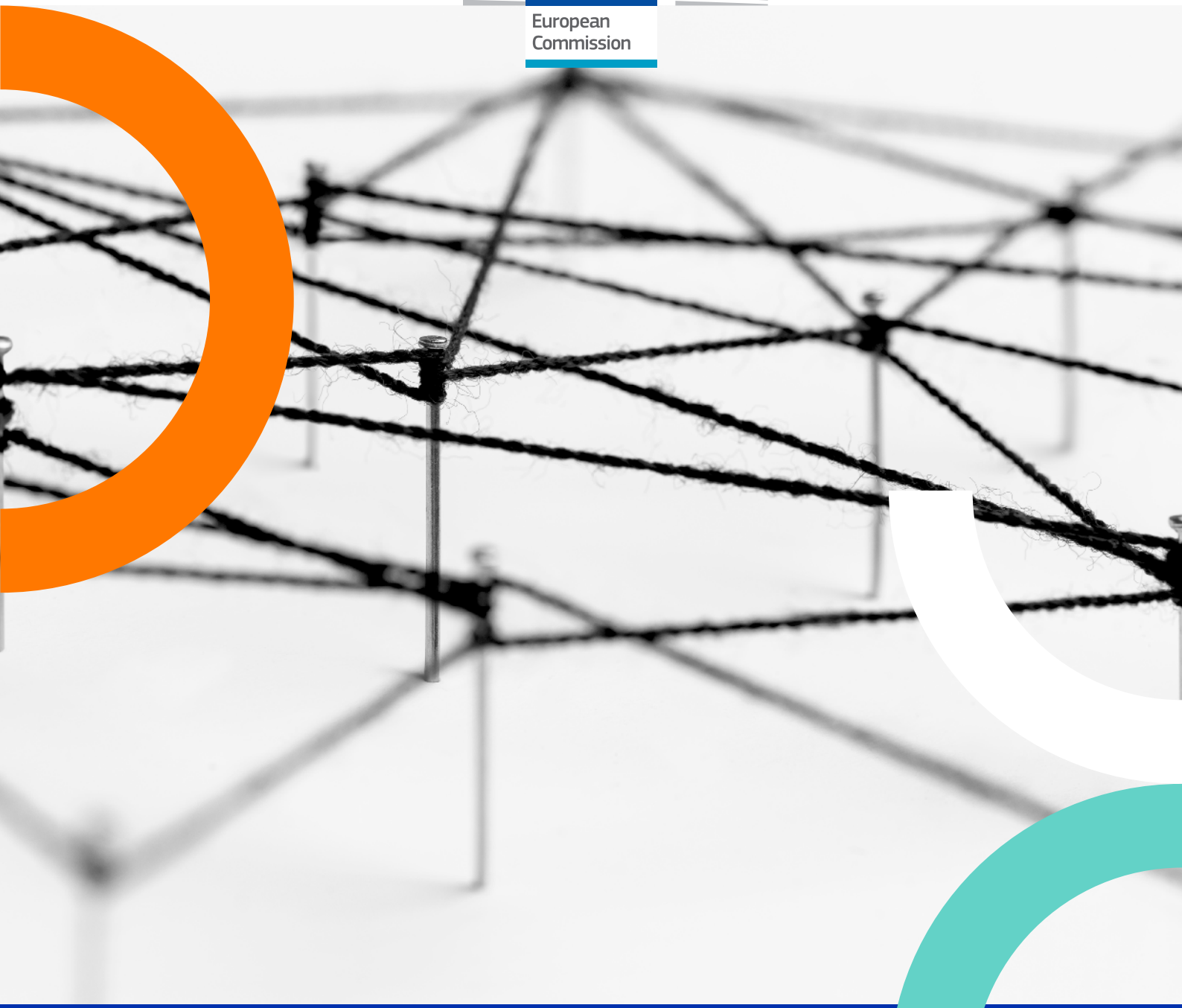
European Commission



An inventory of standards, processes, and ICT systems across Higher Education (Mapping report)

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).

This document has been prepared for the European Commission and for the European Education and Culture Executive Agency (EACEA), however it reflects the views only of the authors, and the European Commission and EACEA are not liable for any consequence stemming from the reuse of this publication.

More information on the European Union is available on the internet (http://europa.eu).

Luxembourg: Publications Office of the European Union, 2025

Print ISBN 978-92-68-18735-7 doi:10.2766/823776 NC-02-24-714-EN-C
PDF ISBN 978-92-68-18734-0 doi:10.2766/058737 NC-02-24-714-EN-N

© European Union, 2025

Except otherwise noted, the reuse of this document is authorised under a Creative Commons Attribution 4.0 International (CC-BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

The reuse policy of European Commission documents (applicable also to documents of the European Education and Culture Executive Agency) is implemented based on Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39).

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders. The EU does not own the copyright in relation to the following elements, which are used under their respective licences:

- *Cover page image - © 2024 Freepik I rawpixel.com*
- *Figures on page 14 - © 2024 Freepik I Freepik*
- *Figures on page 15 - © 2024 Freepik I Freepik*
- *Figure on page 22 - © 2024 Freepik I Freepik*
- *Figure on page 37 - © 2024 Freepik I Freepik*
- *Figure on page 50 - © 2024 Freepik I Freepik*
- *Figure on page 61 - © 2024 Freepik I Freepik*
- *Figure on page 74 - © 2024 Freepik I Freepik*
- *Figure on page 87 - © 2024 Freepik I Freepik*
- *Figure on page 99 - © 2024 Freepik I Freepik*
- *Figure on page 116 - © 2024 Freepik I Freepik*

Executive Summary

This mapping report presents an inventory of standards and solutions currently in use at European University alliances (EU-As) to enable interoperable virtual (inter-institutional) European campuses to become reality. As such, the report provides insights into certain aspects of the technical landscape at EU-As and is aimed at technical experts at Higher Education Institutions (HEIs). The document breaks down standards and tools applied per use case and specifies the capability requirements of solutions implemented.

This mapping report is complemented by the synthesis report which takes a broader perspective, presents the cross-cutting analysis of the data collected in this mapping report, and offers valuable insights for a less technically oriented audience.

This mapping report delves into the technical landscape at higher education (HE) teaching and learning systems. For instance, significant issues such as data portability and the standardisation of course catalogues are highlighted, particularly the challenge of establishing centralised or global catalogues—essential for seamless course information exchange and foundational for other use cases, such as application and enrolment. Alliances have resorted to basic scraping techniques and manual or only semi-automatic data provision to fill these catalogues. While cost-effective as a short-term solution that delivers results quickly, this approach is often not scalable, does not ensure regular updates without manual intervention, and sometimes bypasses validation inherent in more structured data exchanges, thereby compromising data quality and comparability.

Furthermore, building on these catalogues with application and recognition systems – the logical next step – presents another set of challenges, ranging from simple application processes to more sophisticated, fully digital integrations. These efforts are hampered by the lack of widely used standards for data exchange and validation. As a result, manual compliance checks and handling of student data remain common. With manual processes performed by HEIs within an alliance simultaneously, the lack of automation creates significant inefficiencies.

Input from 41 EU-As and experts from the European Digital Education Hub (EDEH) has informed key revisions in high-level workflows and architectural diagrams, alongside a gap analysis, all detailed in this report. These efforts identify crucial deficiencies and call for strategic responses to enhance system compatibility and operational efficiency.

The report is structured to guide stakeