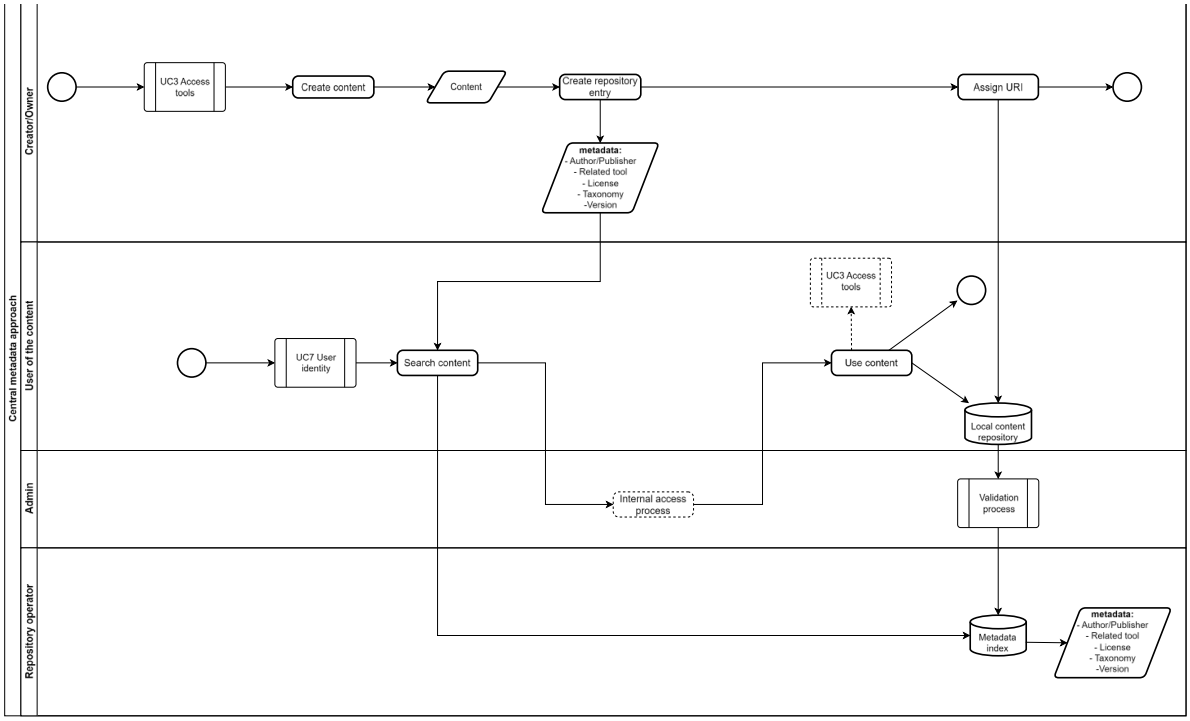


Figure 34 - Overview of the steps required to share and discover educational resources following a decentralised metadata approach.
© 2025 European Union

Another approach emerging from the central repository during squad 4's working sessions is the central metadata repository approach. This central repository holds just the metadata of educational resources. This cuts down on storage needs and provides other benefits. It is also highly compatible with each institution's internal data protection and licensing policies. By storing only metadata, the original resource remains in the local repositories of the institutions, never leaving them. When a user searches for a resource and tries to access it, the request goes through a process at the institution. This process decides whether to grant or deny access.

4.3 Draft architecture

Educators design educational resources to match the learning specification in which they are involved. These resources are stored in a registry, making them discoverable by other educators or learners. To meet this requirement, the following main components are necessary:

Data objects and data standards:

- **Educational resource:** This includes any type of educational material. It also covers metadata attributes that describe and classify the resource completely.
- **Shared index of educational resources:** This is an index of educational resources.
- **Educational resource standard:** This standard outlines the features and terms used to describe educational resources.

Services and systems:

- **Mapping services:** Manage the translation of local registry data models into the educational resource standard.
- **Sharing service:** Sends information from a local registry by using the mapping service for translation. It can actively send data to a catalogue or collect it in real time, responding to external requests.
- **Validation service:** Verifies that the received information meets the data standard and minimum required attributes.
- **Search service:** Offers search functions to find educational resources. It uses the index of resources and controlled vocabularies to enable searches.

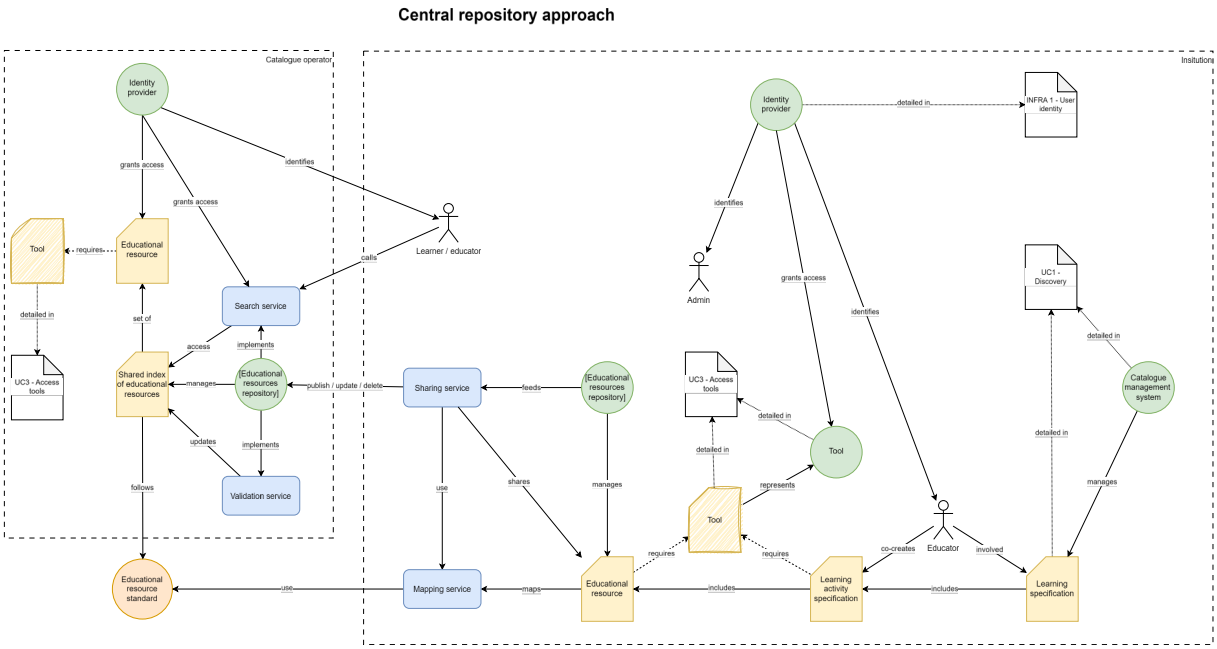


Figure 35 - Main components required to exchange educational resources with a central registry.
© 2025 European Union

The central repositories approach, as shown in Figure 35 above, can be implemented in two ways. If the central repository collects information from the local repositories, the sharing service must accept the request and update the central repository accordingly. The central repository's awareness of the HEIs' local repositories determines the limits. Data collection can be scheduled and based on available infrastructure.

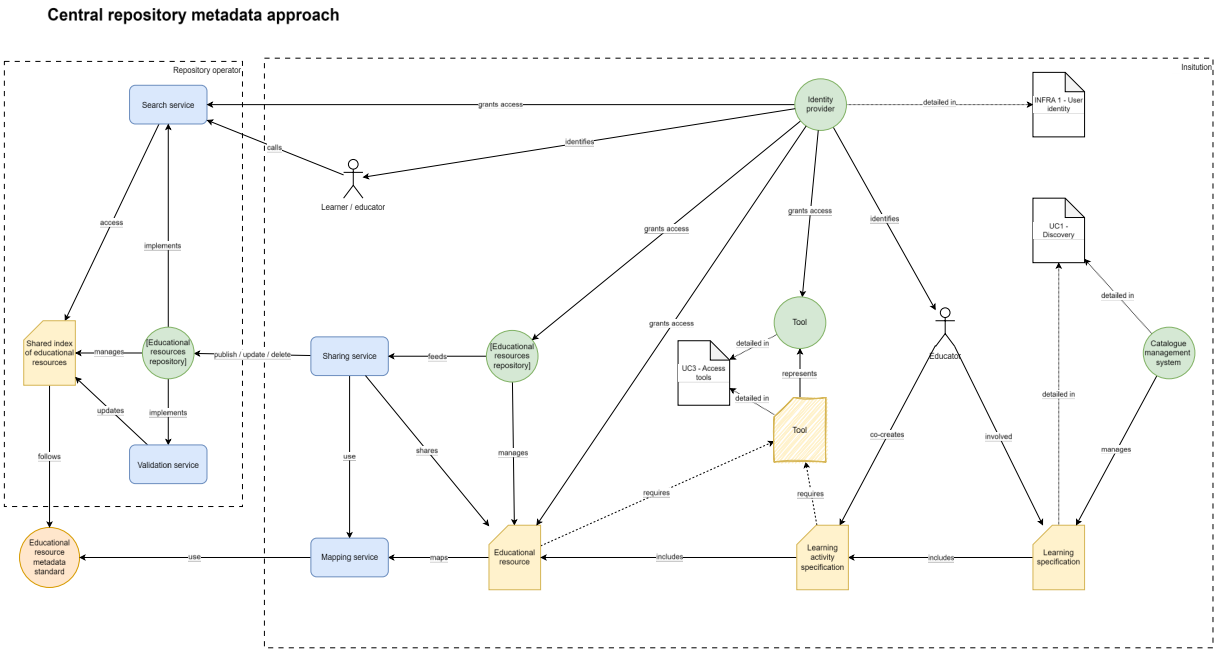


Figure 36 - Main components required to exchange educational resources with a central metadata registry.
© 2025 European Union

The main difference between the above diagram and the central repository approach is how access to the actual resource is managed. Here, the central repository's identity provider is replaced by local identity providers, who manage user permissions internally.

Decentralised repositories rely on local ones to gather and send data to the central repository. This might mean the central catalogue needs to scale up its infrastructure to manage all the updates.

In this approach, the central repository makes its search service available to end users.

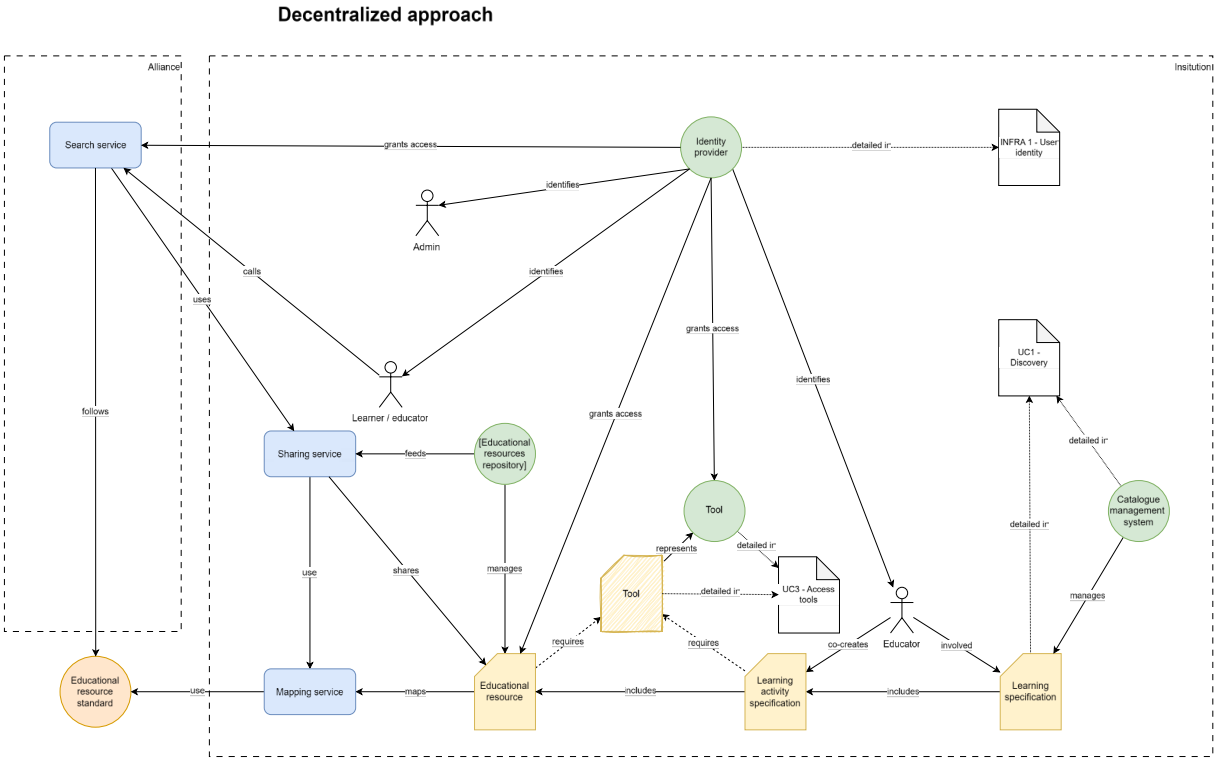


Figure 37 - Main components required to exchange educational resources following a decentralised approach.
© 2025 European Union

Data standards play a major role in semantic interoperability. The chosen data standard should meet a set of metadata and attribute requirements that facilitate the communication between systems.

In the decentralised approach, each repository must either follow the same data standard or implement a mapping service. This mapping service sends data in the required structure. End users can use the search features of each repository. Alternatively, the alliance may provide a central search service. This service collects and presents data from the local repositories to the user.

4.4 Reference architecture

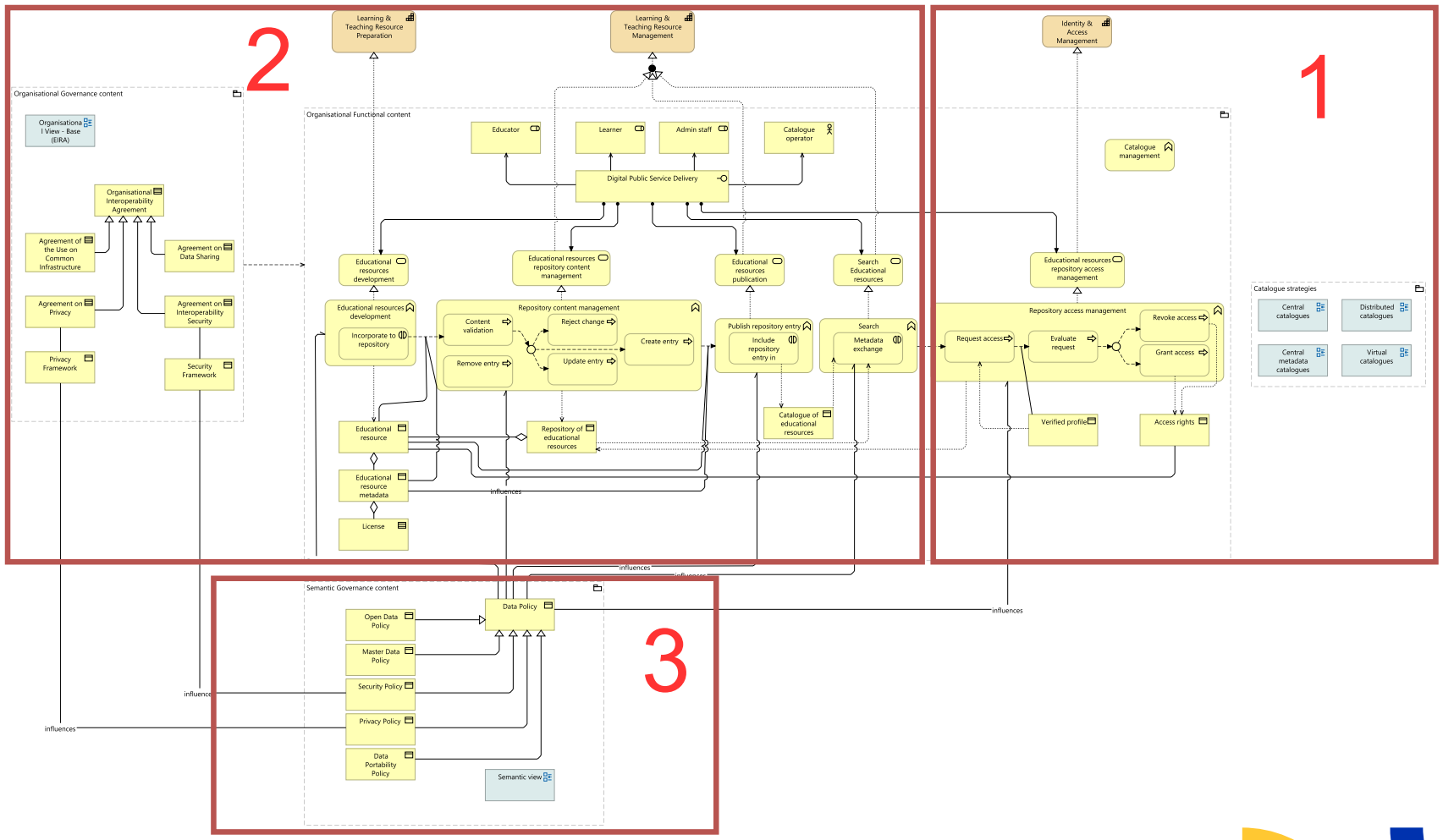


Figure 38 use case 4 (Managing educational resources) - organisational view overview.

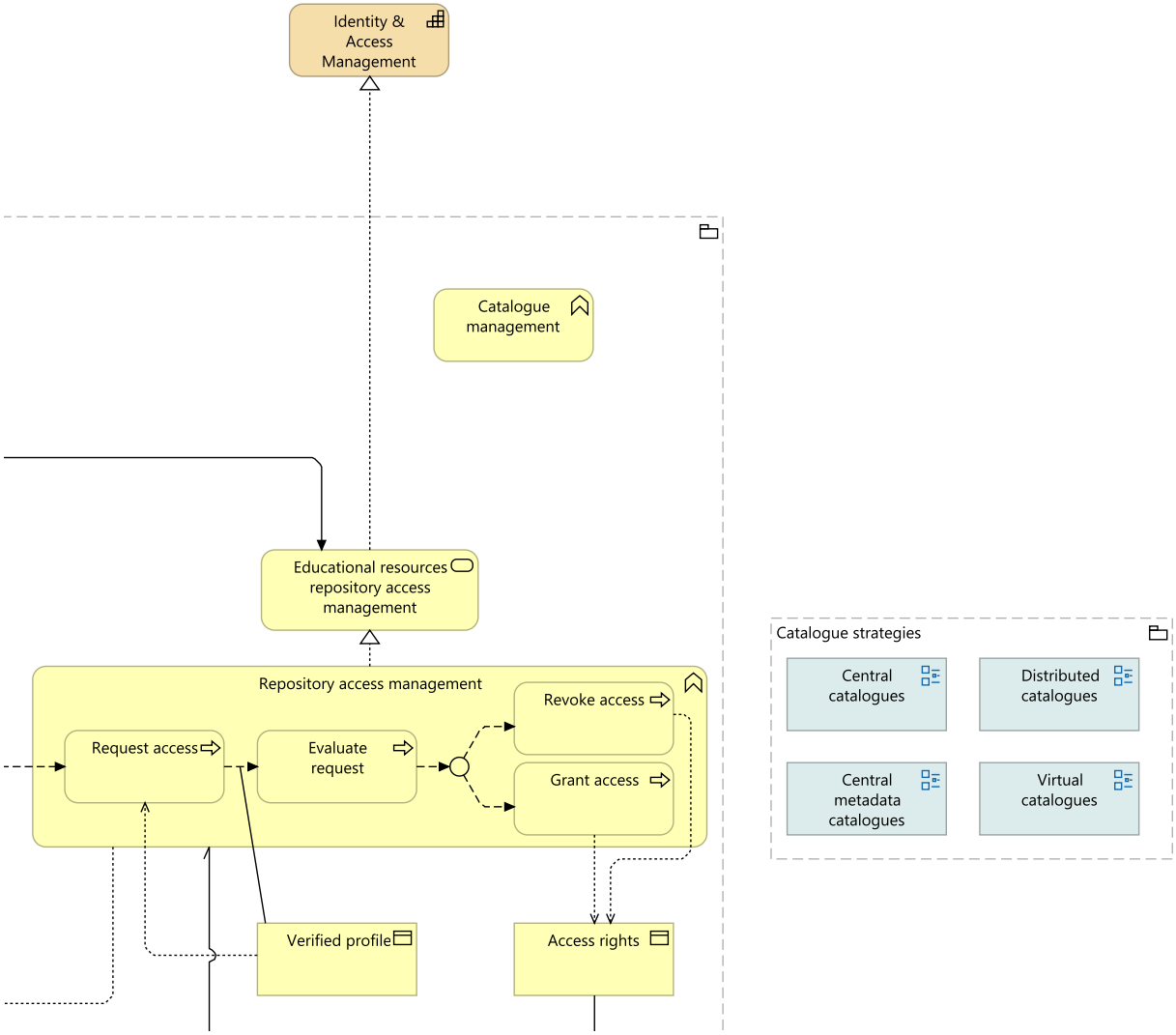


Figure 39 use case 4 (Managing educational resources) - organisational view - part 1.
© 2025 European Union

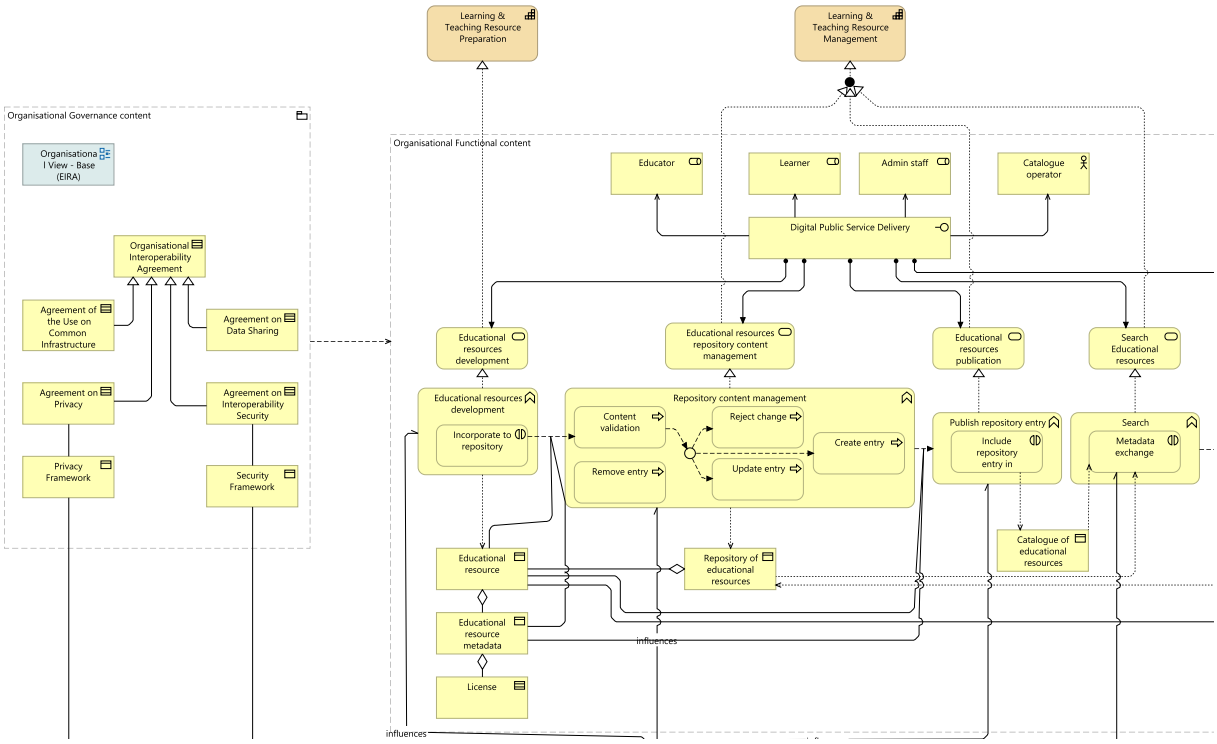


Figure 40 use case 4 (Managing educational resources) - organisational view - part 2.
© 2025 European Union

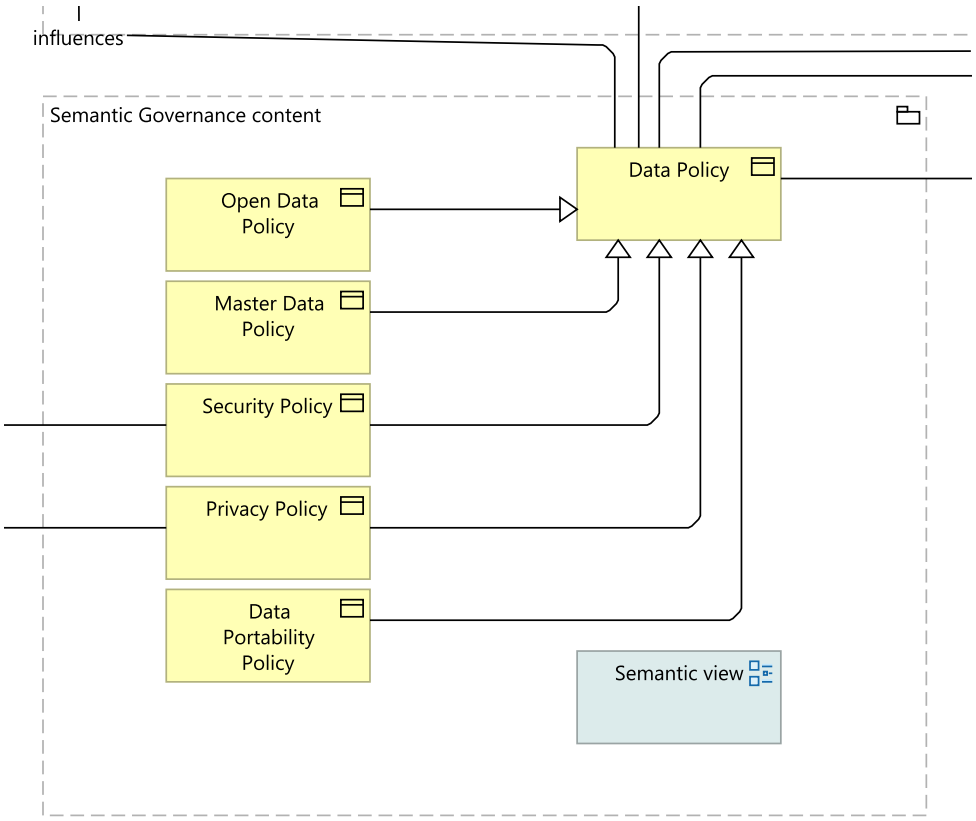


Figure 41 use case 4 (Managing educational resources) - organisational view - part 3.
© 2025 European Union

The previous diagram shows the organisational view. It reveals the necessary capabilities for this use case, such as the learning and teaching resource and its preparation. Both are key to the case.

The main interface in the business logic is a Digital Public Service Delivery. It must implement several business services: developing educational resources, managing the educational resources repository content, and publishing educational resources.

These services come to life through their specific functions and processes. These are shaped by the required data policies and agreements.

In the following table, the most prominent building blocks are described.

Building block	Type	Description
Learning and teaching resource management	Capability	The learning and teaching resource management ensures that students and staff can access learning resources. These resources are found in relevant learning systems, repositories, and facilities.
Learning and teaching resource preparation	Capability	The learning and teaching resource preparation acquires, creates, or assembles learning resources for delivery. This includes items like books, excerpts, documents, X-Reality experiences, 3D models, prints, and video presentations.
Educational resources development	Business function	The educational resources development creates and updates existing educational resources.
Repository content management	Business function	The repository content management implements multiple processes to manage the repository of resources
Repository access management	Business function	The repository access management includes the processes required to administer users' access rights to different assets.
Educational resource	Business object	An educational resource is either physical or digital. It is available and managed by an educational institution.
Access rights	Business object	Access rights determine who can view, edit, or delete data. Proper control of these rights is crucial for keeping information confidential, intact, and accessible.
Availability information	Business object	An availability information indicates whether an asset is available

Catalogue of educational resources	Business object	The catalogue educational resources contains all educational resources.
Verified profile	Business object	A verified profile represents a learner, educator or administrative staff related to an institution.
Terms and conditions	Contract	Terms and conditions are a legal agreement between an institution and the end user of an asset. Provides a set of conditions to make use of an asset.
Provider terms and conditions	Contract	The provider terms and conditions are a legal agreement between an institution and the end user of an asset. Provides a set of conditions to make use of an asset.
Content validation	Business process	The content validation validates the creation or an update of content.
Incorporate to repository	Business interaction	The incorporate to repository interaction involves adding educational resources to the repository.
Metadata exchange	Business interaction	The metadata exchange allows system to communicate properly allowing searching between repositories.
Create entry	Business process	Create entry is a process that creates a new element in the repository or catalogue.
Remove entry	Business process	Remove entry is a process that removes an existing element from the repository or catalogue
Update entry	Business process	Update entry is a process that modifies an existing element.

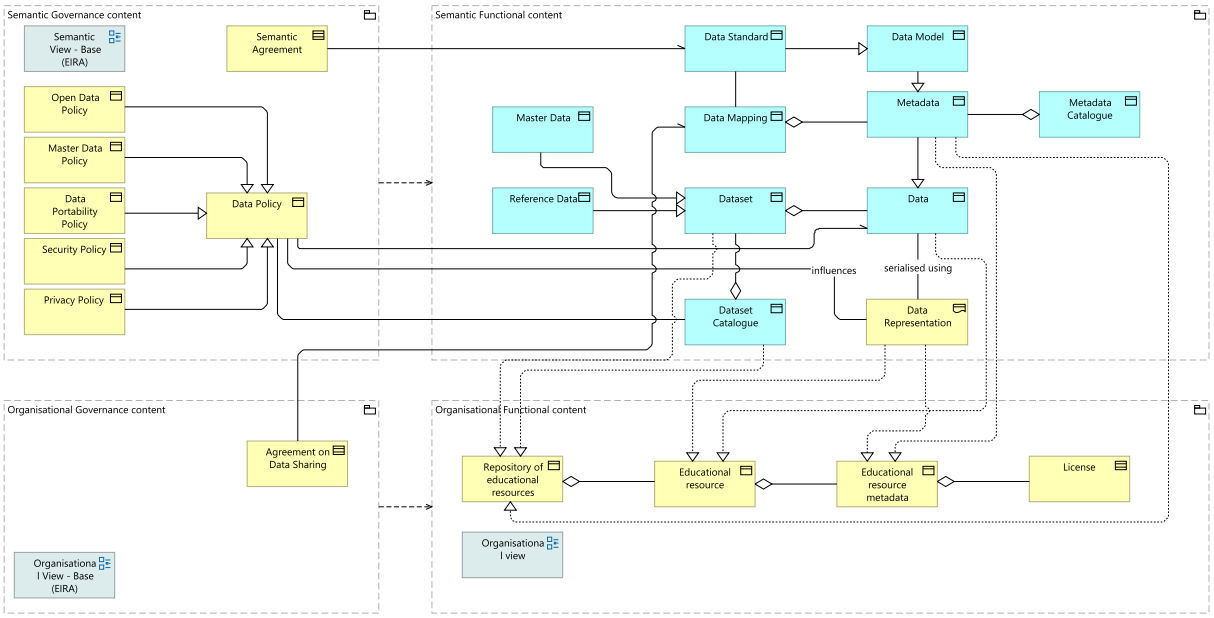


Figure 42 use case 4 (Managing educational resources) - Semantic view.
© 2025 European Union

Building block	Type	Description
Semantic agreement	Contract	A semantic agreement is a contract between a peer and the common ontology, resulting from a matching or mapping process that resolves their semantic discrepancies. This process combines linguistic base, internal and external structure comparison. The resulting match is used to develop an agreement unit, a component of the agreement. The agreement rests on some key assumptions. First, everyone must use the same language for the schema, ontology, labels, and meanings. Also, there should not be personal views in the shared ontology.
Data model	Data object	A data model is a collection of entities, their properties, and how they relate. It aims to represent a domain, a concept, or something in the real world.

Data standard	Data object	A data standard is a predefined structure that guides the organization, integration, and management of data. It includes data models, formats, protocols, and other technical specs. These ensure data stays consistent, works well together, and exchanges efficiently.
Metadata	Data object	Metadata provide information about one or more aspects of the data.

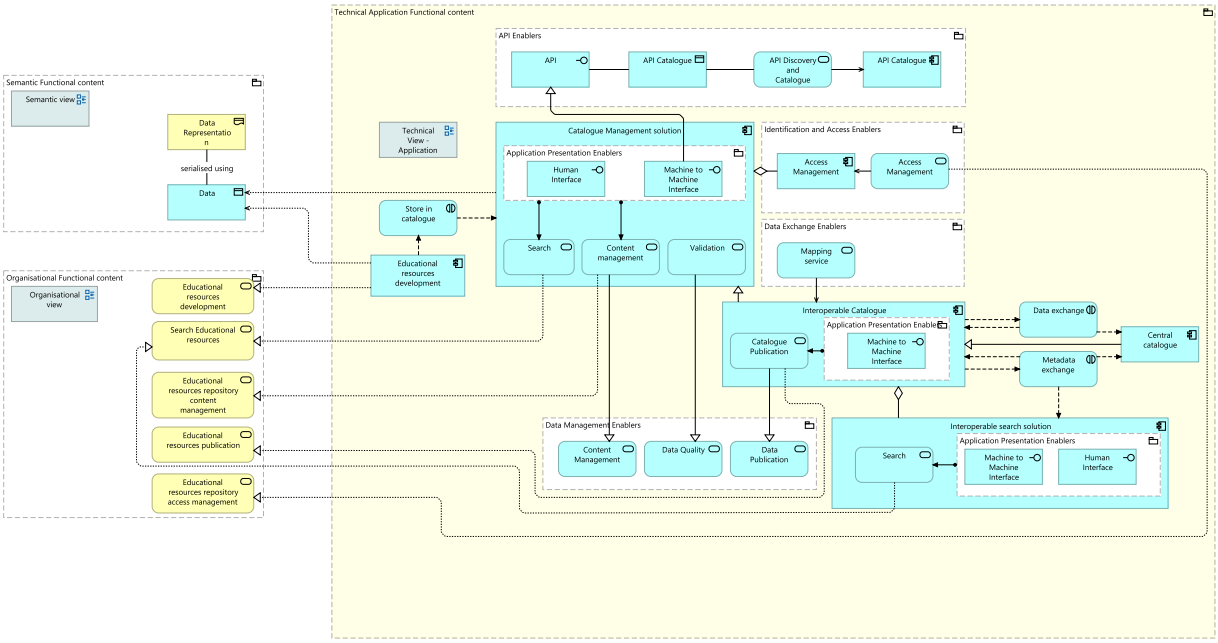


Figure 43 use case 4 (Managing educational resources) - Technical view.
© 2025 European Union

Understanding this use case as a catalogue of educational resources, the primary focus is on effective search and usage. In this context, standards and metadata play a crucial role. Below, the essential building blocks that form the technical layer are outlined.

Building block	Type	Description
Catalogue management solution	Application component	The catalogue management solution implementsation of components that are responsible for managing the storage, validation, publication, and retrieval of data within a catalogue to facilitate the discovery of data.
Interoperable catalogue	Application component	The interoperable catalogue supports the exchange of data between different catalogues.
Data exchange	Application interaction	The data exchange enables the transfer of data between interoperable catalogues. This includes data such as courses and assets.The data exchange enables the transfer of data between interoperable catalogues. This includes data such as courses and assets.
Metadata exchange	Application interaction	The metadata exchange allows system to communicate properly allowing searching between repositories.
Catalogue publication	Application service	The catalogue publication makes learning opportunities, assets, and educational resources accessible and reusable.
Search	Application service	Search enables users to discover, filter, and organise learning opportunities and assets.
Validation	Application service	Validation ensures data accuracy, completeness, and consistency before publication.

For more details on the ArchiMate building blocks in this diagram, check the blueprint reference architecture report. It has all the important information about these schemes.

4.5 Interoperability required capabilities

Describing the contents of an educational resource is crucial for making it discoverable. The first step to sharing resources between institutions is to agree on a shared data standard that fully describes educational resources. Controlled vocabularies provide a solid foundation for standardising terms that describe contents. Each term in a controlled vocabulary should have a set of accepted synonyms and a clear definition. Search services need to know what attributes are available to build effective queries. A shared model enables search services to function effectively.

For more information on the interoperability capabilities of this use case, please refer to the comprehensive final mapping report.

4.6 Recommendations – use case 4

When designing systems, safeguarding data is crucial. Oversharing can unleash security risks, spark performance hiccups, and complicate processes. Share only the essential data and metadata. Pay special attention to licensing; some educational gems may come with strings attached.

Embrace controlled vocabularies; they are key to simplicity. This method streamlines searching and filtering, helping users find the right resources swiftly. Moreover, it could entice mobile students seeking efficient tools across institutions.

Open Educational Resources (OERs) are treasures waiting to be explored. They are free for anyone to use, modify, and share, making them perfect for broadening access to learners, especially in resource-challenged settings. Since OERs are typically in open formats, they shine on any platform—be it mobile devices, desktops, or various learning management systems.

By harnessing the power of OERs, institutions can cultivate a nurturing educational ecosystem. Here, resources are not only accessible to everyone but also adaptable to fit any need. This approach champions the creation of flexible, shareable, and universally accessible educational experiences, perfectly aligning with our aim.

PART 5

Use case 5 – Generate data

5 Use case 5 - Generate data

USE CASE 5

Generate data

Establishing a standardised approach for the exchange of learners' activity data to ensure a seamless integration of various virtual learning environments.

Learning Analytics

Student Analytics

5.1 Use case definition

This use case focuses specifically on information residing in a typical Learning Management System (LMS). The key capability is to generate, store, and exchange learner data at a more granular level than earning the credential. This use case gives means to analyse metadata on the learner journey. It helps to improve platforms and educational resources and can also guide the creation of new educational tools.

5.2 High-level flow

Learners produce activity data as they engage in various learning activities using a range of tools. These activities are stored in a **learner records storage (LRS)**, which can be part of a **learning management system** or a standalone system.

Regardless of the approach chosen by the institution or alliance, learners can track their progress by gathering their own aggregated records from an LRS. The chosen approach should be clear to both learners and educators. Educators can also access these records to see each student's progress in the same way.

There are four approaches to this use case: central operator, decentralised, broadcast, and central metadata operator.

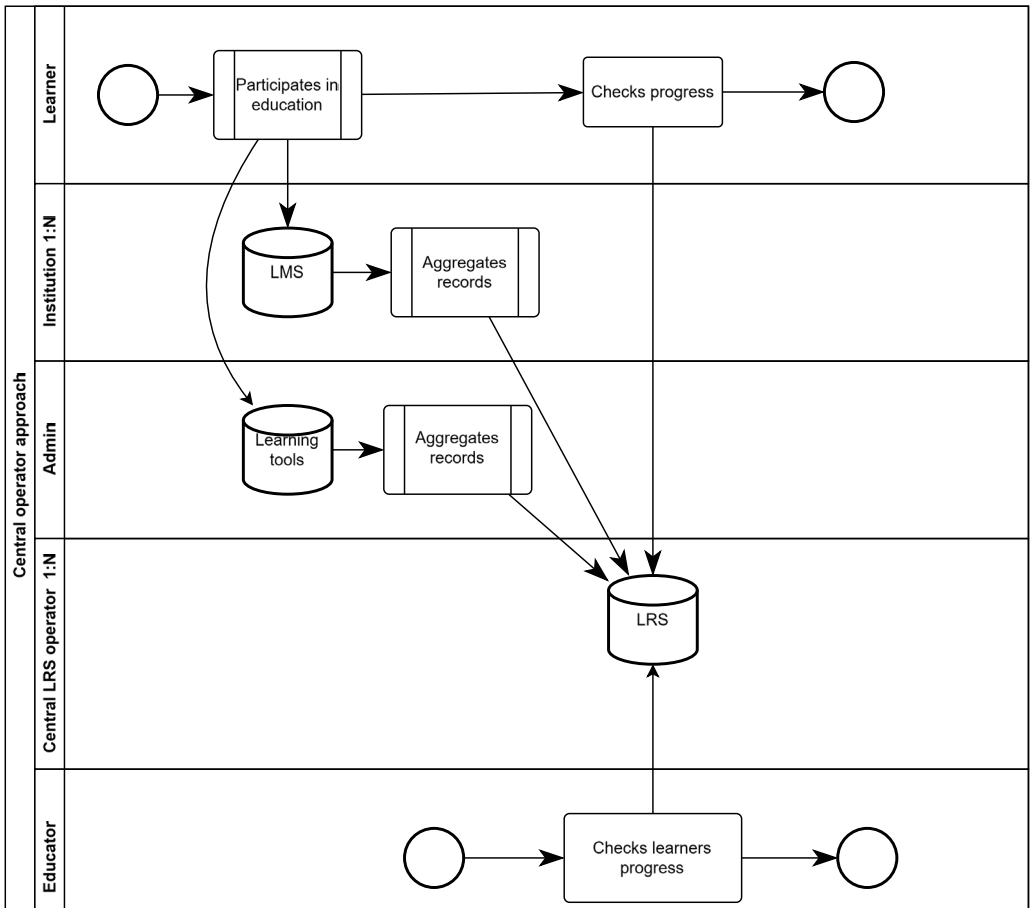


Figure 44 - Overview of the steps required to persist and search the learning records generated by learners following a central operator approach.
© 2025 European Union

The central operator approach forces the LRS to be an independent element. It collects all learning records generated by learners using the LMS and learning tools. This behaviour leads to a delicate state of information duplication. The learner's activity records co-exist in both the local LMS and the central LRS, which can be a source of data inconsistency. For example, a learner could search for their learning progress before the LMS synchronizes the data with the central LRS. This condition could be plausible due to a network connection issue or a high latency scenario.

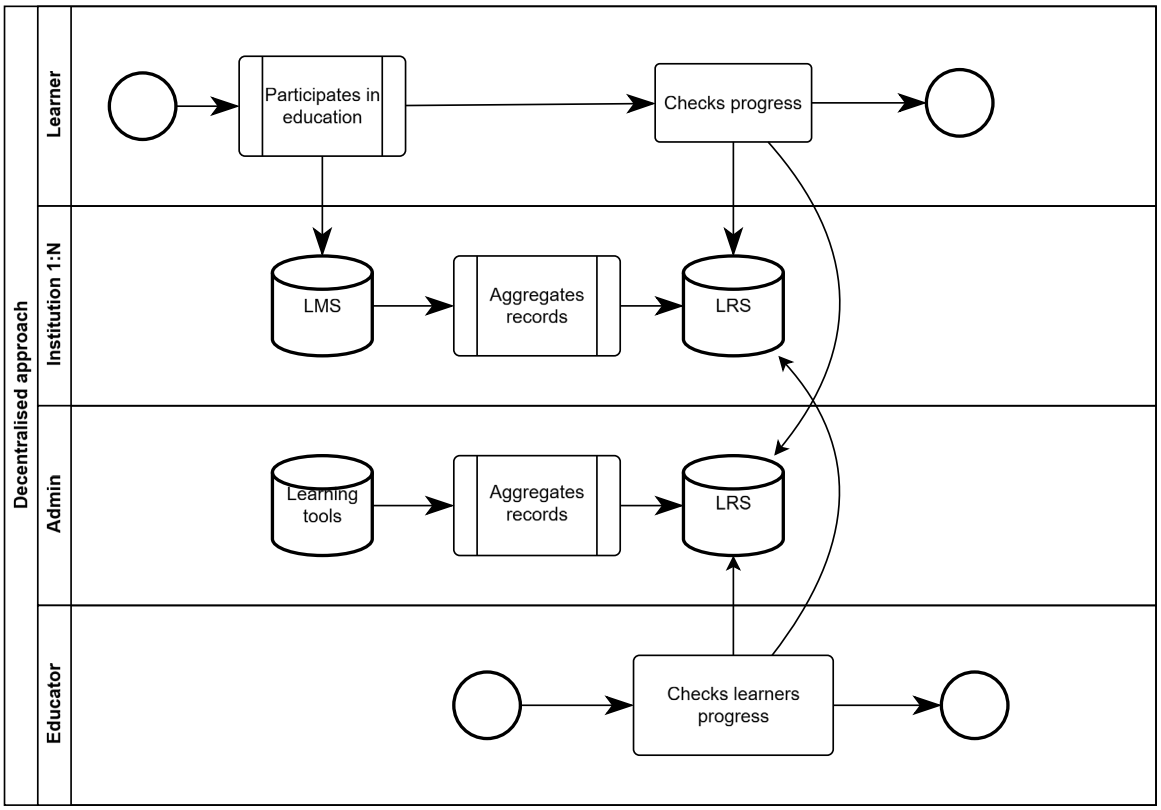


Figure 45 - Overview of the steps required to persist and search the learning records generated by learners following a decentralised approach.
© 2025 European Union

In the decentralised approach, the absence of a central LRS means many requests are made between all the systems involved. This could be a scalability issue. However, this approach prevents data duplication, as there is no need for a central LRS. To track learners' progress, which is stored across LMS and learning tools, learners and educators should have access to all existing LRS.

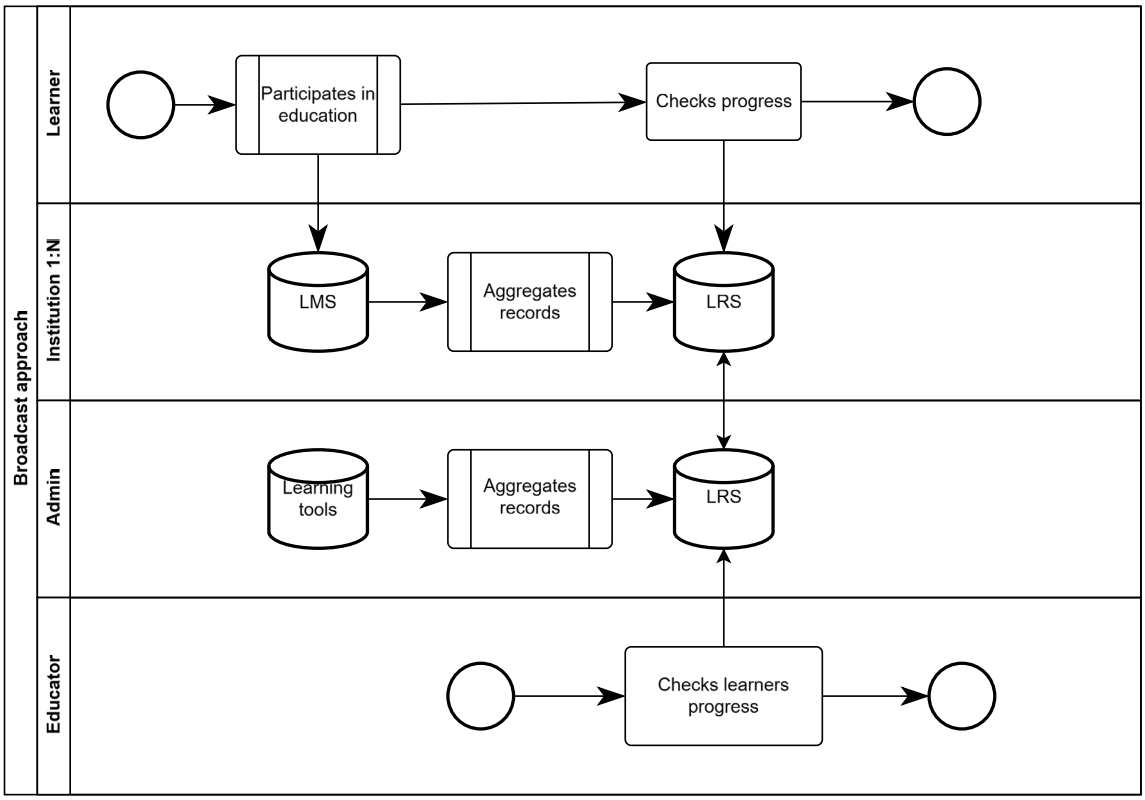


Figure 46 - Overview of the steps required to persist and search the learning records generated by learners following a broadcast approach.
© 2025 European Union

The last approach is broadcasting, which involves each LRS registering the learning records of every other LRS. This allows learners and educators to access their learning records from any exposed LRS. Like the central operator approach, this method also requires duplicating learning records. Moreover, it generates a high volume of requests, similar to the decentralised approach. However, the broadcast approach has a significant advantage: data availability. Even if one or more LRS become unavailable, the learning records remain accessible due to the replication of data between LRS.

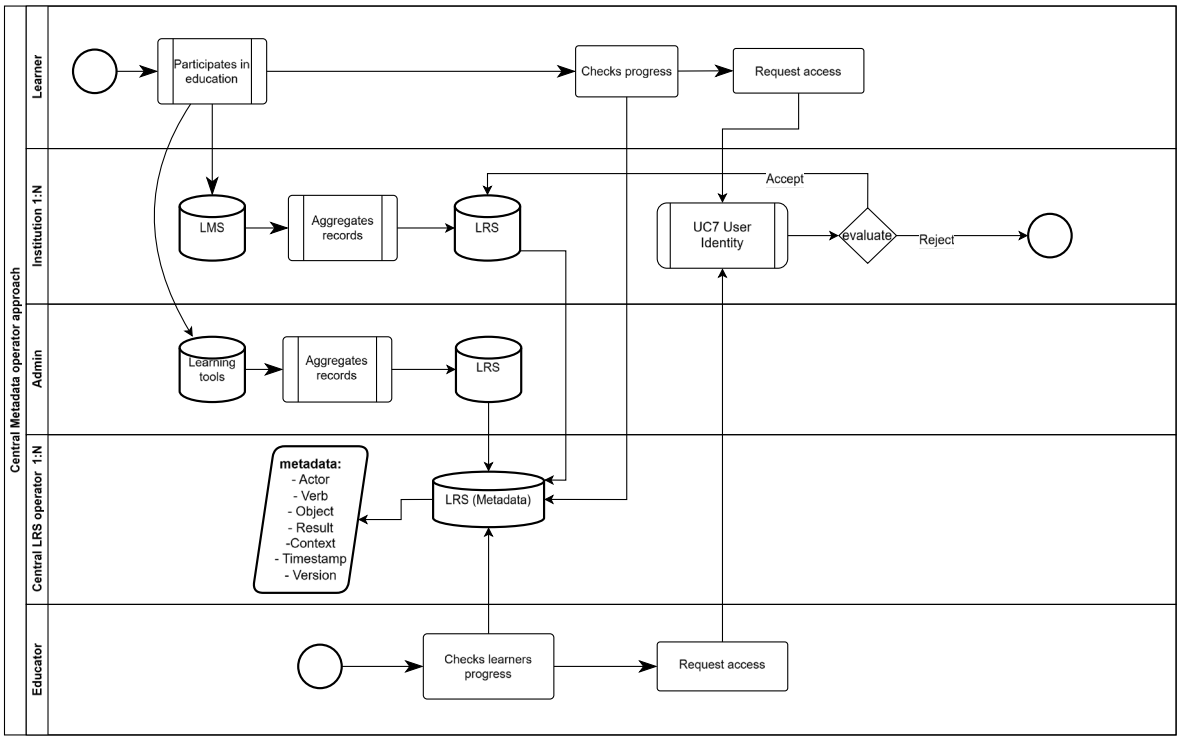


Figure 47 - Overview of the steps required to persist and search the learning records generated by learners following a central metadata operator approach.
© 2025 European Union

As seen in squad 4's working sessions, squad 5 has identified using a central storage system as a metadata repository as a viable approach. This approach, like use case 4 for managing educational resources, helps with licensing policies, privacy, and usage rules. It does this by not moving the generated resources between systems.

5.3 Draft architecture

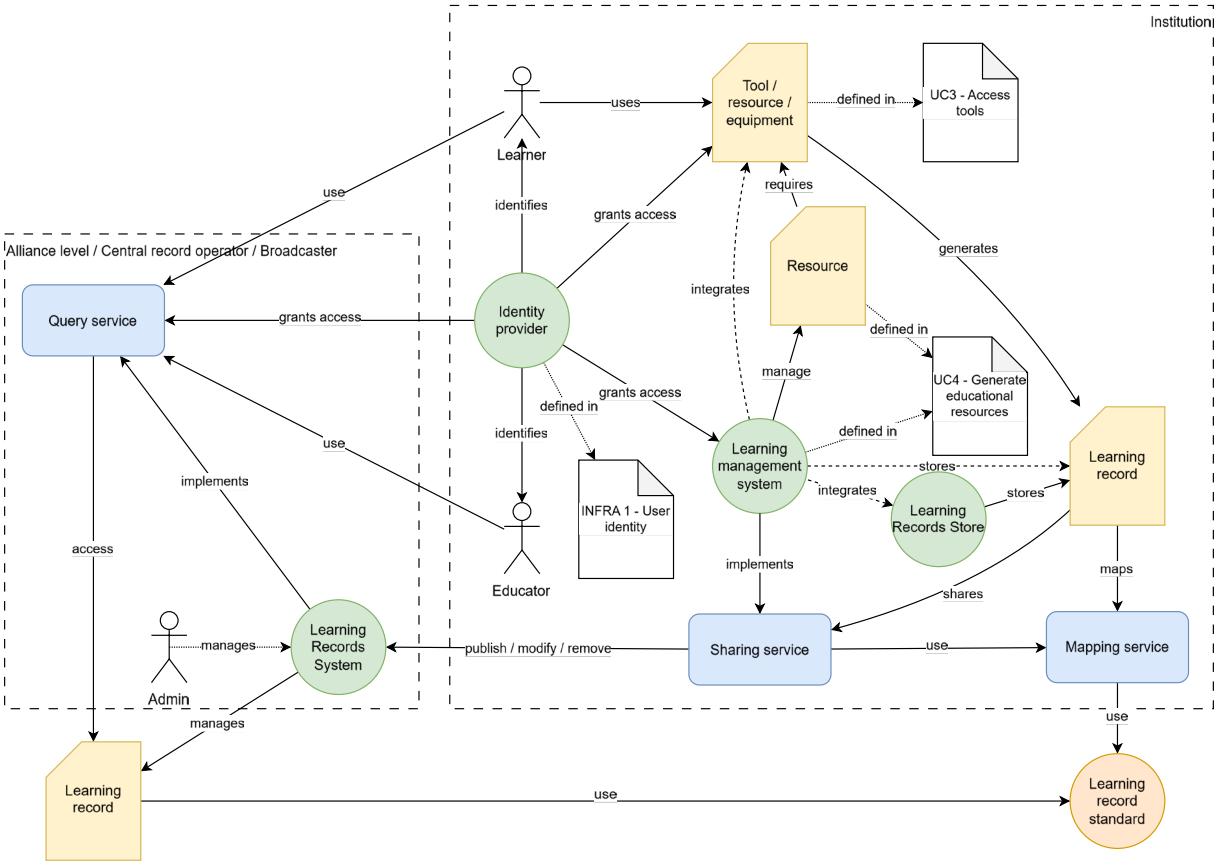


Figure 48- Overview of main architectural components involved in generating, storing, and sharing learner records.
© 2025 European Union

Business objects:

- **Learning record:** This is a statement about a learning activity done by a learner. It includes details about the learner, the action taken, and the outcome of that action.
- **Resource:** An educational resource designed as part of a learning activity, typically created to be used with a specific tool, resource, equipment, or other type of asset.
- **Tool:** Any type of asset available to complete a learning activity.

Services:

- **Sharing service:** Manages sending local records to outside systems. It offers a reading or publishing interface based on the chosen method. This service may rely on a mapping service to translate from the local data model to the shared learning record standard.
- **Query service:** Users interact with the query service to collect information about learner activities. This service will be implemented in different ways, based on the chosen approach. It may broadcast queries to various systems in a decentralised manner, connect with the local record system, or work with the central record system.

Systems:

- **Learning management system (LMS):** A software application that administers and delivers educational processes. In this use case, it integrates information on learners' progress related to different learning activities that make up a learning offering.
- **Learning records system (LRS):** A software application that stores and manages learning records. These systems can be integrated into the LMS or function as an independent system.

5.4 Reference architecture

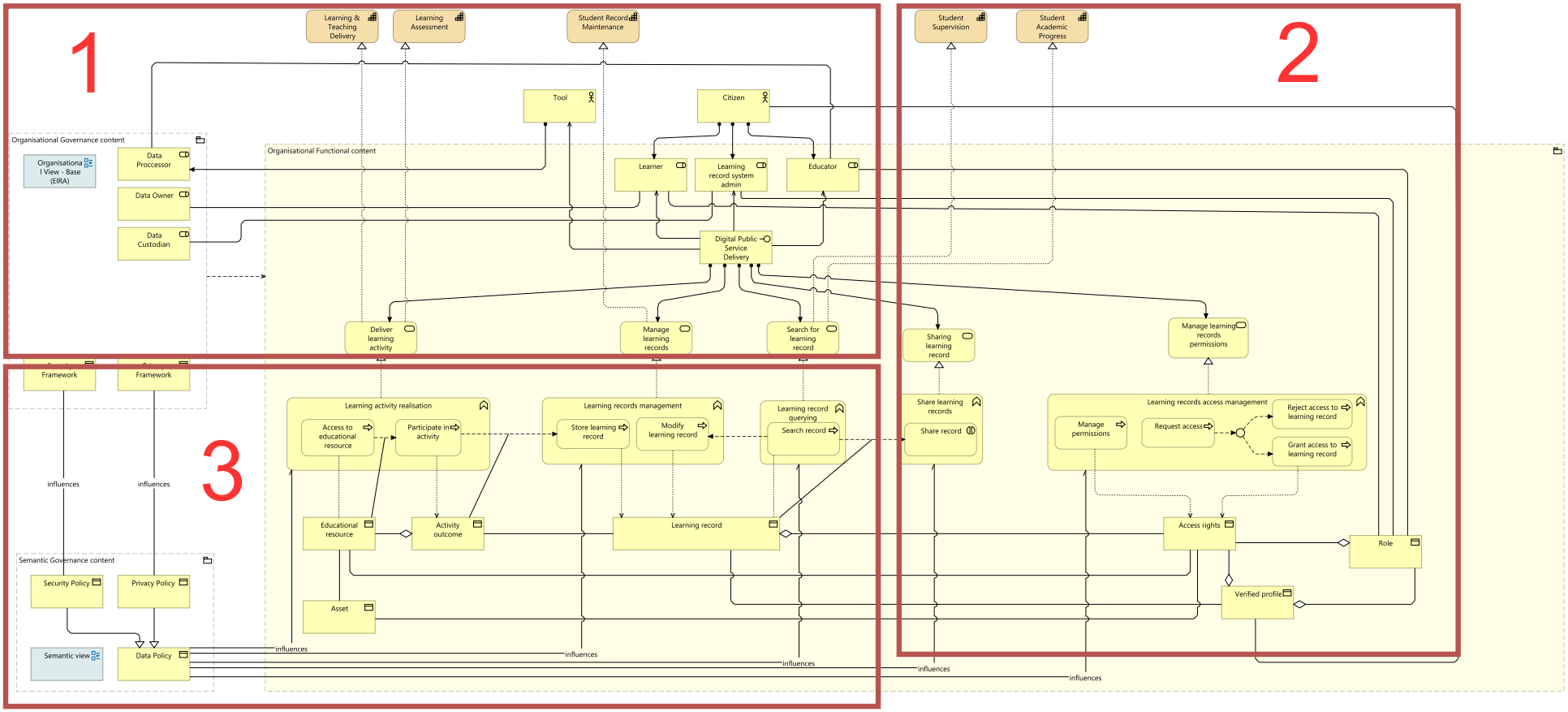


Figure 49 Use case 5 (Generate data) – organisational view overview.

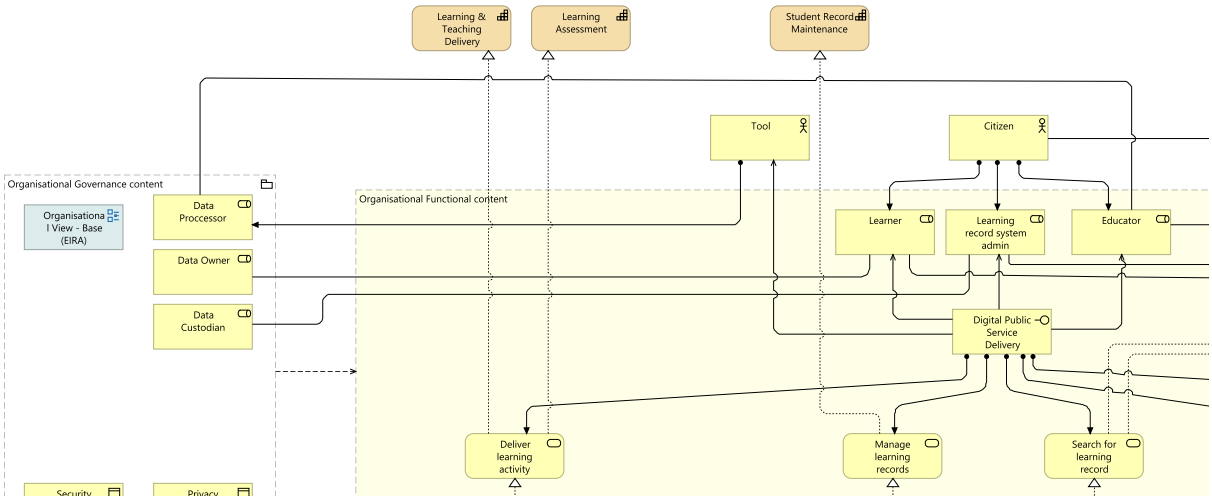


Figure 50 Use case 5 (Generate data) – organisational view - part 1.
© 2025 European Union

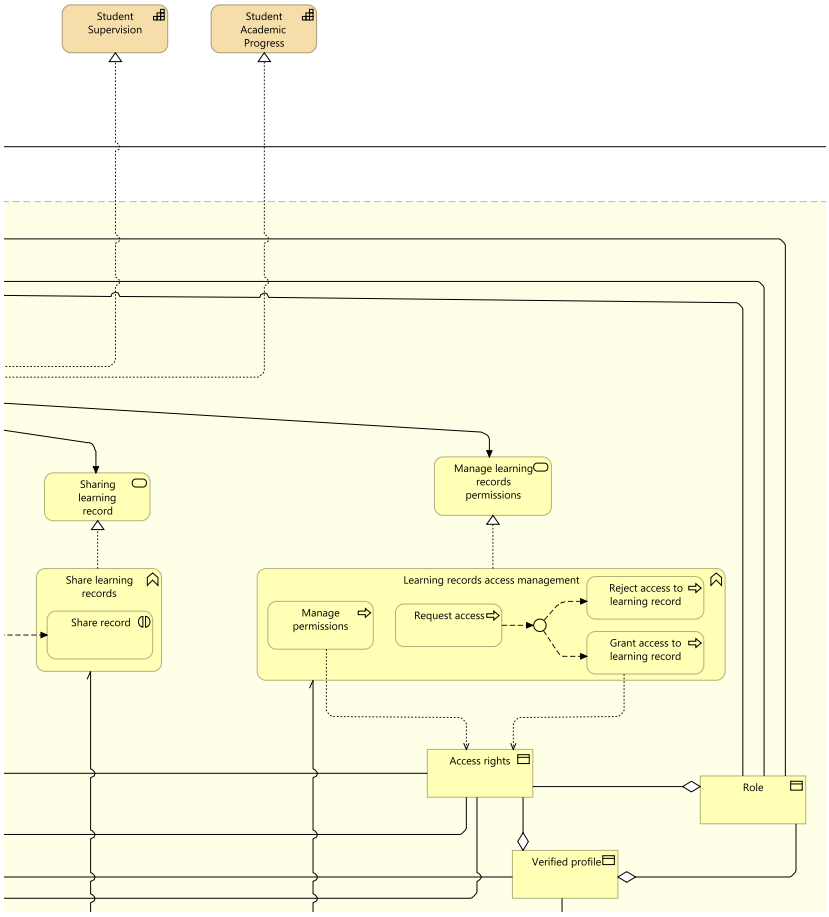


Figure 51 Use case 5 (Generate data) – organisational view - part 2.
© 2025 European Union

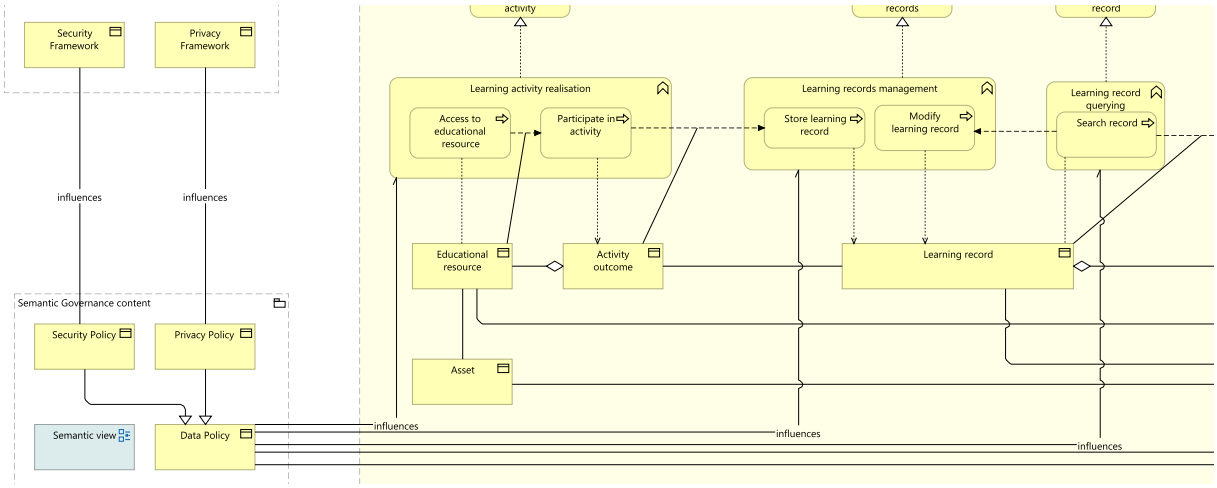


Figure 52 Use case 5 (Generate data) – organisational view - part 3.
© 2025 European Union

This architectural schema shows the organisational layer for learning records. It reflects the lifecycle of records created by students during course activities. The key capabilities related to learning records include learning and teaching delivery, learning assessment, student record maintenance, student supervision, and student academic progress. The schema layers different citizen roles from top to bottom. These roles determine access to services through a public digital services interface. The processes for creating and managing learning records involve learner-generated data. Thus, there is a strong link to various privacy and security frameworks.

The following table describes the most prominent building blocks.

Building block	Type	Description
Learning and teaching delivery	Capability	The learning and teaching delivery conducts activities specified in the institution's curricula.
Learning assessment	Capability	The learning assessment capability checks what students know about learning outcomes in all delivery modes. This includes blended learning, work-based learning, and work-integrated learning.
Student record maintenance	Capability	The student record maintenance captures and manages information on each student, including permanent evidence of their attainment and attendance.

Student supervision	Capability	The student supervision capability oversees a student's academic work. This includes course-based, dissertation-based, and research-based efforts.
Student academic progress management	Capability	The student academic progress management guides a student to completion of their studies.
Learning record system admin	Business role	The learning record system admin manages the learning records generated by learners within a single profile.
Data processor	Business role	A data processor is a natural or legal person, public authority, agency, or any other body that processes personal data on behalf of the controller. There are situations where an entity can be a data controller, or a data processor, or both.
Data owner	Business role	A data owner is a business role assigned to an individual who creates or generates the data or the entity that has legal ownership or control over the data. In other cases, a data owner might be the individual or entity responsible for managing or overseeing the use of the data. Under the European General Data Protection Regulation (GDPR), a „data controller" is defined as the entity that determines the purposes, conditions, and means of the processing of personal data. This means that the data controller is the entity that decides why and how personal data is processed.
Data custodian	Business role	A data custodian is a natural or legal person, public authority, agency, or any other body that processes personal data on behalf of the controller. There are situations where an entity can be a data controller, or a data processor, or both.
Learning activity realisation	Business function	The learning activity realisation combines two main business processes. First, it allows access to educational resources. Then, it enables participation in an activity. This leads to a learning outcome for the learner. Finally, this outcome is noted in a learning record.
Learning records management	Business function	The learning records management encompasses the processes of storing and modifying learning records.

Learning record querying	Business function	The learning record querying involves searching for learning records linked to different workflows. This function is shaped by the data policy for business objects. It includes privacy and security rules for managing this type of data.
Share learning records	Business function	The share learning records manages the service of sharing learning records. This function is influenced by the business object data policy. This policy includes privacy and security rules for sharing such data.
Learning records access management	Business function	The learning records access management involves handling access and permissions for user-generated learning records.
Activity outcome	Business object	The activity outcome is the outcome of an activity, either physical or virtual.
Learning record	Business object	A learning record is a digital record for a learning experience that one learner has participated in.
Access rights	Business object	Access rights determine who can view, edit, or delete data. Controlling these rights is crucial for keeping information confidential, intact, and accessible.
Privacy framework	Business object	The privacy framework is a business tool. It helps keep data, information, and knowledge safe. It also protects how organisations manage these resources.

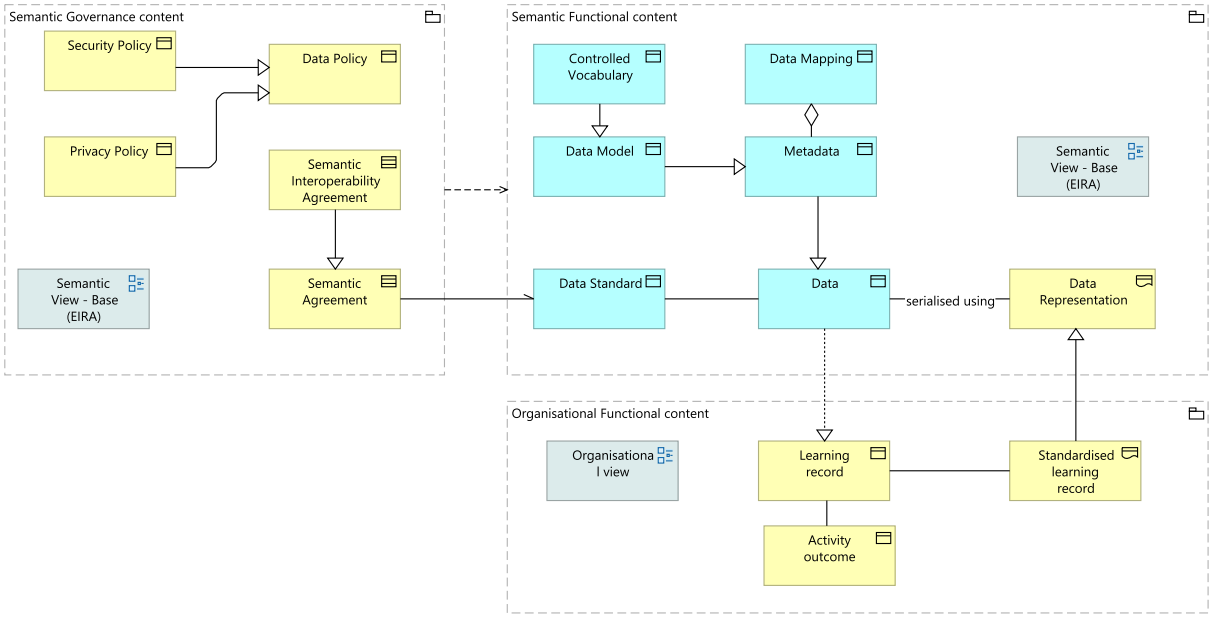


Figure 53 Use case 5 – semantic view.
© 2025 European Union

For this use case, the reference architecture at the semantic level shows only the ABBs tied to the current data representation. It explains how these should link to standardised data representations for better interoperability.

In the following table, the most prominent building blocks are described.

Building block	Type	Description
Standardised learning record	Representation	The standardised learning record defines the standardised state of a learning record.
Semantic interoperability agreement	Contract	The semantic interoperability agreement formalises governance rules that help digital public services work together. This agreement has important ontological value.

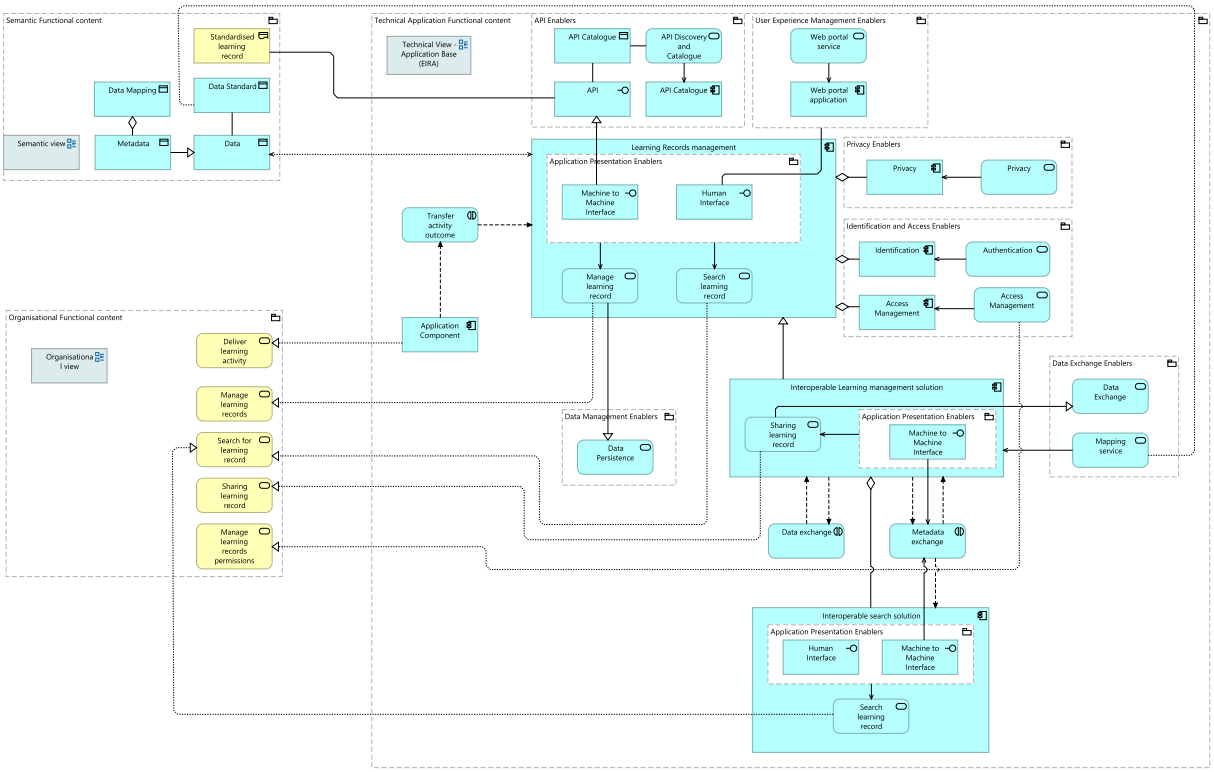


Figure 54 Use case 5 – technical view.
© 2025 European Union

The technical view of the reference architecture for this use case shows how learning records management currently works for learners. On top of this foundation, the necessary components are added to make sure this use case allows interoperability. This is achieved through data exchange enablers and components that facilitate the exchange and retrieval of standardised metadata.

In the following table, the most prominent building blocks are described.

Building block	Type	Description
User experience management enablers	Grouping	The user experience management enablers are components and services. They track, measure, analyse, and improve how people interact with the organisation.
Privacy enablers	Grouping	The privacy enablers are components and services. They facilitate the implementation of privacy-related functionality within an application or system.
Identification and access enablers	Grouping	The identification and access enablers help securely identify and authenticate users, systems, and services on a platform.
Data exchange enablers	Grouping	The data exchange enablers are tools or components facilitating the exchange of data between systems or applications.
Data management enablers	Grouping	The data management enablers are components and services supporting effective data management practices and procedures.
Learning records management	Application component	The learning records management ABB is a service for managing and searching learning records. These services are exposed through the application presentation enablers. The data processing in this application combines features from other components. These include access management, identification, and privacy.
Interoperable learning management solution	Application component	The interoperable learning management specialises the learning records management. This specialisation helps share learning record data. It uses data exchange tools to map to standardised data and make it accessible.

Interoperable search solution	Application component	The interoperable search solution specialises the search functions for learning records. It is part of the interoperable learning management solution.
Transfer activity outcome	Application interaction	The transfer activity outcome shows how to move a learner's learning record. This record relates to the activity the learner completed. It transfers data from the generating application to the storage where it will be kept.

For more details on the ArchiMate building blocks in this diagram, check the blueprint reference architecture report. It has all the important information about these schemes.

5.5 Interoperability required capabilities

In this use case, certain capabilities must be met to ensure interoperability in terms of data transmission. The wide range of available tools related to educational resources generates learning records that form a very heterogeneous group. The goal of interoperability is to group these learning records under the same system, depending on the chosen implementation approach. Similar to the previous use cases, a common data standard must be agreed upon by the
concerned institutions.

From the institutions' perspective, it is important to define what type of learning records they want to store. Agreeing on the granularity of the learning records to be stored helps choose a suitable standard that aids interoperability. For example, they can save only the learning records corresponding to completed activities with an associated score. Alternatively, they can agree on a series of verbs or actions related to the learning records they wish to save, allowing for a complete tracking of learners' actions and the status of each one. These methods of selective storage avoid storing all generated learning records in full, reducing noise in data analysis tasks.

For more information on the interoperability capabilities of this use case, please refer to the comprehensive final mapping report.

5.6 Recommendations – use case 5

To manage learning data effectively and improve interoperability between systems like Learning Management Systems (LMS), Learning Record Stores (LRS), and Student Information Systems (SIS), we propose the following recommendations. They focus on data sharing, process streamlining, and clearer learner progress tracking.

Key areas include defining shared data, understanding LRS and LMS roles, and outlining data management tasks. They also focus on ensuring real-time insight into learning activities. These recommendations tackle challenges in system integration. They provide practical solutions for improved collaboration and interoperability.

- **Scope of shared data:** The LMS typically holds a wide range of data related to course delivery, such as learning resources, assignments, assessments, and progress tracking. In contrast, the LRS and SIS focus on recording completion data, capturing learners' achievements, and tracking their interactions within the system. The shared data scope should work like this: the LMS keeps detailed content and teaching data. The LRS and SIS manage the lasting records of completion and achievement. This ensures each system is optimised for its purpose and reduces redundancy.
- **Type of shared data:** The data shared between systems should primarily consist of metadata rather than the content of learning activities themselves. Share metadata instead of whole assignments or course materials from the LMS. This includes activity titles, due dates, completion status, and relevant tags. This allows other systems, such as the LRS or SIS, to efficiently track progress without duplicating content that should remain within the LMS. Focusing on metadata helps institutions keep a simple, interoperable data-sharing model. This way, they can stay aligned without overloading their systems or causing extra data duplication.
- **LRS responsibility for sharing learners' data:** The LRS should be responsible for sharing learner data across systems. This includes data related to learner interactions with the content, assessments, and completion status. As the LRS tracks learners' experiences and achievements, it ensures that data is standardised and accessible to relevant stakeholders. Making the LRS the centre for learner data helps institutions share accurate and current records with systems like the SIS. This simplifies data management and boosts interoperability.
- **Admin staff manages the LRS and educators the LMS:** To manage data efficiently, administrative staff should oversee the LRS. They maintain institutional records, ensure data integrity, and handle data sharing between systems. In contrast, course-level metadata, like course descriptions,

assignments, and learning objectives, should synchronise from the LMS and be managed by educators. This split in responsibilities lets educators focus on instructional design and learner progress. Meanwhile, admin staff ensure accurate record-keeping and smooth data flow between systems.

- **Accurate information on ongoing activities:** A major challenge in the current setup is the lack of visibility into real-time activities across systems. Currently, the absence of a completion record is often the only clue that an activity is behind schedule. To address this, it is crucial to establish interoperability between the LMS and LRS, allowing real-time updates on the status of planned and incomplete activities. This integration gives deeper insights into learners' progress. It helps educators and administrators spot issues early. They can see overdue activities or struggling learners without just checking the final completion record. This enhanced transparency would improve intervention strategies and overall course management.

PART 6

Use case 6 – Earn a credential

6 Use case 6 - Earn a credential

USE CASE 6

Earn a credential

© *2024 Freepik*

The digital management of educational credentials (issuance, verification, revocation), affirming the achievements from diverse learning experiences.

Micro-credentials

Portable credentials

6.1 Use case definition

Credentials are all about communicating with the job market or enrolling in further learning opportunities. For this use case, credentials can be both digital and physical. The foundation of any credential is trust. This use case covers issuing, sharing, and verifying the credential with trust data.

6.2 High-level flow

Learners who successfully complete learning activities can request a credential that asserts they have acquired a set of skills or learning outcomes. Credentials can be physical, like signed diplomas. They can also be digital, such as signed PDFs or advanced machine-readable formats like verifiable digital credentials.

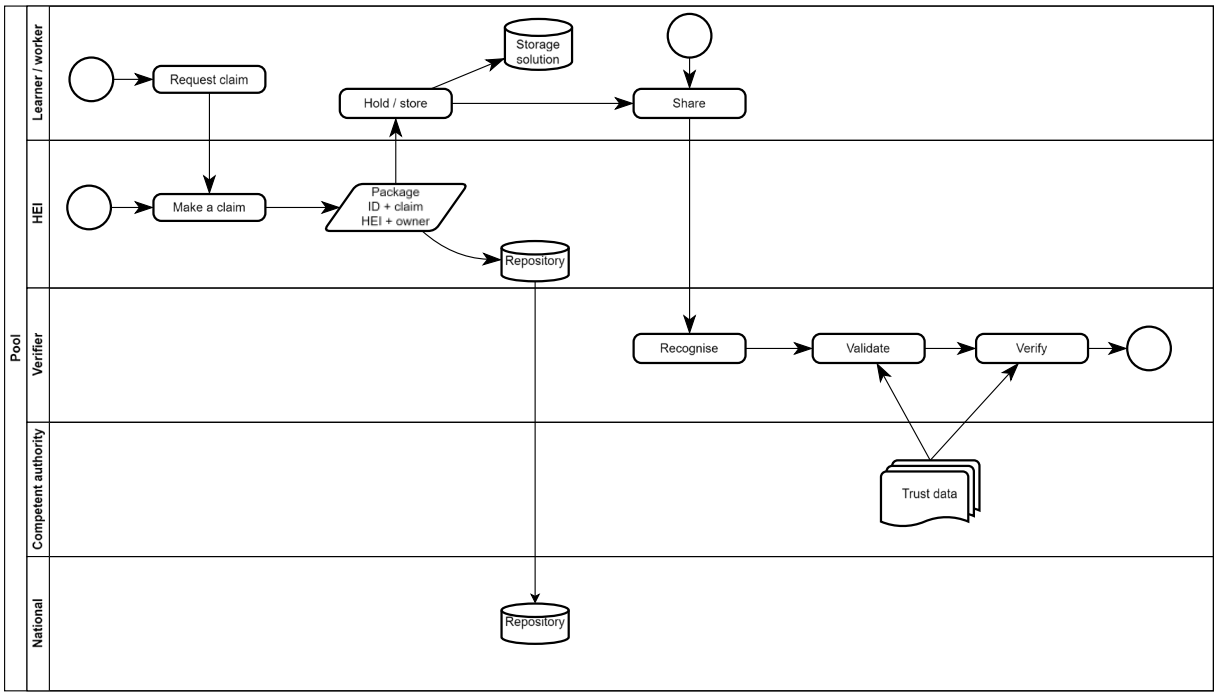


Figure 55 – steps to issue, store, present and validate educational credentials.
© 2025 European Union

Institutions are responsible for generating claims. At a minimum, they need to include three sets of attributes: identifying the learner receiving the credential, the learning achievements accredited, and the issuing institution. The actual set of attributes and format depend on the chosen standard or technology.

Issuing institutions store a record of issuance for validation and verification purposes. Learners who receive the credential store it in their own storage solution. Digital storage solutions are not required for this data flow to work; for instance, printed copies of a credential can be stored in a folder and handled manually. There are several projects, such as DC4EU[10], aim to standardise digital credentials and Open Badges[11] (among others) and how they are stored and shared.

Stored credentials can be shared as proof of successfully completed learning activities in application processes. Verifiers recognise and check the validity and veracity of a credential. This process requires agreed trust mechanisms between the issuing institution and the verifier.

[10] Digital Credentials for Europe | DC4EU
[11] Home | 1EdTech Open Badges

6.3 Draft architecture

Business objects:

- **Credential:** A set of one or more claims made by an issuer. The claims in a credential can be about different subjects.[12]
- **Trust data:** Data used to validate and verify a set of claims.
- **Revocation list:** A list of digital certificates that have been revoked by the issuing certificate authority..
- **Identity attributes:** A set of learner-related attributes linked to the credential issued by the institution.
- **Issuing credential consent:** An institution signs consent, allowing a third party to use its signature as a certificate authority. This applies to future credentials in a joint programme's framework.

Services:

- **Credentials storage service:** Stores copies of issued certificates and a register of their status. It allows users to check the status of a previously issued certificate.
- **Credential issuing service:** Creates a certificate with claims based on learning achievements and records. It uses the identity provider to add details about the person receiving the certificate.
- **Credential sharing service:** Offers ways to share saved credentials with credential storage solutions.
- **Credential revocation service:**Manages the revocation list and is in charge of revoking a credential.
- **Signing service:** Signs a credential with the institution's signing private key.
- **Credential verification service:** Checks the veracity of a claim, involving getting information about the status of a claim.

Systems:

- **Student information system (SIS):** Manages student data, including grades and records of the student needed to issue a claim about the achievements obtained.
- **Learning record store:** SA software application for storing and managing learning records, which can be integrated as part of the LMS or be an independent system.
- **Identity provider:** A system that creates, maintains, and manages identity information for users. It also provides authentication services to applications within a federation or distributed network[13].
- **Credentials storage solution:** A system to store and manage the certificates issued to the user, owned by the subject receiving a credential.

[12] Verifiable Credentials Data Model v2.0 (w3.org)
[13] Verifiable Credentials Data Model v2.0 (w3.org)

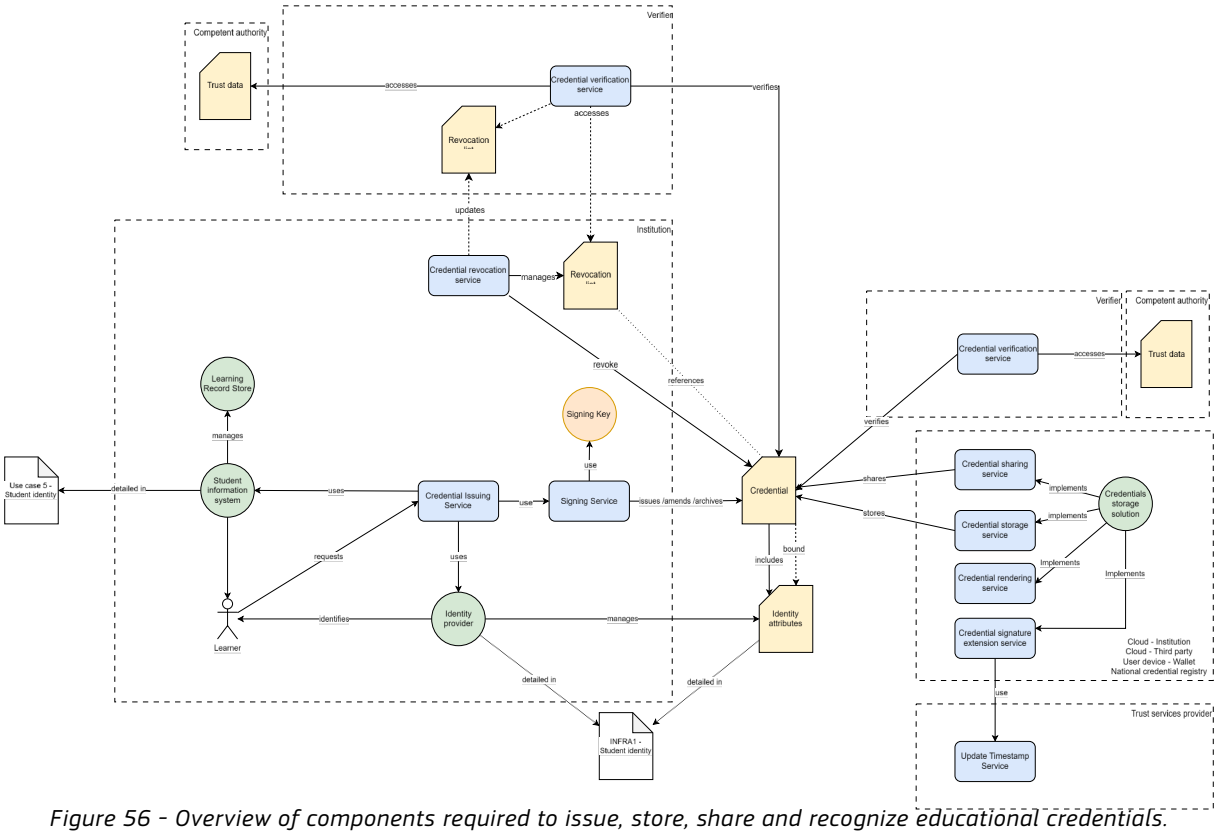


Figure 56 - Overview of components required to issue, store, share and recognize educational credentials.
© 2025 European Union

In the above diagram, the draft architecture is presented for a scenario where an institution issues a credential to a learner. The institution signs this credential with its signing key, and the necessary identity attributes of the user are linked to it so that it can be recognised in the future. The credential is stored in a credential storage solution, which is defined in a generic manner and can represent modern solutions like wallets, as well as more traditional ones, including national repositories. This storage solution is responsible for sharing the credential, displaying it in a readable format, and, in certain cases, extending its validity.

In the following diagram, the credential signing process changes due to it being a joint programme scenario. In this case, several approaches can be followed when signing the credential. For instance, there could be a prior agreement between the involved institutions that allows the learner's home institution to sign the credential on behalf of all participating institutions. Another option is to create an agreement. This would let the home institution sign using its own key. It could also use the signing keys from other institutions. This way, the credential would be signed by all of them. Both of these cases are represented in the diagram.

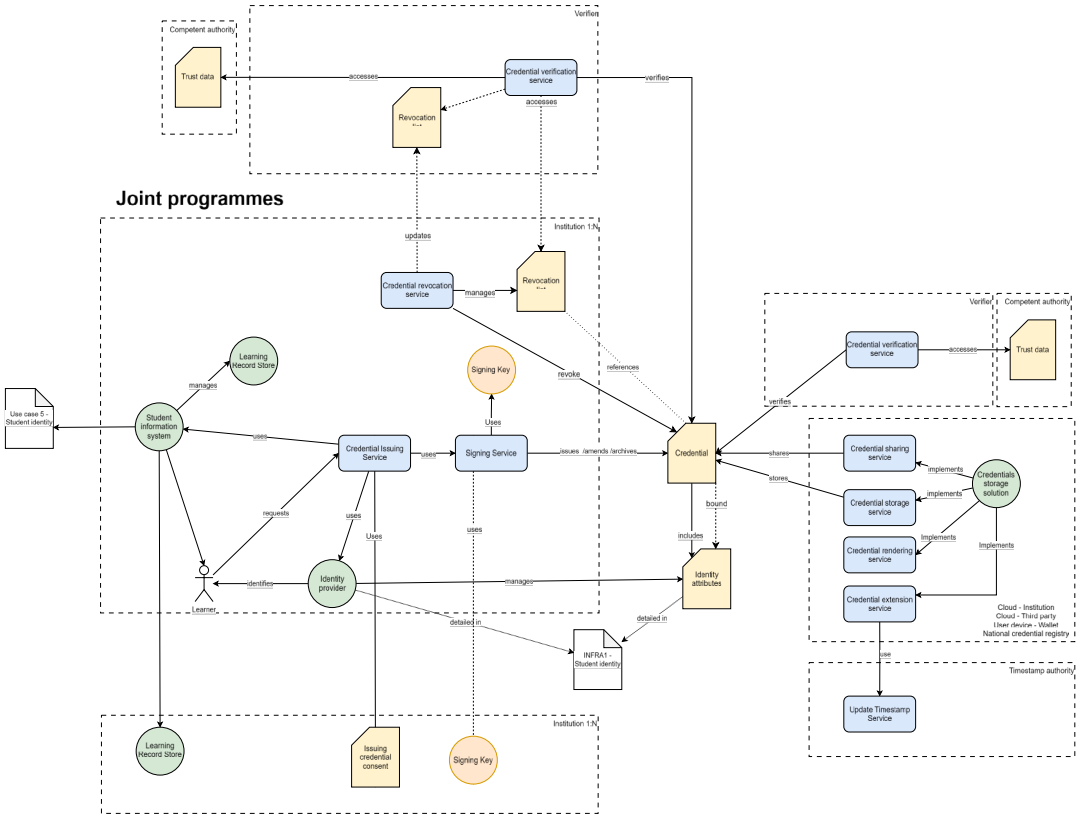


Figure 57 Overview of components required to issue, store, share and recognize educational credentials - Joint programme.
© 2025 European Union

Finally, the following architecture diagram shows a mobility scenario outside the framework of joint programmes. To create a common credential, the learner's home institution must include credentials from third parties. These third-party credentials need to be embedded in a credential that the home institution signs. This embedding process requires a sub-process to verify the credentials, confirming both their validity and that they belong to the learner who holds them. This entire process is reflected in the architecture of this scenario.

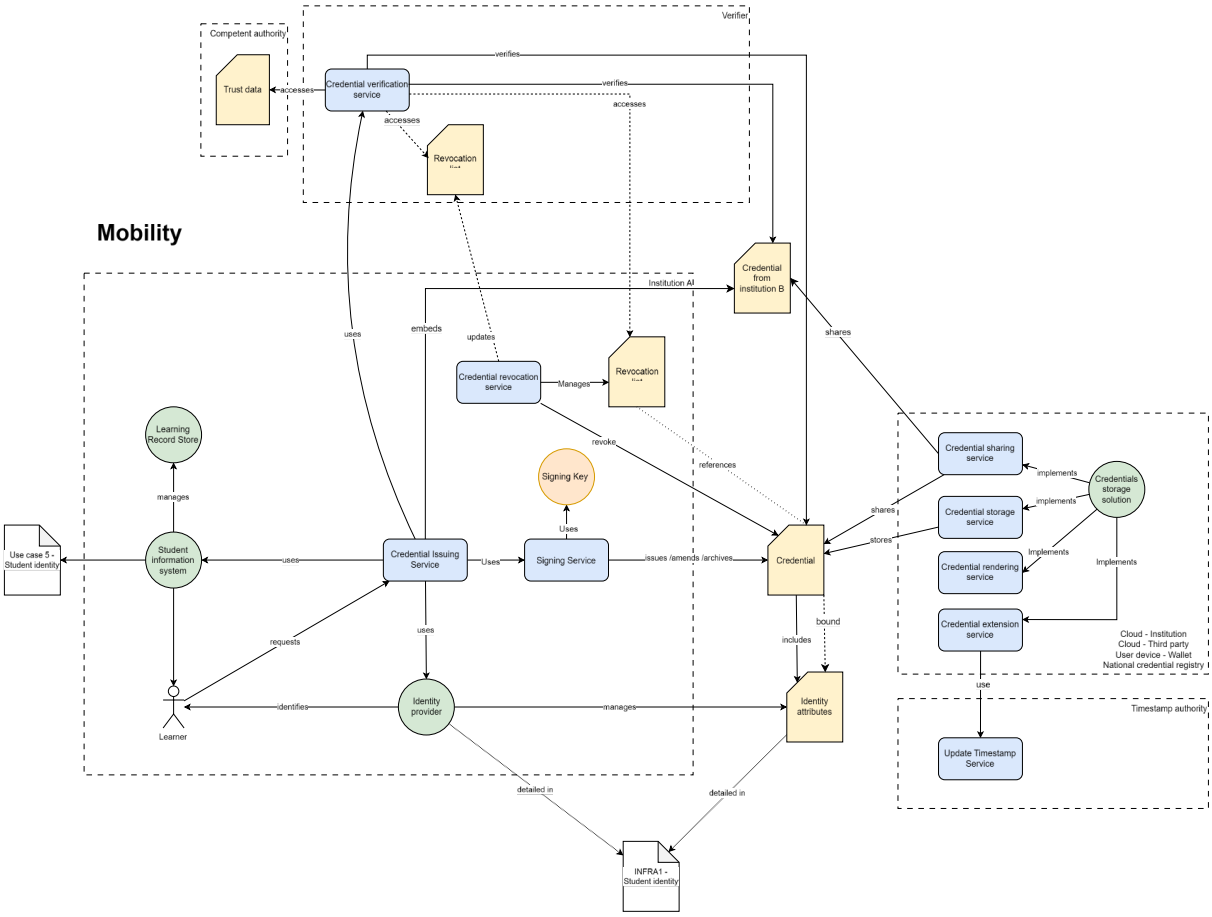


Figure 58 Overview of components required to issue, store, share and recognize educational credentials - Mobility scenario.
© 2025 European Union

6.4 Reference architecture

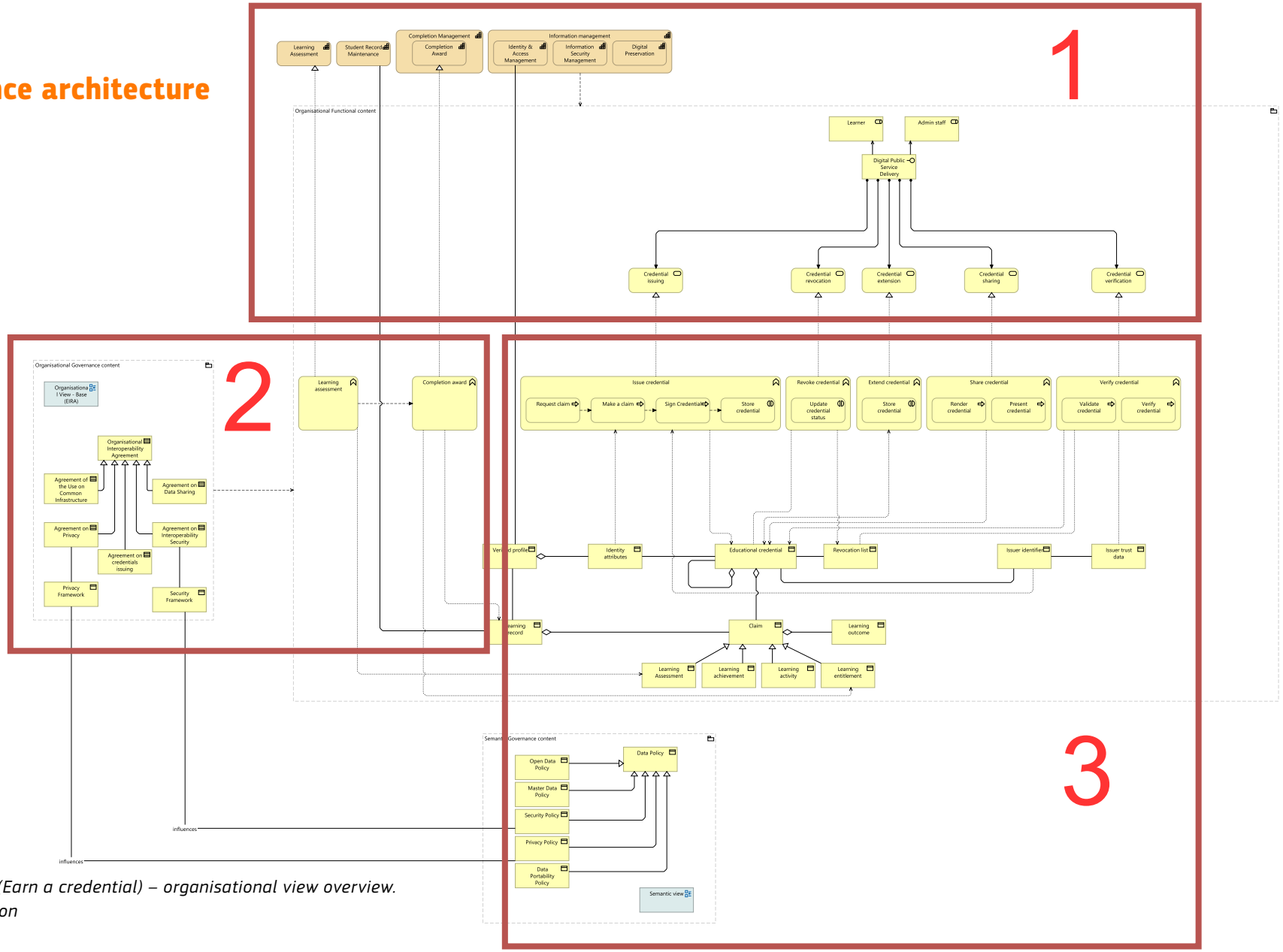


Figure 59 Use case 6 (Earn a credential) – organisational view overview.

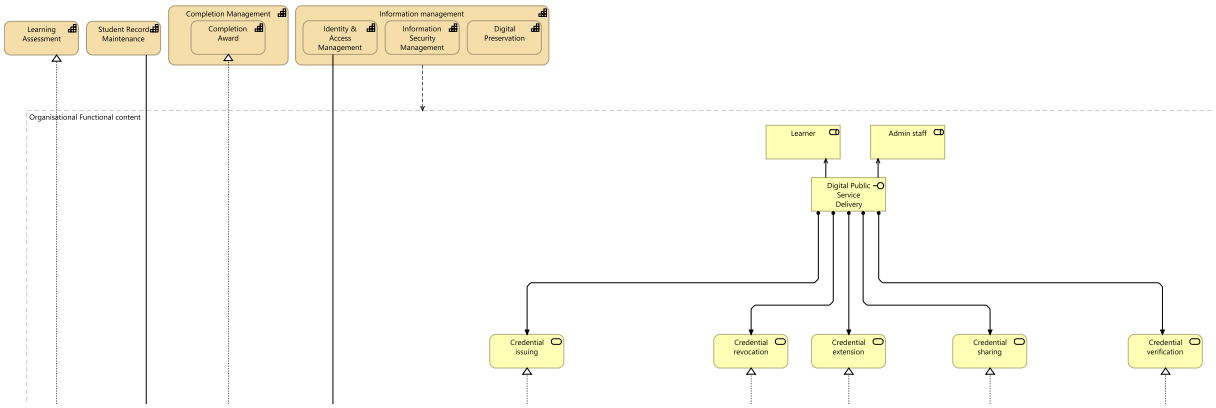


Figure 60 Use case 6 (Earn a credential) – organisational view - part 1.
© 2025 European Union.

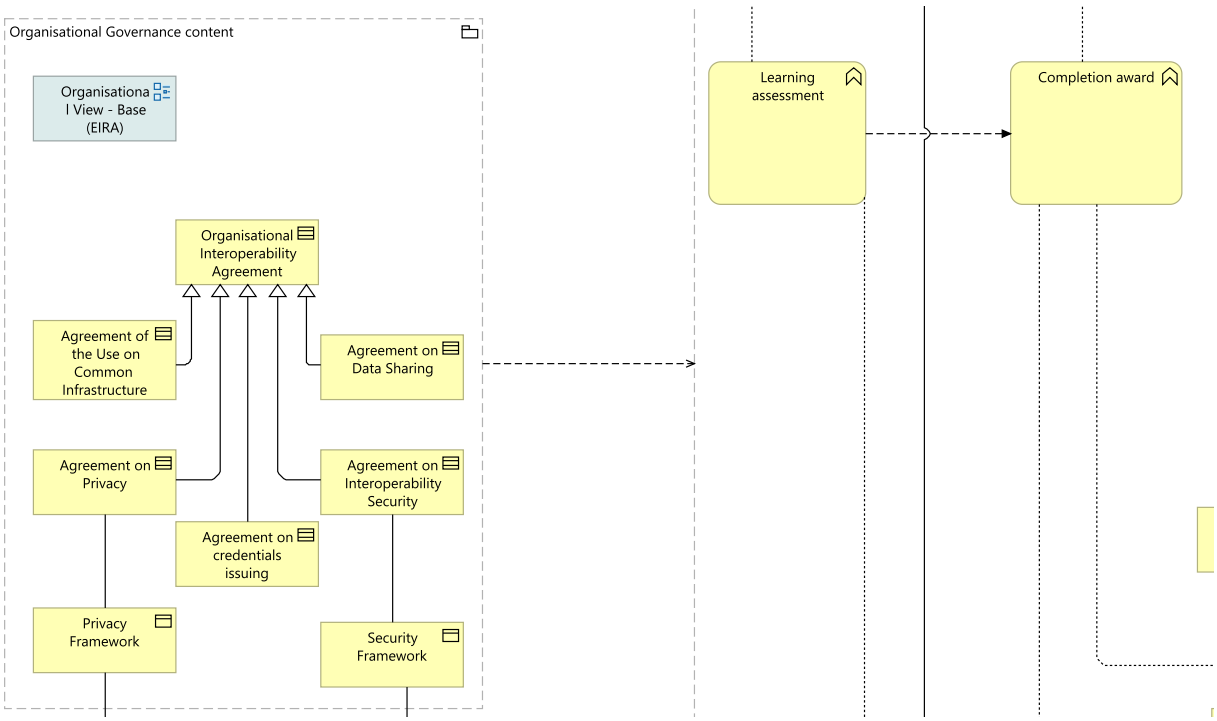


Figure 61 Use case 6 (Earn a credential) – organisational view - part 2.
© 2025 European Union.

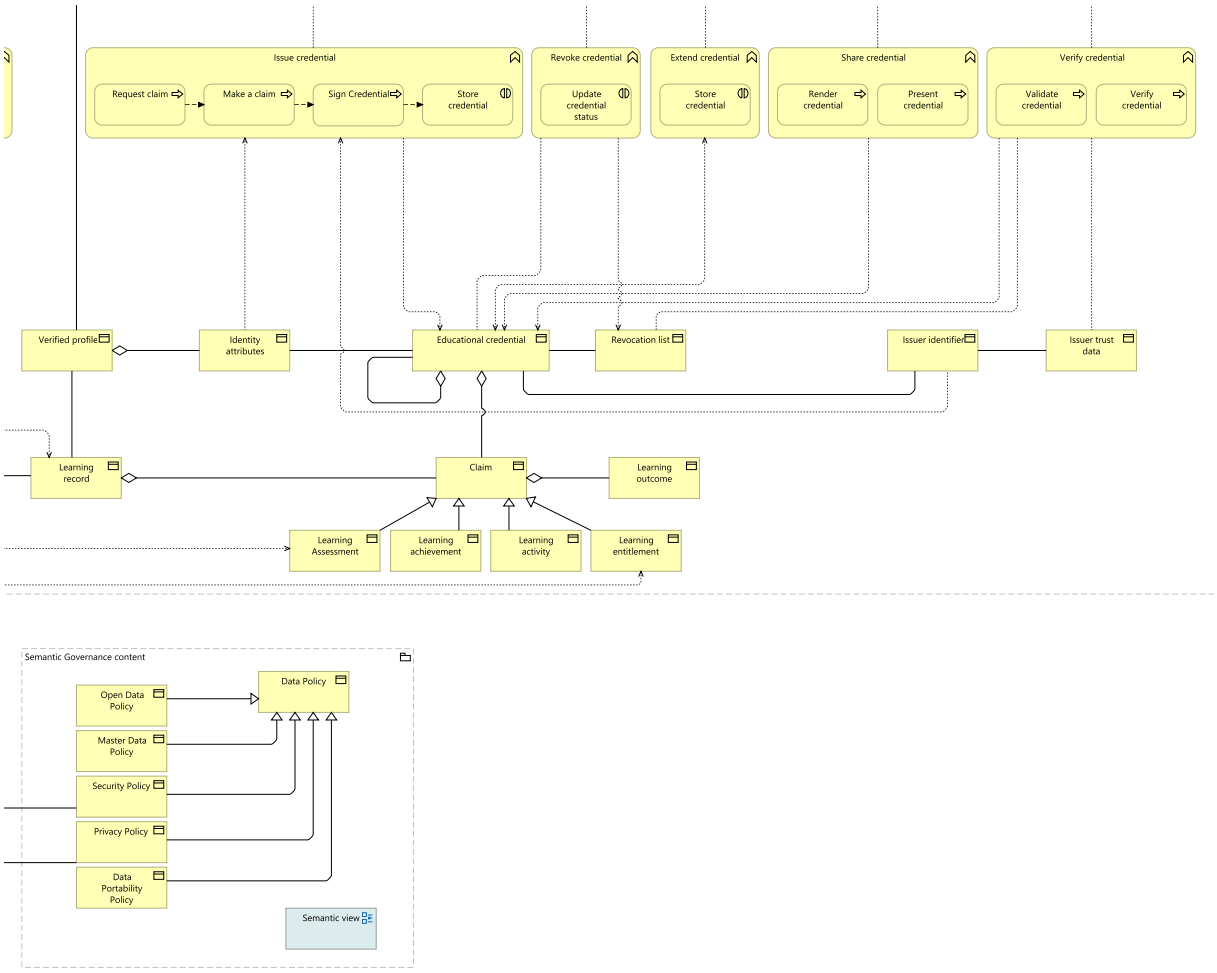


Figure 62 Use case 6 (Earn a credential) – organisational view - part 3.
© 2025 European Union

Use case 6 presents a reference architecture at the business layer that is slightly more complex than the others. This complexity arises from the need to manage different capabilities. It is not just about generating, issuing, and recognising credentials. It also involves the entire security framework that supports these data flows. This use case also contains a significant amount of content related to organisational governance. This is due to the need for organisational interoperability agreements that implement aspects related to privacy, security, and data sharing. As with previous use cases, these organisational-level agreements represent pain points in achieving interoperability. This is primarily due to factors such as differing data protection legislation across countries. Such factors can hinder institutions seeking agreements. They pose issues over which institutions may not be able to act swiftly or directly.

In the following table, the most prominent building blocks are described.

Building block	Type	Description
Learning assessment	Capability	The learning assessment checks students' knowledge of learning outcomes in all delivery modes. This includes blended learning, work-based learning, and work-integrated learning.
Student record maintenance	Capability	The student record maintenance keeps track of each student's information. It shows their achievements and attendance permanently.
Completion management	Capability	The completion management confirms and recognises the completion of study.
Information management	Capability	The information management describes, organises, distributes, and governs information.
Issue credential	Business function	The issue credential covers the steps to create a credential. This includes making, signing, and storing it.
Revoke credential	Business function	The revoke credential updates both the revocation list and the status of the credential during the process of revoking a user's credential.
Extend credential	Business function	The extend credential extends the validity of issued credentials.
Share credential	Business function	The share credential presents credentials in a readable format, making them accessible for sharing.
Verify credential	Business function	The verify credential checks and confirms credentials using trust data from the issuer identifier that issued the credential.
Educational credential	Business object	A credential is an attestation, evidence, or proof of qualification, activities, assessments, or entitlements.
Revocation list	Business object	A revocation list is a list of credentials that have been revoked by the issuing authority.
Claim	Business object	A claim is a statement made by an issuer.
Organisational interoperability agreement	Contract	The organisational interoperability agreement formalises governance rules that enable collaboration between digital public services, facilitating seamless interoperability.
Issuer trust data	Business object	The issuer trust data is the information required by a verifier to validate that the issuer of a claim is accredited, ensuring the authenticity and validity of a credential.

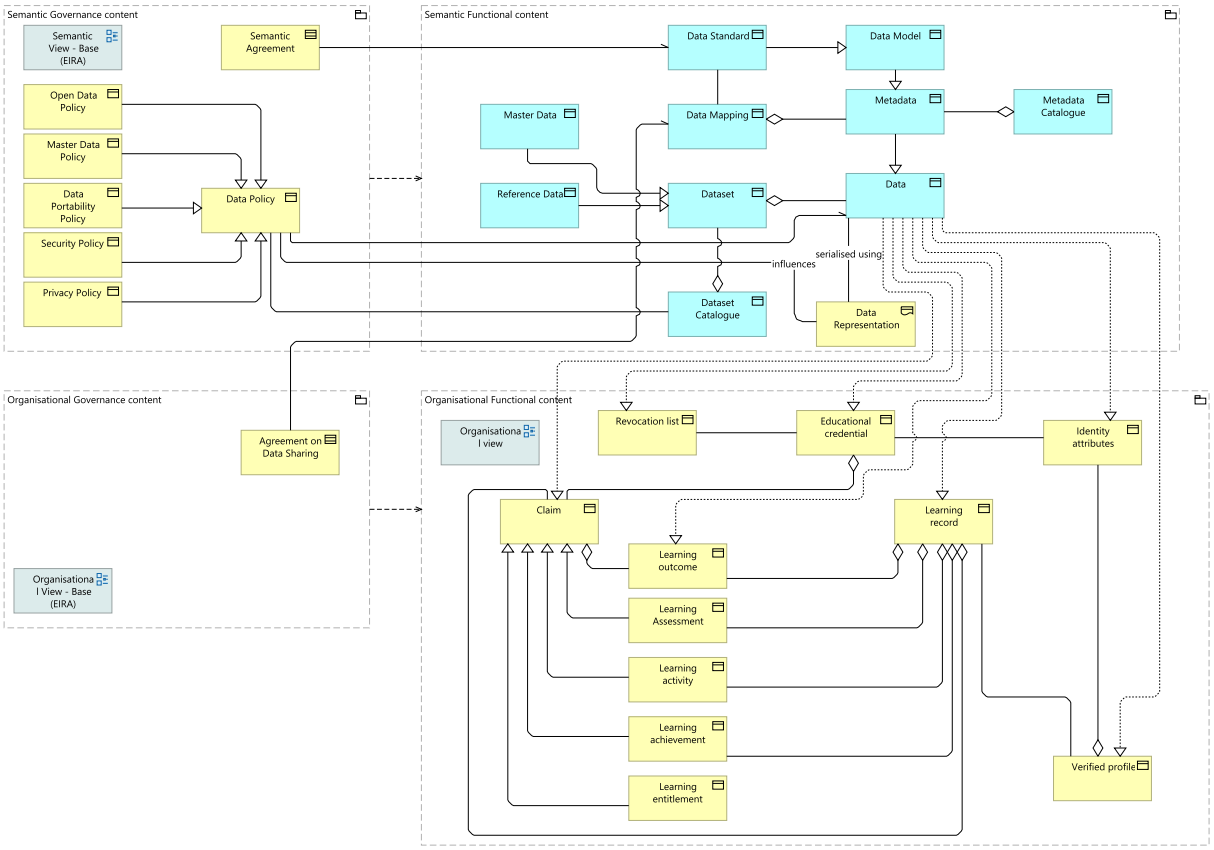


Figure 63 Use case 6 (Earn a credential) – semantic view.
© 2025 European Union

The semantic layer in the ArchiMate model for this use case directly affects the building blocks of the technical layer. Managing credential-related information involves sensitive data. This requires security, privacy, and data portability policies, among others. These policies are always accompanied by semantic and data-sharing agreements to ensure proper handling and interoperability.

To adapt the current model to an interoperable solution, we have linked the data object “Data” to the main business objects in the organisational layer. This lets them use standard data models. These are organised into interoperable catalogues and datasets. It also includes mapping functions.

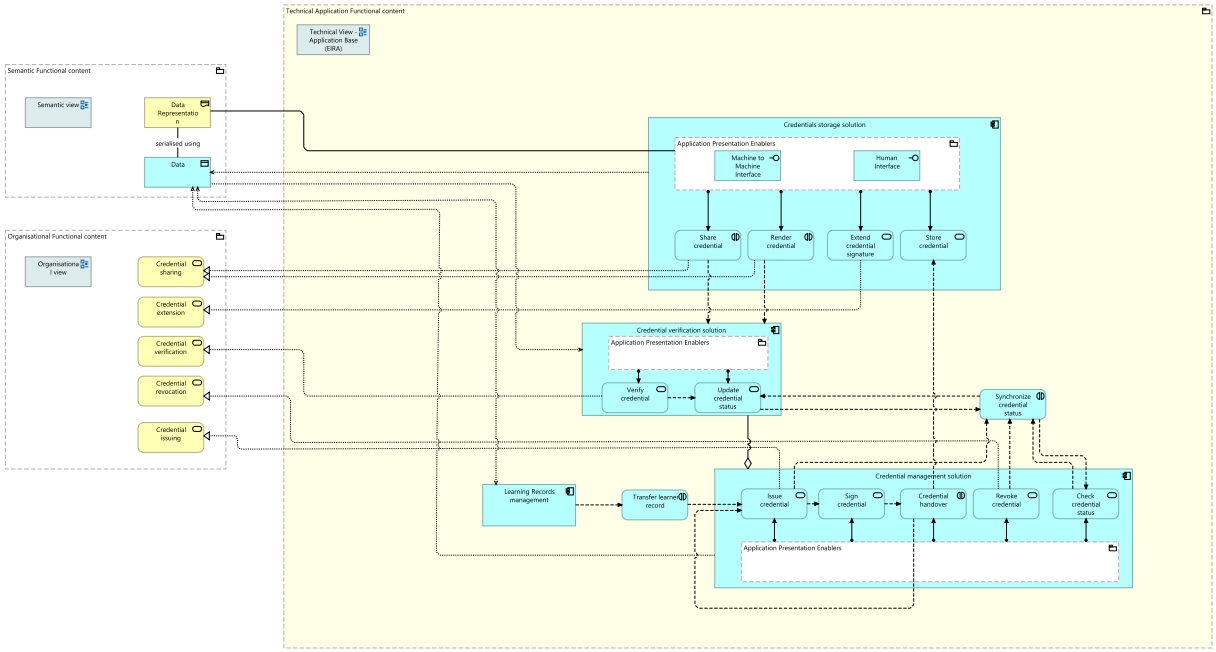


Figure 64 Use case 6 (Earn a credential) – technical view.
© 2025 European Union

This architecture has three main components: the credentials storage solution, the credential verification solution, and the credential management solution. These flexible building blocks can work with existing systems, like wallets or traditional credential management tools, such as national repositories or institutional stores. The main challenge is adopting and integrating these new credential management models. Most difficulties arise in the other two layers.

The following table describes the most prominent building blocks.

Building block	Type	Description
Credentials storage solution	Application component	The credential storage solution handles storing and managing certain parts of the credential. It interacts with other application components by sharing the credential and making it accessible in a readable format. This application component is adaptable to any type of available solution, such as a national registry or a wallet, for example.

Credential verification solution	Application component	The credential verification solution interacts with other application components to validate shared credentials. If necessary, it update their status.
Credential management solution	Application component	The credential management solution issues and signs credentials related to a specific learning record. The record can for example represent a complete course or a part of one. It also revokes issued credentials when necessary.
Learning Records management	Application component	The learning records management represents solutions such as an LMS (Learning Management System) or LRS (Learning Record Store).

For more details on the ArchiMate building blocks in this diagram, check the blueprint reference architecture report. It has all the important information about these schemes.

6.5 Interoperability required capabilities

The interoperability among higher education institutions (HEIs) for managing student credentials involves several steps. It relies on standards and technologies that ensure the validity, security, and recognition of these credentials.

After a learner finishes a learning assessment and earns a learning achievement, they can claim a credential. This credential reflects the claims of the learning achievement. To ensure that a claim is recognised by different institutions, there must be a prior agreement. This agreement establishes standards for learning outcomes, ensuring that the learning achievement meets the expectations of all parties.

The issuing institution must collect the necessary data from the student and the achievement it is going to certify. This includes the student's name, the completed learning assessment, the results, and the skills gained. It also covers the date of issue, the credential's validity, and the institution's identification. To access the student's data, the service generating the credential must have access to the Student Information System (SIS). The generated credential will contain the previously described metadata. It must have a standardised format that is readable and interoperable. To ensure authenticity and that the credential has not been altered, the institution must digitally sign using its digital certificate.

When choosing a solution for storing, verifying, and sharing generated credentials, the following capabilities must be considered:

- **Data Security:** A secure storage of credentials, including both student and institution data and credential details, is essential. This includes elements such as data encryption, user authentication, and access control. It is also essential to maintain the integrity of the stored data by preventing unauthorized changes.
- **Identity Management:** Identity management capabilities are required to verify the identity of users accessing the system and to ensure the correct use of stored credentials.
- **Verification Functionality:** A service that allows third parties to verify the authenticity of a credential is needed. This implies a validation of the digital signature, the integrity of the data, and the source of the credential.
- **Interoperability:** The system must be compatible with interoperability standards to facilitate its integration with other systems.
- **Audit:** The system must have a detailed record of all activities related to the credentials (e.g., issuance, verification, validation, revocation).

Standard communication protocols should be used that allow the secure and reliable transmission of data between systems, considering the sensitivity of the data shared in this use case.

For more information on the interoperability capabilities of this use case, please refer to the comprehensive final mapping report.

6.6 Recommendations – use case 6

Several key recommendations for credential issuance by HEIs have come from the community live sessions. These recommendations aim to enhance the security, reliability, and interoperability of credentialing systems. They also focus on aligning with new technologies and frameworks.

- **Adopt modern technologies for credential management:** HEIs should prioritise the adoption of modern technologies such as digital wallets to manage and store credentials. This aligns with the European agenda for digital transformation, which encourages the use of portable and secure digital credentials. Digital wallets offer a flexible and future-proof solution that allows learners to hold, manage, and share their credentials in a decentralised and secure manner.
- **Enable selective disclosure of credentials:** Solutions adopted for holding credentials, such as digital wallets, should enable learners to choose which specific parts of their credentials to share

with third parties. This approach is essential for protecting learners' privacy while allowing for flexibility in the verification process. For instance, when applying for a job or further studies, a learner might only need to disclose certain courses or qualifications rather than the full credential.

- **Verify identities in multi-signed credentials:** When issuing multi-signed credentials, HEIs must rigorously verify the identity of the person holding the credential before signing it. This ensures the integrity of the credential and prevents cases of fraud. Institutions should use strong identity checks. They can use secure digital identity systems to make sure the person claiming the credential really holds it.
- **Establish a clear revocation process:** The revocation process of credentials should always be carried out by the issuing institution. HEIs need to establish clear processes and policies for revoking credentials when necessary. The issuing institution has the authority and responsibility to maintain the credibility of its issued credentials.
- **Avoid using LMSs for issuing and holding credentials:** It is not recommended to use Learning Management Systems (LMSs) to issue or hold credentials in the context of higher education. LMSs are primarily designed for course management and learning delivery, rather than serving as secure systems for credential storage or issuance.
- **Maintain a trusted list for credential issuers:** A critical issue in the credentialing landscape is establishing trust in the credential issuers. It is essential to have a mechanism for verifying that the institution issuing a credential is legitimate. One solution is the integration of DEQAR (Database of External Quality Assurance Results) with the EDC (European Digital Credentials for Learning) ecosystem.
- **Address versioning issues with EDC & ESCO:** HEIs should keep up with the latest versions of the European Digital Credentials (EDC) and ESCO (European Skills, Competences, Qualifications and Occupations) frameworks. This means they may need regular technical reviews and updates to their credentialing systems. Doing this helps prevent disruptions from version mismatches.

By following these recommendations, HEIs can improve their credentialing processes. This will align them with European initiatives for digital transformation in education. Key steps include adopting digital wallets, ensuring selective disclosure, and maintaining strong identity verification. Also, using trusted issuer lists helps create secure and reliable credentialing systems. Additionally, keeping updated with EDC and ESCO changes will help institutions avoid technical issues and ensure smooth operations.

The context of credential issuance by HEIs, several key recommendations have been collected through all the different community live sessions. These focus on ensuring the security, reliability, and interoperability of credentialing systems, while aligning with new technologies and frameworks.

PART 7

Use case 7 – User identity

7 Use case 7 - User identity

USE CASE 7

User identity

© 2024 Freepik

Achieving interoperability for user identities across educational transitions, ensuring consistent identification throughout their academic journey.

Access | Federated identity | Student cards

7.1 Use case definition

This use case is the first of two supporting use cases, which means interoperability in this case is a basic requirement for most of the core use cases (1 – 6). The importance of this use case for many others is also clear from the numerous references in the flowcharts and architecture diagrams above.

A single user identity allows easy access to tools and services. It also helps learners see how their data is used and by whom. Many universities, alliances, and European initiatives have made progress toward this goal.

Still, more work is needed for complete interoperability of learner identities during educational transitions. This means consistent identification throughout a learner's academic journey. In this use case, we aim to facilitate the transfer of user attributes that can be used to infer roles and automate the management of permissions and access rights based on them.

7.2 High-level flow

Identifying, authenticating, and authorizing users is crucial for every other use case. In the Design Thinking workshop, experts discussed the concept of verified profiles. These verified profiles combine a person's identity attributes with institution-specific attributes, such as their roles or access rights.

Verified profiles can include a wide range of attributes that different institutions can share, update, and remove. A verified profile uses data from the student information system. It helps create local accounts, but local authorisation processes stay the same.

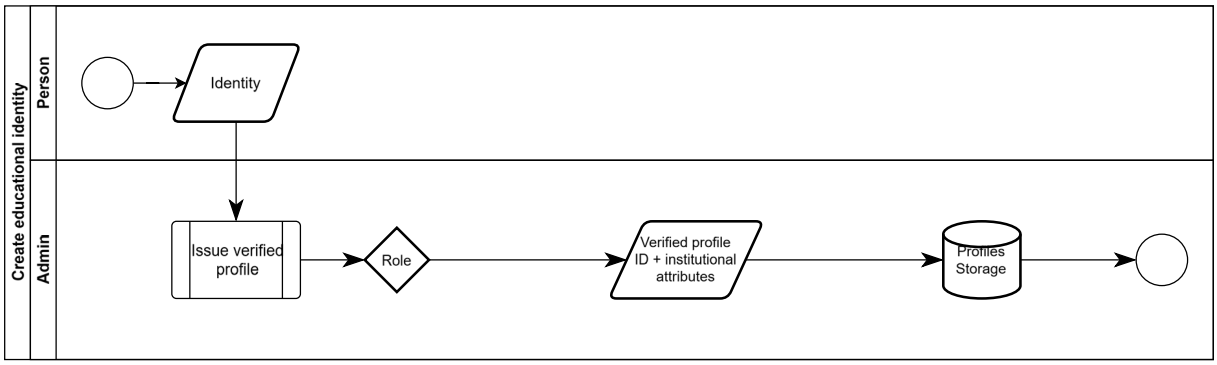


Figure 65- Steps required to issue a verified profile based on identity attributes.
© 2025 European Union

When people join an institution, they provide their identity attributes and details needed to verify their identities. With this information, a verified profile is created for them. Depending on their role, specific institutional attributes are added to their verified profile. These attributes may determine the access rights they need when interacting with different systems, among other things. Access rights can come from different sources. They may result from internal processes like enrolling in a learning offering or becoming a staff member. They can also come from being granted access to a specific tool or asset, as shown in use case 3 (access tools).

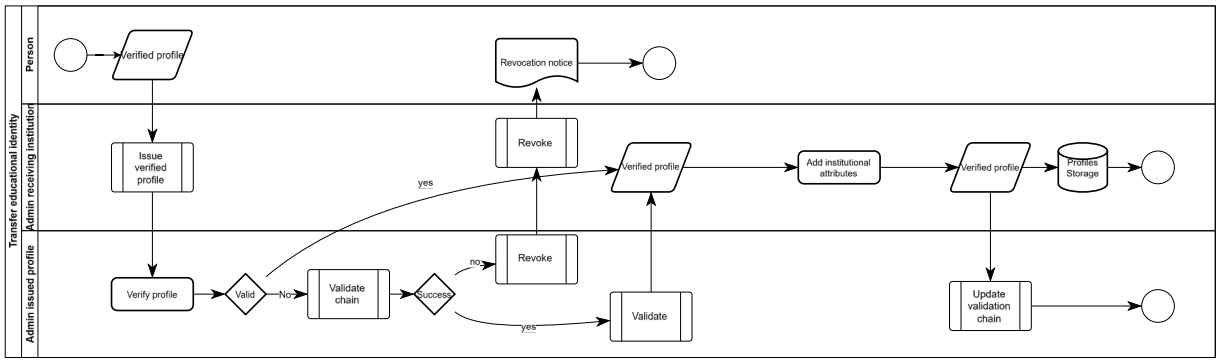


Figure 66 - Steps required to transfer a verified profile between institutions.
© 2025 European Union

People **moving** between institutions can show their verified profiles. This helps them access local systems at another institution, for example when using a tool from a different institution in their EU-A. This process depends on trust between institutions. The receiving institution may only accept profiles from institutions in their trust network.

The process of issuing an additional verified profile (by the receiving institution) begins with a request to verify the existing profile sent to the issuing institution. If the verification process is successful, a new record is stored in the local profiles' storage. This record will incorporate additional local institutional attributes based on the user's role in the receiving institution (and resulting access rights).

Once the new verified profile has been issued, the original issuer may be notified to update the profile validation chain. Validation chains can include information about all the profiles issued based on that verified profile. This information is later used to notify and propagate changes to the original profile's validity. If the verification process fails, a new verified profile must be issued as described in Figure 65 - Steps required to issue a verified profile based on identity attributes.

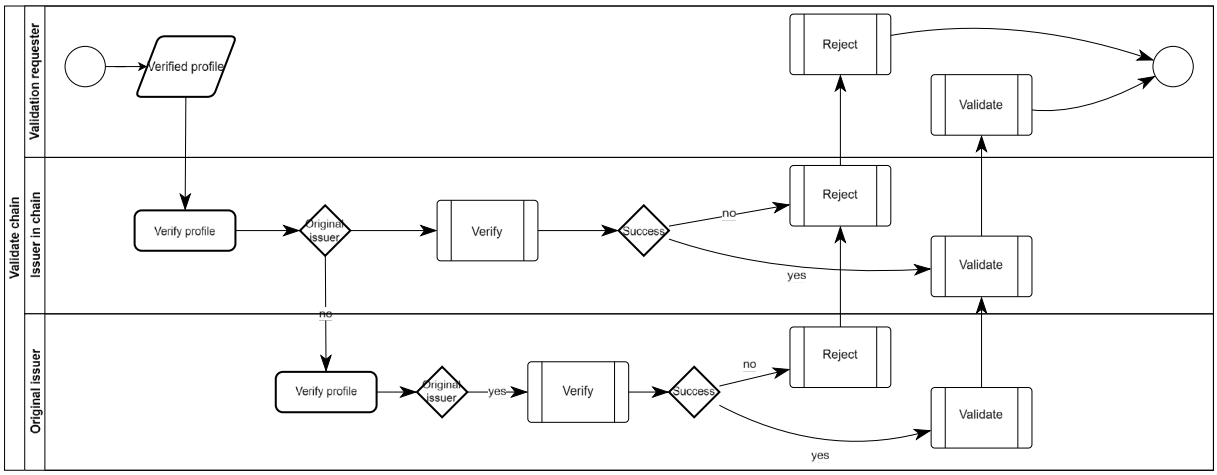


Figure 67 - Validation of an existing profile process.
© 2025 European Union

Institutions receiving a verified profile must validate it before they can accept the data it includes. As mentioned earlier, a single verified profile can be used to issue multiple local profiles, creating a validation chain. To verify an attribute, we follow the validation chain until we find the original issuer of the attribute. The original issuer then checks the validity and veracity of the required attributes, either validating the data or rejecting the validation request.

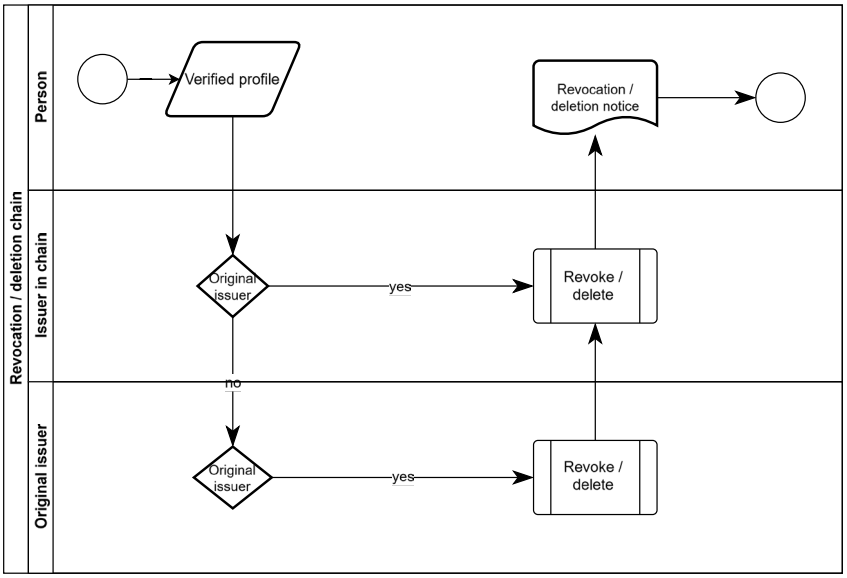


Figure 68 - Steps required to remove information from a verified profile.
© 2025 European Union

Attributes incorporated to a verified profile can be removed or revoked by the original issuer. This process requires propagating the change to all the institutions in the validation chain.E.

7.3 Draft architecture

This use case enables the transfer of user data needed to identify, authenticate, and authorise users between institutions. It is essential to distinguish between the following concepts:

Business objects:

- **Identity:** A data object containing the attributes required to distinguish one person from others.
- **Verified profile:** A combination of identity attributes and institution-specific attributes, such as roles or access rights, belonging to a person.
- **Validation chain:** Information about other verified profiles issued based on attributes incorporated into the verified profile by that institution.

Services:

- **Verified profile issuing service:** This service manages the creation of a verified profile. It can use identity attributes or pull details from an existing verified profile from another institution. It implements the issuing processes shown in Figure 65 - Steps required to issue a verified profile based on identity attributes and Figure 66 - Steps required to transfer a verified profile between institutions.
- **Verified profile transfer service:** This service securely shares an existing verified profile with another institution.
- **Verified profile validation service:** This service implements the validation process described in Figure 67 - Validation of an existing profile process.
- **Verified profile revocation service:** This service implements the process described in Figure 68 - Steps required to remove information from a verified profile.

Systems:

- **Student information system (SIS):** SIS handles student data. This includes registering students for courses, managing grades, and overseeing transcripts and test data.

The following is the simplified architecture diagram for this use case. This diagram is the result of the work done during the first two squad meetings. After the second squad meeting, it was clear that the diagram grew too complex. It could not fit all the existing solutions, and adding more would make it even less clear. In addition, since this was a foundational use case, the vast majority of the community already had their own developed solutions.

As a result, it was decided to shift the focus of this use case to a practical perspective, focusing on recommendations and the impact of this base case on other use cases. Consequently, the architecture diagram was not further developed. This led to the definition of a Level of Assurance (LoA) for user identity and the minimum required set of attributes for different scenarios.

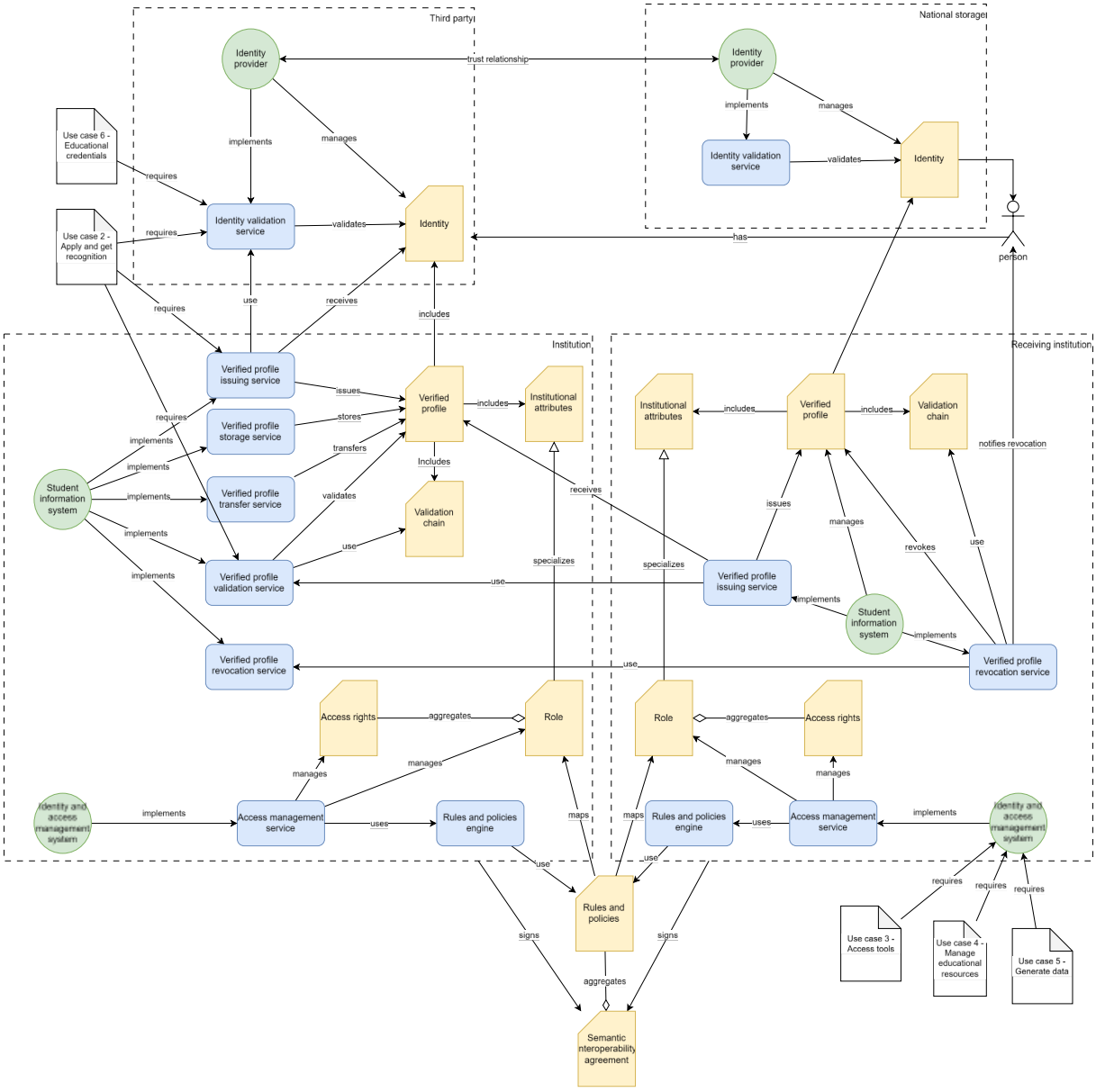


Figure 69 - Main components required to share and manage verified profiles linked to an identity.
© 2025 European Union

7.4 Interoperability required capabilities:

The central identity provider (IdP) must meet various needs to ensure identity validation works across the HEIs in an alliance. The IdP should support identity standards like SAML, OAuth, or OpenID Connect. It should adapt to those already used by the institutions in the alliance. This approach will enable secure sharing of authentication and authorisation information. As a result, HEIs can collaborate and share resources without needing to create unique integrations for each system.

On the other hand, there is the possibility of not centralizing users' identities and instead using a decentralised identity. This approach offers an advantage by reducing the risks of data security breaches, as the information is not centralized, and by facilitating mobility. A student uses a decentralized identity wallet to store academic credentials like degrees and transcripts. When applying to universities worldwide, the student shares only the needed credentials from their wallet. Each institution verifies the credentials on its own. This process does not depend on a central authority, which enhances privacy and simplifies cross-border credential recognition.

For more information on the interoperability capabilities of this use case, please refer to the comprehensive final mapping report.

7.5 Recommendations – use case 7

Most higher education institutions use two types of solutions. The first type is student information systems. These systems manage the creation, storage, deletion, and validation of student data. The second type is identity providers. These services handle user identities and extract permissions and roles. They also provide login solutions for tools, websites, and applications.

Most of the identity providers implement the Single Sign On (SSO) principle, the idea is using just one login to multiple systems. Some identity providers allow institutions to interconnect in a federated way.

Interoperable user identity stands out because it is already backed by popular national and European solutions. Many higher education institutions use these. EduID is a digital identity that works across institutions. It is designed for the education and research sector and is currently used in the Netherlands and Sweden.

Connect to eduGAIN: EduGAIN is an international service that connects identity federations specifically for research and education purposes. It allows users (students, researchers, staff) to access online resources from other institutions around the world with just their own institutional login. This eliminates the need to create separate accounts for each resource, making things easier and more secure. Attributes can be incorporated to the verified profile by the local institution. Many of the specific tools mentioned above are connected to the EduGAIN identity federation network. Institutions that are not part of the eduGAIN federation should explore the possibility of connecting, through their national research and education network (NREN).

The European Student Card (ESC) establishes a common European identity for higher education students. With their European Student Card, students can easily get their student status verified across Europe.

Agree on alliance-wide attributes beyond the minimum eduGAIN profile: EduGAIN has strong single sign-on features. However, some key use cases, like access to tools, need improved interoperability. Specific attributes, such as programme or field of study and status, must be understood consistently across the alliance to apply access policies effectively. A major point to note from the table above is that the absence of a mark in storage service, revocation service... does not mean they do not have those services, but rather that they do not constitute a student information system.

PART 8

Use case 8 – Institutional identity

8 Use case 8 - Institutional identity

USE CASE **8**

Institutional identity

Developing a cohesive framework for trusted institutional identities, facilitating smoother collaborations and exchanges between HEIs.

Accreditation Ranking

8.1 Use case definition

This second supporting use case outlines the framework for trusted institutional identities. It helps higher education institutions (HEIs) collaborate and exchange information more easily. To enable seamless exchange and flow, HEIs need reliable ways to identify each other. This is important whether or not they know each other. An institution's identity includes various attributes. These range from formal ones like accreditation to indicators such as rankings and enrolment data.

The need for a systematic approach to institutional identity arises when HEIs exchange data, especially beyond EU-As. Within an alliance, which usually has fewer than 10 institutions, all members know each other. They can easily verify that each partner is accredited.

The diagrams for this use case are being refined based on feedback from recent squad 8 sessions. The final versions will appear in the comprehensive final mapping report and the updated blueprint reference architecture for the Interoperability Framework.

8.2 High-level flow

Sharing data in a systematic way builds trust between institutions. The main use cases depend on this supporting use case. They need basic institutional identity and accreditation status. This is the focus of this use case and the reference architecture at this stage.

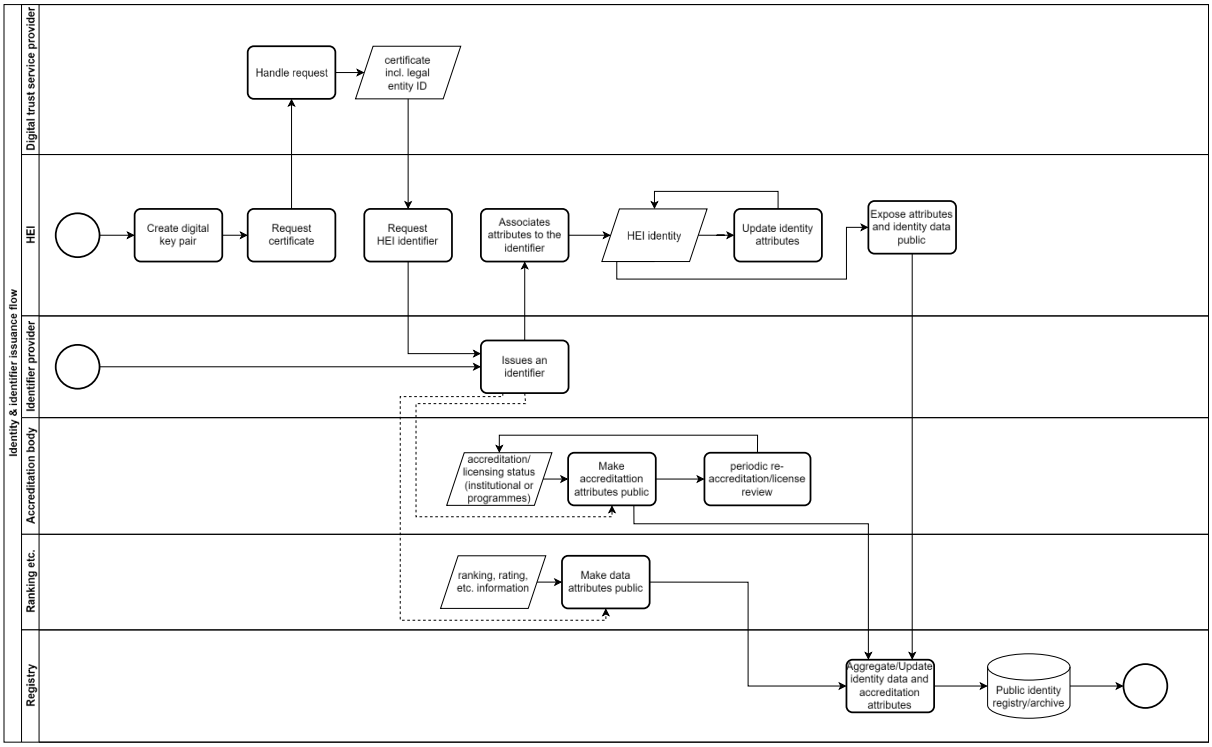


Figure 70 - Steps required to make public institutional attributes.
© 2025 European Union

In the diagram above, the process of obtaining an identity by an institution is represented, considering all parties involved:

- An **identifier provider**, like a national ministry or agency for higher education, gives the institution an identifier. This can happen if the institution asks for it or if the provider does it on their own. The provider also shares this information publicly.
- The **higher education institution** itself may add additional attributes and data to the identifier and publish them; it also requests accreditation or renewal.
- The **accreditation body** decides on the institution's (re-)accreditation and makes the accreditation decision public.
- The **ranking** entity provides additional information to the identity, such as a comparative rating or ranking.

- The **registry** aggregates all institution-related information and maintains it, making it publicly accessible.
- The **digital trust service provider** issues a certificate that the entity can use later to digitally sign assets.

The above process outlines the actions required for an institution to be recognised and registered in a trusted public identity registry. The identity provider is responsible for issuing the institution's identifier, based on the institution's own identifier. The accreditation body and other players, like ranking providers, will reference this identifier. They will link extra details, such as ratings or licensing status. This information will be combined with the institution's core details and the identifier. It will be stored in a public registry that shows all this information. In addition, this registry will manage versioning, recording any updates to these attributes made by the institution or by any of the other actors. A certificate object has also been defined, which includes a legal entity ID. However, it is possible that an alliance may not possess this ID, although this is neither expected nor required for this flow.

The next two flows illustrate typical processes in the validation and use of institutional identity.

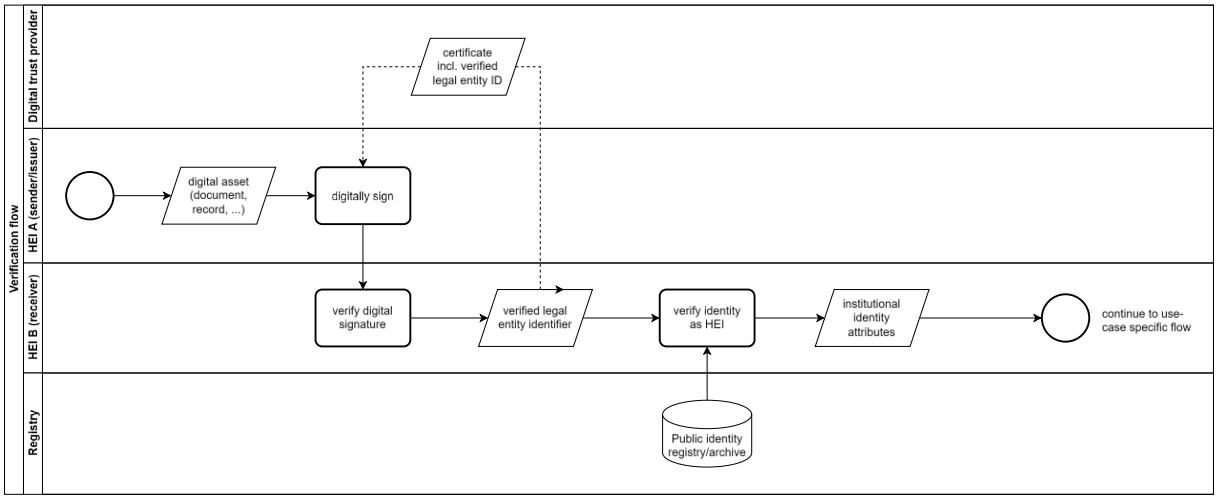


Figure 71 - Steps required to verify an institutional identity.
© 2025 European Union

The diagram above outlines the process of verifying the trustworthiness of the institution issuing a digital asset. The asset is signed with a certificate from a digital trust provider. The receiving institution verifies this signature using a secure public registry storing the institution's data. Once verified, the process can proceed to other use cases, such as use case 2, where an institution receives a credential and confirms the reliability of the issuing institution.

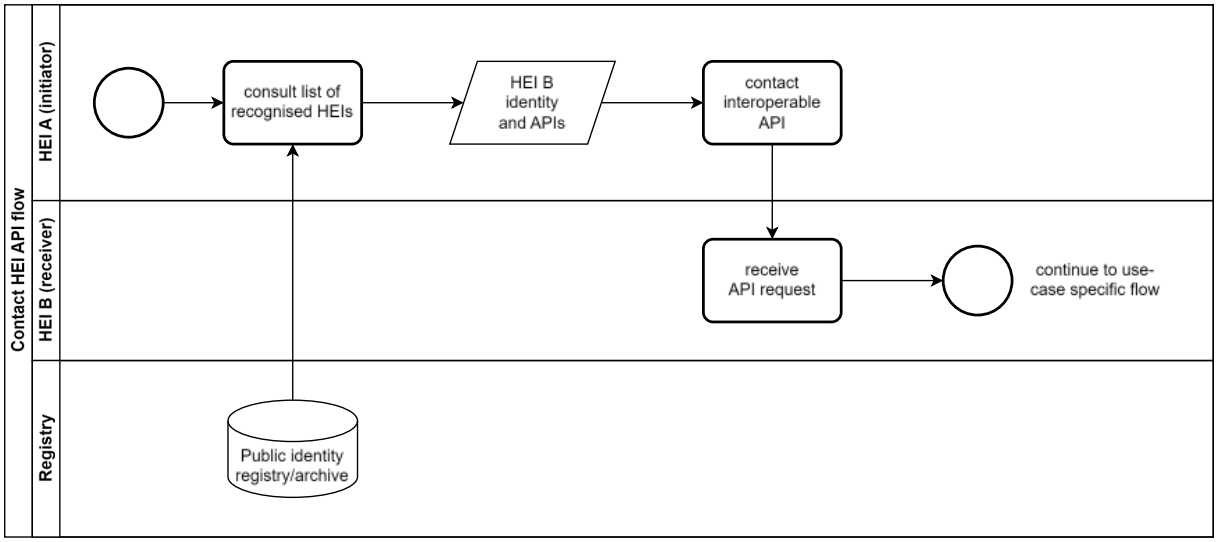


Figure 49 - Steps required to get interoperable API information from an institution.
© 2025 European Union

This flow, the simplest of the three, outlines the steps to make API calls to an external institution. First, the identity registry is queried to obtain a list of trusted institutions. Then, contact is made with the desired institution's exposed API, which provides information on how to integrate with it in an interoperable way. This flow may lead to a more complex one, such as querying the available courses at the contacted institution once the necessary integration information has been obtained.

8.3 Draft architecture

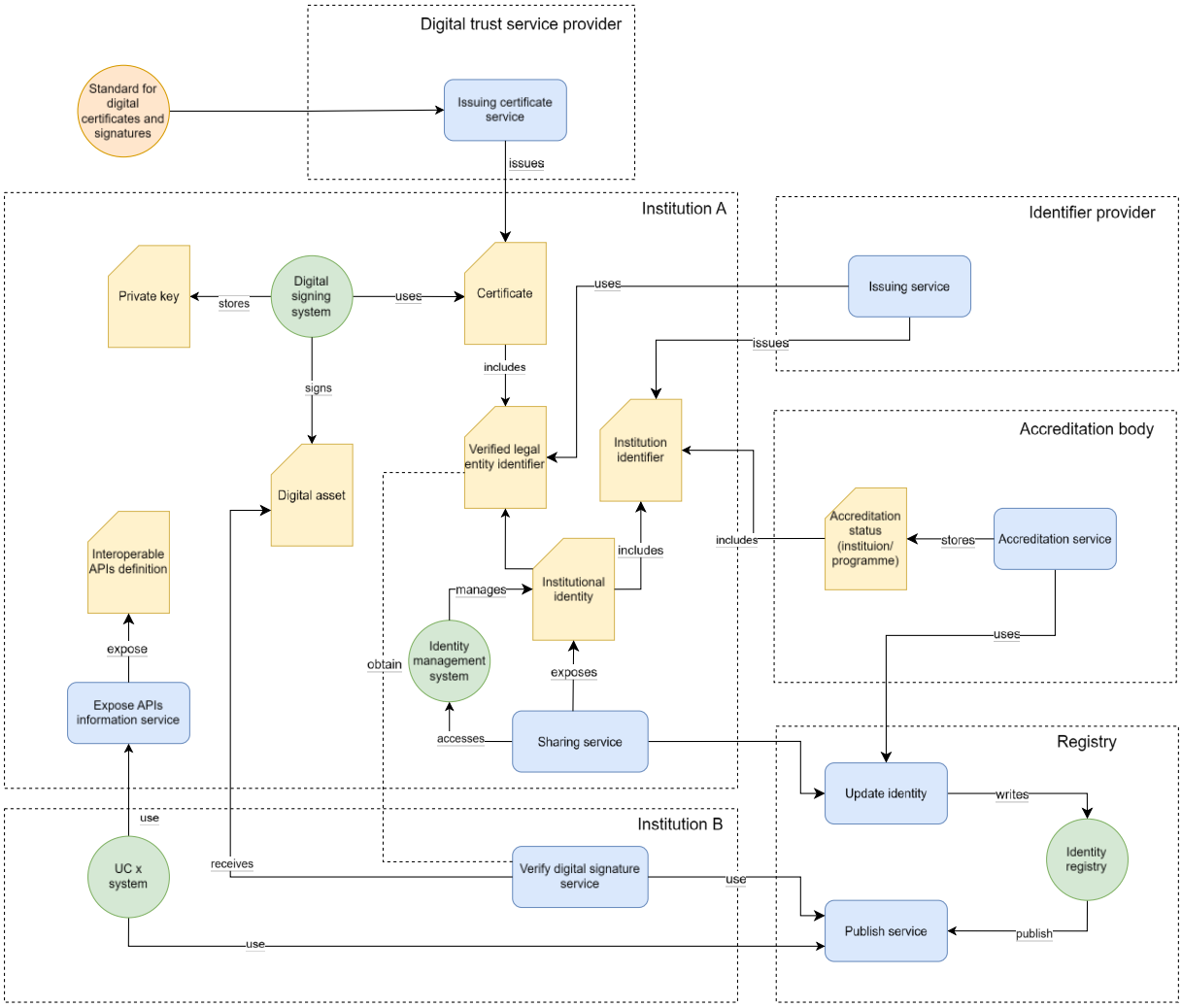


Figure 73 - Main components required to share institutional identity attributes.
© 2025 European Union

This draft architecture shows the key components needed for the high-level flows mentioned before. The following sections detail the key components of this architecture:

Business objects:

- **Institution identifier:** A unique identifier that distinguishes one institution from another.
- **Institutional identity:** A data object containing additional information about the institution.
- **Interoperable APIs definition:** The definition of the interoperable APIs exposed by the institution to facilitate seamless integration with external institutions.

Services:

- **Sharing service:** This service shares identity information and technical details needed for interoperability. This includes the API endpoints of other services the institution offers. You can also find the identity information on the institutional webpage. It may be combined into listings of institutions, including global rankings and those from the ENIC-NARIC networks..
- **Verify digital signature service:** This service validates the signature used to verify an asset from an external entity. It uses the publication service of the identity registry to confirm the verified legal entity identifier of the institution..

Systems:

- **Identity management system:** This system stores and manages institutional identity attributes.
- **UC X system:** This system provides a general representation of the first step required to enable other use cases. This involves contacting the service of the institution that publishes information on interoperable APIs.

8.4 Reference architecture

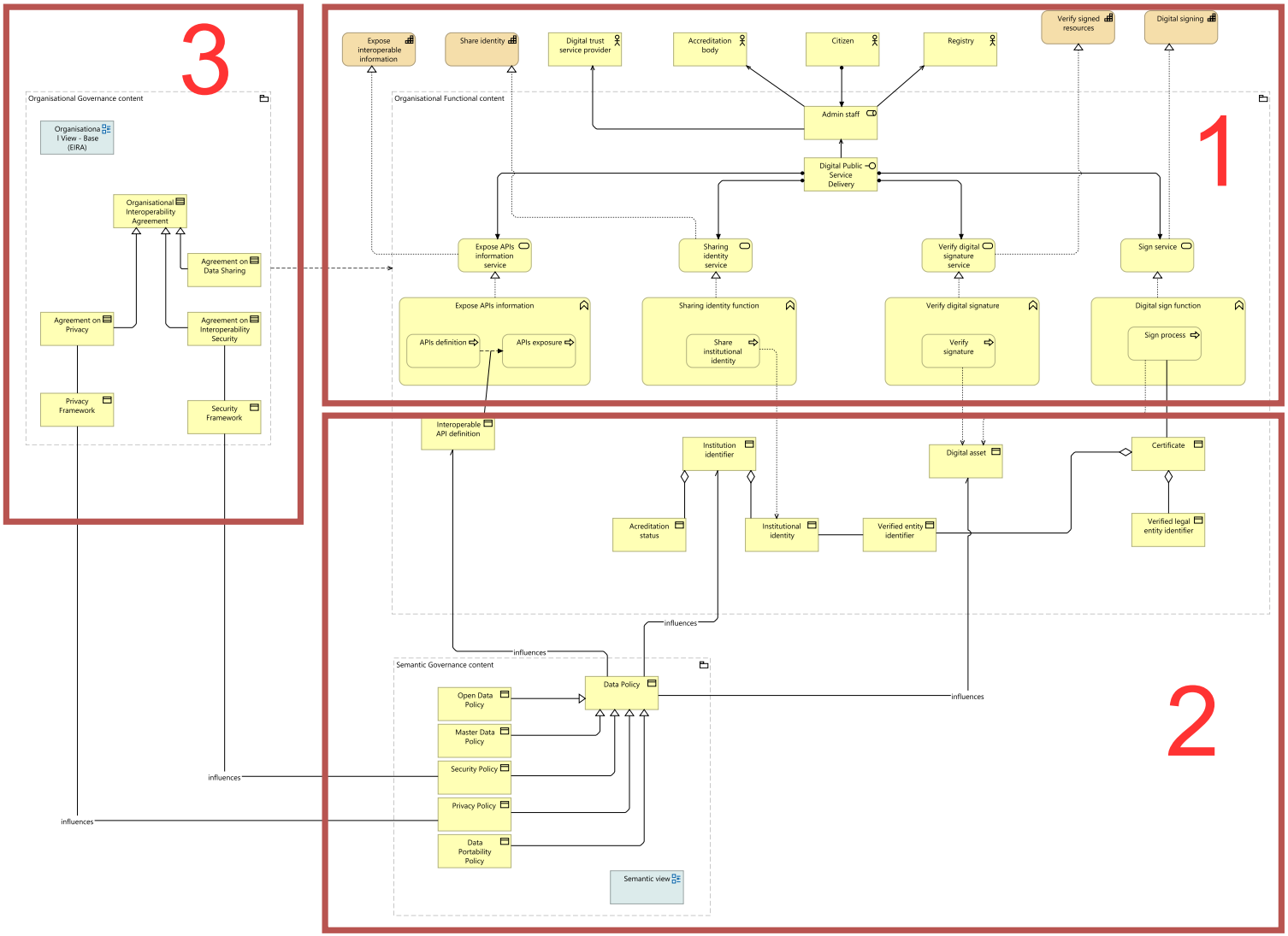


Figure 74 - Use case 8 (Institutional identity) – organisational view overview.

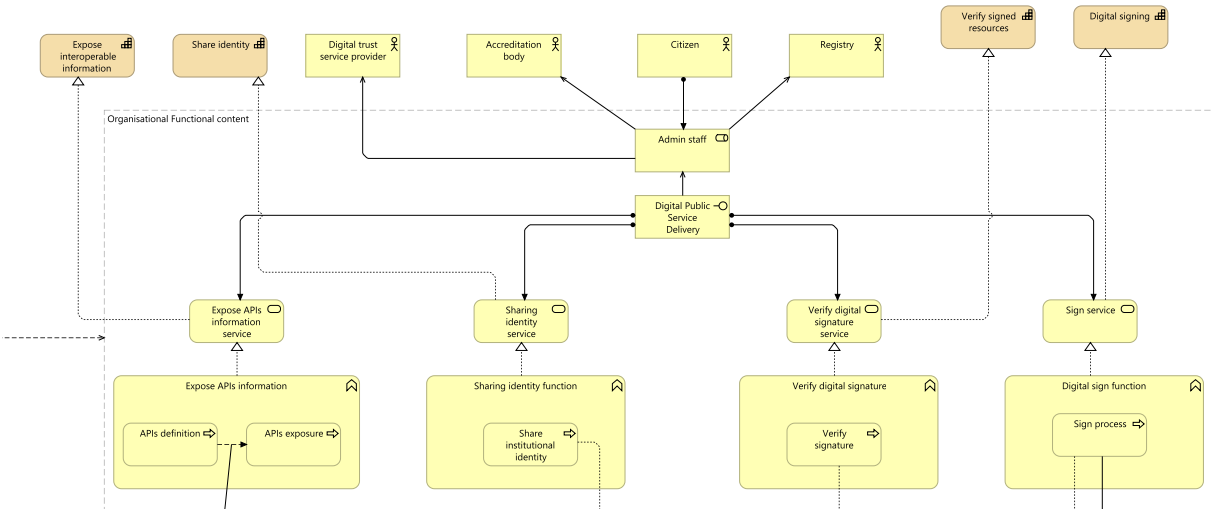


Figure 75 - Use case 8 (Institutional identity) – organisational view overview - part 1.
© 2025 European Union

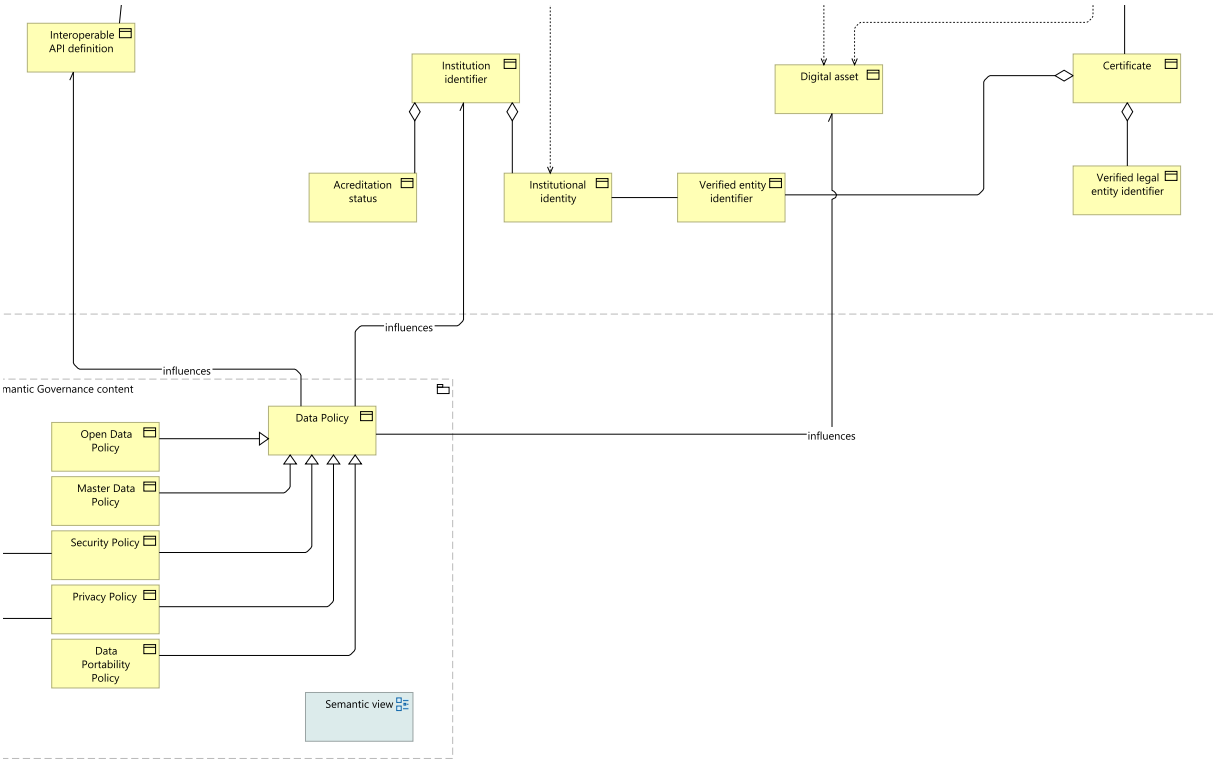


Figure 76 - Use case 8 (Institutional identity) – organisational view overview - part 2.
© 2025 European Union

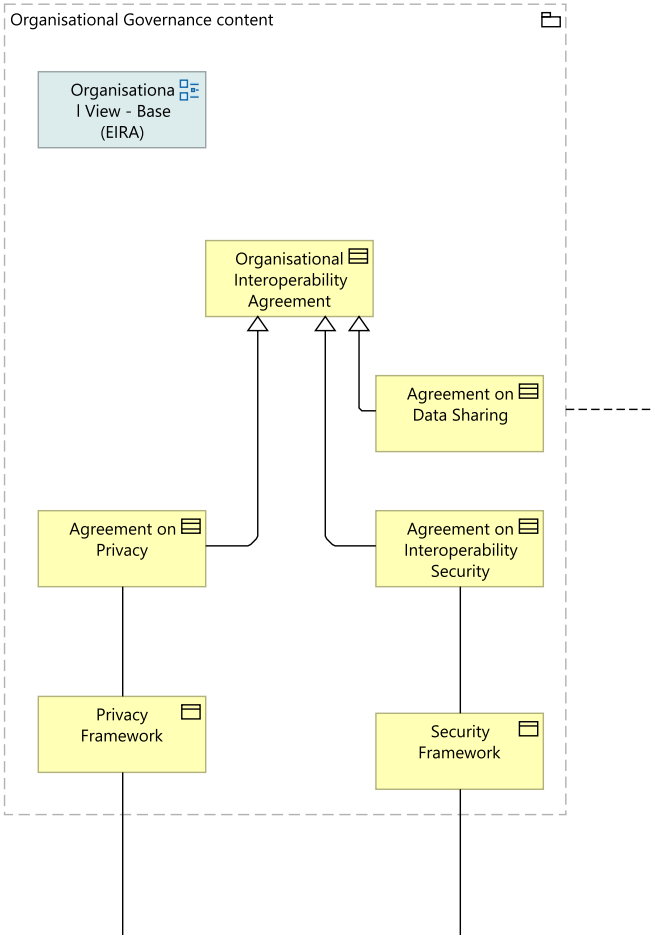


Figure 77 - Use case 8 (Institutional identity) – organisational view overview - part 3.
© 2025 European Union

In the above architecture diagrams, the organisational layer relevant to this use case is shown. The required capabilities identified during sessions with the community and experts on institutional identities are outlined as follows: exposing interoperable information, sharing identity, verifying signed resources, and digital signing. These capabilities are implemented through their corresponding services, which are accessed via a digital interface. Since handling identities and certificates is vital, the components of this architecture link closely to the governance layer. This connection is important for security frameworks and the data policies that govern sharing institutional information.

The following table describes the main building blocks.

Building block	Type	Description
Accreditation body	Business actor	The accreditation body manages and validates the quality and compliance of an institution or program with established standards.
Accreditation status	Business object	The accreditation status indicates whether an institution or program meets the required standards set by an accreditation body.
Digital asset	Business object	The digital asset is a digital representation of data or resources that can be shared or verified within the educational ecosystem.
Digital signing	Capability	The digital signing uses cryptographic methods to sign documents or credentials. This ensures their authenticity and integrity.
Digital trust service provider	Business actor	The digital trust service provider offers services such as digital signatures, timestamps, and certification to ensure trusted transactions.
Expose interoperable information	Capability	The expose interoperable information enables the sharing of data in a standards-compliant manner. It facilitates seamless communication across systems.
Institution identifier	Business object	The institution identifier implements a unique identifier representing an educational institution.
Institutional identity	Business object	The institutional identity represents the attributes, roles, and status of an institution.
Share identity	Capability	The share identity capability enables the secure exchange of identity information between systems or entities.
Sign service	Business service	The sign service provides tools and methods for digitally signing documents or credentials.
Verify signature	Business process	The verify signature process confirms the integrity and origin of a signed document using cryptographic techniques.
Verify signed resources	Capability	The verify signed resources ensure that resources have been signed correctly and have not been tampered with.

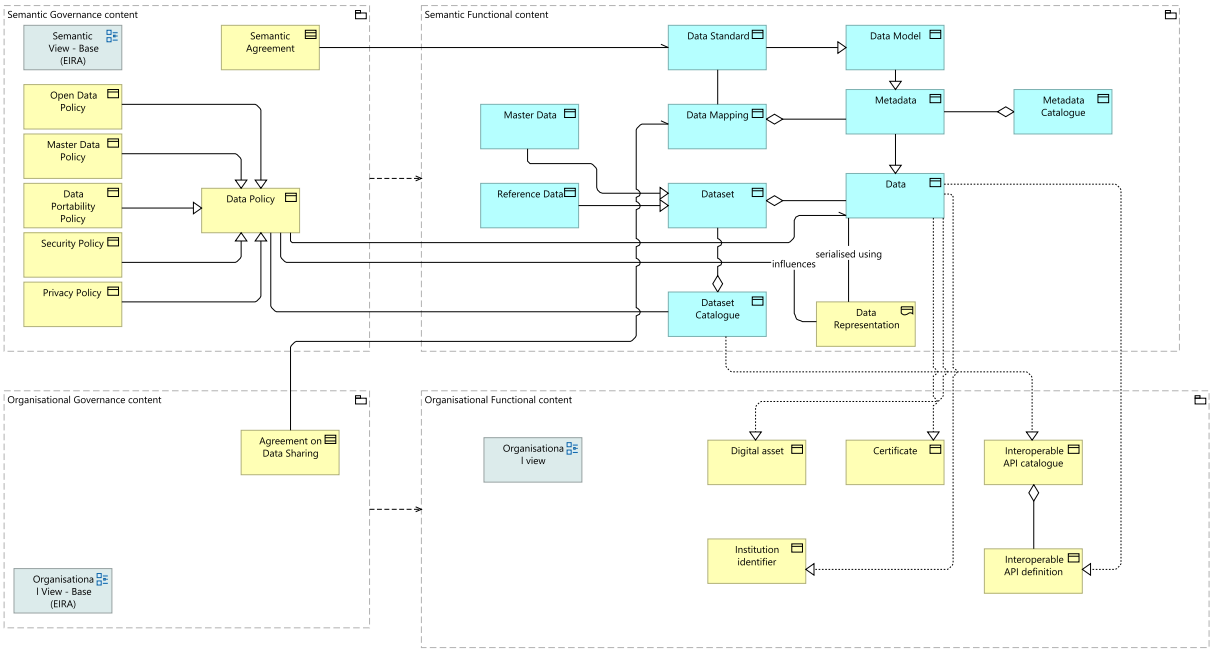


Figure 78 - Use case 8 (Institutional identity) – semantic view.
© 2025 European Union

This view, like other use cases, focuses on a core application object, Data, which is governed by a data standard based on a semantic agreement. From this central data object, specialized business objects are derived, each with their own representations in the technical view.

The following table describes the main building blocks.

Building block	Type	Description
Interoperable API catalogue	Business object	The interoperable API catalogue is a centralised repository that lists APIs designed for seamless system integration and data exchange.

For more details on the building blocks that make up this and other views of the reference architecture, please see the reference architecture report's blueprint.

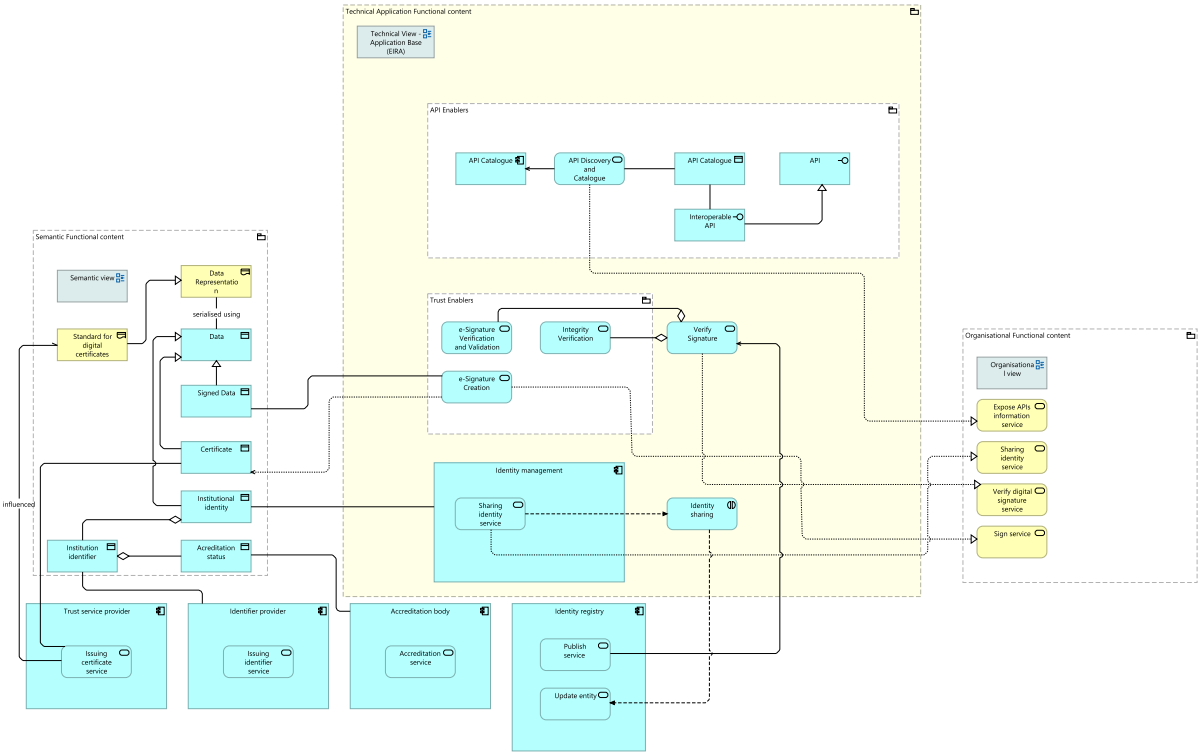


Figure 79 - Use case 8 (Institutional identity) – technical view.
© 2025 European Union

Finally, four distinct blocks are identified from a technical perspective. The first block covers the semantic functional content. This defines application objects linked to services and applications in this layer, focusing on the base object data. The second block includes applications for new actors in the organisational layer. It centres on external interactions like identity storage, entity certificate creation, and accreditations. The third block describes the organisational functional content. This implements the capabilities outlined in the organisational view. Lastly, the central block defines the enablers and applications. These allow the institution to develop the functionalities described by the defined capabilities.

In the following table, the key building blocks are described.

Building block	Type	Description
Accreditation service	Application service	The accreditation service helps validates and recognises that an institution or programme meets quality standards.
E-signature verification and validation	Application service	The e-signature verification and validation enable the process of verifying and confirming that an electronic signature or seal is valid.

Identity management	Application component	The identity management governs the creation, maintenance, and use of digital identities.
Identity sharing	Application interaction	The identity sharing enables the secure exchange of identity information between trusted systems or entities.
Integrity verification	Application service	Integrity verification checks that information has not been changed without permission since it was created, sent, or stored.
Issuing certificate service	Application service	The issuing certificate generates and delivers digital certificates to individuals or institutions.
Issuing identifier service	Application service	The Issuing identifier creates and assigns unique identifiers to entities.
Standard for digital certificates	Representation	The data representation refers to the method or mechanism by which data is encoded and stored in a computer system. This involves the transformation of data from its original form into a format that can be processed and manipulated by a computer.
Trust service provider	Application component	The trust service provider gives secure services like digital signatures and timestamping. It helps ensure trusted interactions and transactions.

8.5 Interoperability and required capabilities

At present, this use case is a low priority for alliances and institutions. The reason is that few institutions in each alliance manage identity based on trust. They do not need an automated method to check each other's accreditation.

However, as the need for interoperability grows, more institutions may join. This will form new trust relationships that require formal validation through certified identities. These identities must have clear characteristics that define and position each institution within the landscape.

Having a common model of basic characteristics to identify institutions would be a logical step to facilitate their recognition and verification. This would also help classify and group institutions by their traits. It makes it easier to place them in areas like research, technology resources, or academic offerings that match their vision. This, in turn, could ease their entry into certain alliances or promote interoperability among institutions with common interests, leading to the formation of new alliances. A suggested institutional identity standard is described in chapter 9.5 Institutional identity standard.

For more information on the interoperability capabilities of this use case, please refer to the comprehensive final mapping report.

For more information on the interoperability capabilities of this use case, please refer to the comprehensive final mapping report.

8.6 Recommendations – use case 8

Use established European standard for HEI identification: To ensure seamless interoperability and data exchange across the European Higher Education Area, a unified standard for institutional identification is necessary. The widely used SCHAC schema, as seen in projects like EMREX, Erasmus Without Paper, MyAcademicID and others, provides a solid foundation for systems that support many of the use cases. For instance, ETER IDs are used in the European Higher Education Sector Observatory. Higher Education Institutions should contribute to developing a robust and universally adopted European standard for HEI identification.

Monitor and manage institutional identity in European registries: Most European higher education institutions appear in key Europe-wide databases or registries. These are used for different purposes. Some of these registries directly link to the institution's trusted identity for specific use cases. An example is shown in use case 6 with the DEQAR's integration into European Digital Credentials. Therefore, it is crucial for institutions to monitor their identity and attributes in these registries. They should also take steps to keep their information current. For example, if accreditation data is inaccurate, they should contact their QA bodies.

Provide transparent information on APIs implemented: Institutions provide interoperable functions through well-documented Application Programming Interfaces (APIs). These APIs follow widely accepted standards like Erasmus Without Paper (EWP). Clear and accessible information about an institution's APIs can boost interoperability. It helps partner institutions connect easily.

Share key information openly: Current standards like EWP APIs, OOAPI, and OCCAPI let institutions share important data, such as details on organisational units and courses, in an interoperable manner. To maximise the use of this data, it can be helpful to provide it openly and through a public API, as long as no sensitive or personal data is concerned.

PART 9

Key data standards

9 Key data standards

Data standards play a crucial role in achieving semantic interoperability. The following sections propose a set of essential data standards necessary for achieving interoperability in one or multiple use cases. Within a single European University alliance, the data standard to be used for interoperability can be agreed upon at the alliance level. For interoperability between and beyond EU alliances, standards agreed at a higher level may be required.

9.1 Learning data standard

The chosen data standard should meet a set of metadata and attribute requirements that facilitate the discovery of learning opportunities. Each data object contains a minimum set of relevant data identified as key values that the selected standard should include.

Learning Specification

- **Identifier:** A unique identifier is needed to identify the learning specification clearly. This identifier must be unique at the alliance or institution level. It is better for it to be unique at the alliance level to prevent future overlaps between identifiers from different institutions.
- **Title:** The title of the learning unit is required.
- **Description:** A description of the learning specification is also necessary to make it readable, clearly explaining and including all its aspects.
- **Mode:** The mode of the learning specification, which identifies the supported modalities (e.g., online, live, or hybrid), is important as it could be a barrier for some learners.
- **Activities:** The learning specification includes related activities, like problem solving and report writing. These activities should be clear and easy to identify.
- **Prerequisites:** Each learning specification must show the required knowledge or skills. This may relate to other specifications. Learners begin their discovery by looking for learning opportunities that fit their path.
- **Assessments:** The learning specification includes related assessments that demonstrate the learner's acquisition of a particular knowledge or skill.
- **Outcome:** The outcome presents to learners the specific knowledge or skills they will acquire through the learning specification.
- **Credits:** The number of ECTS credits awarded for successful completion of the learning unit is required.

- **Entitlement:** A specification of an entitlement that this learning specification may give access to another learning opportunity is included.
- **Usage Rights:** Information about the usage rights and license of the course content is provided.
- **Intellectual Property:** Information about the intellectual property of the content is included.

As a more specific object instance than a learning specification, a learning offering should also have at least the following fields:

Learning Offering

- **Mode:** The learning specification may include this information. In some cases, it can also offer access to learning options with different modalities.
- **Schedule:** This shows the timetable for the learning opportunity. It helps learners create their own learning path and avoid conflicts between opportunities.
- **Duration:** The total course duration, for example, in weeks or months.
- **Cost:** The course cost for learners.
- **Accessibility Options:** Information on the available accessibility options for learners with disabilities

In use case 2 (apply and get recognition), learning application standards are discussed so institutions can agree on enrolling learners in joint programs. To achieve interoperability, these learning applications should have the following standard base fields.

Learning application

- **Personal Identification:** The learner's name, date of birth, and national identification number.
- **Contact Information:** The learner's email and telephone number.
- **Academic History:** Information about previous institutions, degrees obtained, and their corresponding dates.
- **Learning Offering Information:** The name of the learning offering the learner wants to enrol in, along with its identifier.
- **Destination Institution:** The institution where the learner wants to take the learning offering.
- **Privacy Policy:** Acceptance of the privacy policy, including the processing of personal data.
- **Truthfulness Statement:** A declaration that the provided information is truthful and accurate.
- **Interoperability:** Learning data standards should be compatible with existing standards in this area, such as ELM.

9.2 Agreements standards

To achieve interoperability, it is often necessary to establish a series of agreements between institutions. These agreements help exchange information and give learners from different institutions access to resources. They can even create joint programmes. Standardising these agreements can boost collaboration between institutions. This promotes mobility programmes and improves interoperability.

These agreements include a mutual understanding between institutions. They set requirements to recognise each other's learning offerings. This ensures that learners' achievements are acknowledged by their home institution and all participating institutions once they finish the programme. A standard for this type of agreement should cover at least the following fields.

General learning agreement standard

- **Basic information of the learning offering:** Identifier of the learning offering, course name, course description.
- **Details of the destination institution:** Name of the institution, identifier of the institution, contact.
- **Educational level:** Information on the educational level of the learning offering (e.g., bachelor's degree, master's degree).
- **Modality:** Definition of the modality of the course delivery: face-to-face, online or hybrid.
- **Credits:** Number of ECTS credits.
- **Duration:** Duration of the course.
- **Outputs:** Assessments, outcomes, entitlements.
- **Evaluation:** Evaluation methods used in the learning offering and criteria for evaluating the learner's performance.
- **Admission requirements:** Previous requirements necessary to enrol.
- **Credit recognition:** Definition of course equivalences and credit transfers.
- **Usage rights:** Information on usage rights and licenses of the course content.

The previous agreement focused on the recognition of learning offerings between institutions. If we expand the framework to facilitate higher-level collaboration between institutions, the agreements need to be similarly broader. A standard that covers the basic concepts of these agreements would help and encourage collaboration between institutions. A standard agreement between multiple institutions for a common mobility plan, such as use case 2 (apply and get recognition), should include at least this information:

Joint education provision agreement standard (e.g., joint programme)

- **Programme Name:** The defined name for the inter-institutional collaboration programme.
- **Participating institutions:** The names and details of the institutions that will be part of the collaboration agreement.
- **Objectives:** The objectives and goals of the collaboration programme.
- **Curriculum:** A clear overview of the curriculum for the collaboration programme, highlighting its learning offerings.
- **Credits:** The distribution of ECTS credits.
- **Distribution:** The distribution of teaching among the different participating institutions.
- **Admission criteria:** The prerequisites that learners must meet to be able to apply to the programme.
- **Application process:** The procedures and deadlines for the application and admission of learners to the programme.
- **Credit recognition:** The measures of credit recognition and their transfer between participating institutions.
- **Evaluation process:** The methods and scales for evaluating the performance of learners with respect to the programme.
- **Roles and responsibilities:** The definition of roles and responsibilities of each institution in the management of the programme in which they collaborate.
- **Intellectual property:** The agreements on intellectual property for the materials used in the offerings that make up the programme.
- **Jurisdiction:** The determination of legal jurisdiction in case of disputes for conflict resolution.
- **Agreement terms:** The validity period, termination, and review procedure.
- **Agreement signature:** The signatures of the authorized representatives of the interested parties
- **Interoperability:** Agreement standards should be compatible with existing standards for learning agreements and inter-institutional agreements, such as those developed by EWP.

However, the Erasmus+ project has created templates[14] for these agreements. They help institutions set up new partnerships.

[14] https://erasmus-plus.ec.europa.eu/resources-and-tools/mobility-and-learning-agreements/learning-agreements

9.3 Tools and assets data standard

To facilitate the search for resources like tools, this document has discussed controlled vocabularies. These controlled vocabularies are a set of terms with their definitions and translations, representing basic concepts. Using these words consistently helps group different information into similar groups. This facilitates their interoperability, making them easier to use and share.

The use of controlled vocabularies can be complemented by standardising tool definitions. Below are the minimum fields a standard representation of a tool should have. Please add any additional fields you think necessary for this standard representation.

Tool/asset data standard

- **Identifier:** A unique identifier for the resource, allowing each one to be uniquely identified.
- **Name:** The name of the resource.
- **Description:** A summary of the resource's functionality and purpose.
- **Resource type:** The category of the resource, such as software or laboratory.
- **Provider institution:** The name and identifier of the institution providing the resource.
- **Access details:** The requirements for accessing the resource, including the application procedure and any limitations on its use.
- **Cost:** Information about the cost of the resource.
- **License and terms of use:** The terms and conditions of use associated with the resource.
- **Format:** The data format and protocols supported by the resource. This will facilitate interoperability and integration of data across multiple institutions.
- **Tags:** Keywords that enable grouping and facilitate searching between resources.
- **Usage indicator:** Data on the resource's usage, which is important for obtaining usage statistics and planning its scaling if necessary.

The use of tools, whether integrated within institutions' LMSs or as external tools, generates a multitude of data that can be difficult to organise. These data - learning records - must be standardised to organise and consult them effectively. Moreover, considering interoperability, standardization is especially necessary to share learning records generated by learners with tools that other institutions, different from their original one, may share.

For standardising learning records, several models currently exist, some of which have already been mentioned in this document as they are used by some alliances. Therefore, this section focuses on the minimum capabilities that must be met to be considered on the path to interoperability.

- **Interoperability:** The standard must be compatible with a wide range of systems and learning platforms (LMS), as well as other educational standards like xAPI, SCORM, and cmi5.
- **Flexibility:** The standard needs to accommodate the diverse results from activities using various tools.
- **Scalability:** With the large amount of data that can be generated, the standard should be lightweight to avoid negatively impacting processing and storage performance.
- **Detail:** The standard must capture data accurately and in detail to provide a comprehensive picture of learning records.
- **Metadata:** It should support descriptive metadata that adds context to learning record.

In summary, the selected standard must be strong and adaptable. It should manage different data and learning scenarios while ensuring interoperability, security, and usability. By combining advanced analytics, descriptive metadata, and privacy measures, we can make learning data valuable for both learners and students.

A standard model for learning records could have the following scheme:

Actor

- Name: Name of the actor involved in the creation of the learning record.
- Contact: Actor contact information.

Verb

- Action: Information about the action that has been carried out through the use of the tool.
- Status: State of the activity after the action.

Object

- Object type: Type of the object (e.g., Activity).
- Identifier: Unique object identifier.
- Name: Name of the object (e.g., Lesson 1).
- Description: Description of the object (e.g., First lesson of physics course).

Result

- Score: Score related to the learning record.

Context

- Platform: Name of the platform that leads to the created learning record (e.g., Moodle).
- Additional information: All other valuable related information such as timestamp or language.

This model has many similarities with, for example, xAPI, as it follows the standard actor-verb-object-result format.

9.4 Educational resources standard

Educational resources come in a variety of formats, making it difficult to find a shared model to describe them. To successfully share resources between institutions, agreeing on a common standard is essential. This section analyses the interoperability requirements of the different systems and services outlined in the reference architecture.

To make educational resources discoverable, a metadata standard is required that provides:

- **Identifier:** A unique identifier for the educational resource.
- **Name:** The name of the resource.
- **Description:** A summary of the resource's functionality and purpose.
- **Author:** Information about the resource's creator.
- **Owner:** Information about the owner of the resource's rights.
- **Learning objectives:** A description of the resource's objectives and competencies.
- **Format:** A description of the resource's format, such as video or text.
- **Access point:** The location from which the exposed resource can be accessed.
- **Terms of use:** The licences and conditions under which the resource can be used.
- **Access requirements:** Information about the internal processes that need to be followed to gain access to the resource.
- **Date:** The date of publication of the resource.
- **Version:** The current version of the exposed resource.
- **Technical requirements:** The software or hardware necessary to use the resource.
- **Compatibilities:** Information about the resource's compatibility with educational standards.
- **Tags:** Keywords that facilitate its search and categorization.

When using an existing educational resource, you need tool metadata. This includes details about the tools that can open the content, like the tool identifier. You can search for this identifier in the tool catalogue. This will provide all the detailed standard information about it, as described in chapter 9.3 (tools and assets data standard).

Furthermore, a controlled vocabulary is necessary to standardise descriptive terms. This ensures a better understanding of the content by all parties.

Additionally, it is necessary to have a controlled vocabulary to standardize descriptive terms, ensuring better understanding of the content by all parties.

9.5 User identity standard

In student mobility scenarios, such as those described in use case 7 (user identity), the exchange of student data becomes necessary. To facilitate the integration of this user data into central systems, standards should be adhered to. A standard defining a user identity must contain the necessary information to identify the user uniquely and unequivocally.

The minimum fields required for a user identity standard would be:

- **User ID:** A unique and persistent identifier for the user.
- **Full Name:** The user's first and last name.
- **Contact**: The user's contact information.
- **Role**: The user's role within the institution.
- **Department**: The department or faculty to which the user belongs.
- **Authentication** Methods: Information about the supported authentication methods (e.g., MFA).
- **Digital Certificates**: Certificates used for authentication, if applicable.
- **Permissions**: A list of specific permissions assigned to the user.
- **Last Update**: The date of the last update to the user's data.
- **Change History**: A record of changes to the user's information.
- **Privacy Preferences**: Settings on the visibility and sharing of their data
- **API Tokens**: Tokens used for API access.
- **Notification Settings**: Preferences on how the user receives notifications.

When expanding this standard or using a proprietary user identity model, it is essential to differentiate between the identity provider system and student information system. This model refers to user data stored in the identity provider, so data related to academic aspects should not be included, as this would be stored in the student information system.

9.6 Institutional identity standard

To promote interoperability between institutions, it is essential to create a clear and recognizable identity, as described in chapter 8.3 (interoperability and required capabilities – institutional identity). The main characteristics that should define an institution are:

- **Name:** The official name of the Higher Education Institution (HEI).
- **Address:** The complete physical address of the HEI, including street name, number, city, postal code, and country.
- **Erasmus/Organisation Identity:** The unique identifier assigned to the institution within the Erasmus+ programme or other organisational identity systems. It may include the Erasmus code, facilitating the recognition and exchange of information between institutions.
- **Organisational units:** A list of the main subdivisions within the institution, such as faculties, schools, departments, or colleges.
- **Contact:** The primary contact details for the institution. This includes phone number, email address, and any other relevant communication channels.
- **Institutional accreditation:** Details of the formal recognitions and accreditations that the institution has received. It certifies its educational quality and standards.
- **Optional:**
    - **Indicators/metrics:** Quantitative data providing insight into various aspects of the institution's performance. This includes student-to-faculty ratio or graduation rates.
    - **Ranking:** The position or score of the institution in! various national and international rankings.
    - **Link to source with standardised data/indicators:** A URL linking to an external source providing standardised data or indicators about the institution.

This could serve as a foundation standard for building a comprehensive profile that defines institutions as such. Another factor to consider is the use of controlled vocabularies in these definitions to facilitate later groupings, allowing for various ways to exploit this data.

Interoperability: The institutional identity data standards should be compatible with existing standards, such as those used in DEQAR, EWP, and ETER.

9.7 Mapping services

Mapping services act like interpreters. They translate local terms into a common vocabulary and also reshape local data fields to fit the shared standard.

Central catalogue approach: The mapping only translates metadata. The sharing service takes a reactive role, receiving a request from the central catalogue to send data and responding with the list of updated learning opportunities. If the local catalogue is proactive, sending updates to the central catalogue, it does not need to expose a query interface.

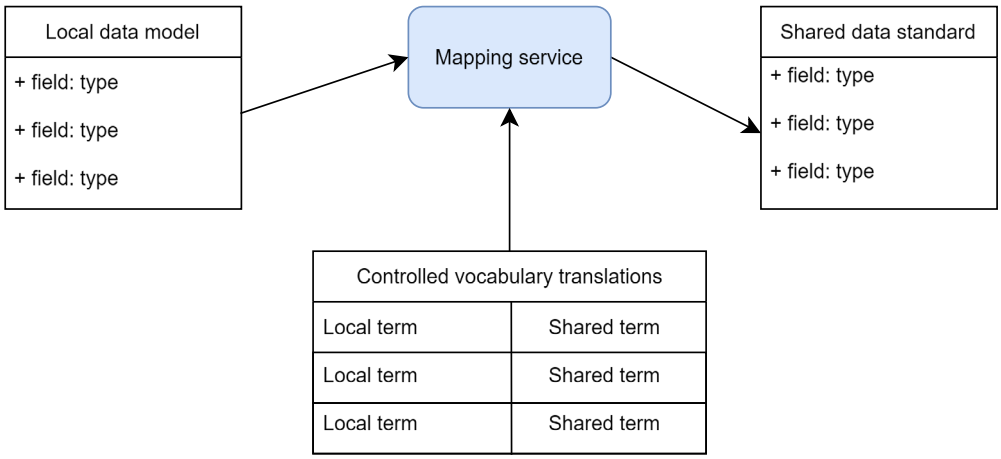


Figure 80 - Mapping service data conversion process schema.
© 2025 European Union

Contact us

For more information please consult our website where you will find details on upcoming events and publications on how to apply for funding.

eacea.ec.europa.eu/
eacea-info@ec.europa.eu

For more information about EDEH please consult the European Education Area Portal page:
European Digital Education Hub | European Education Area (europa.eu)

Publications Office
of the European Union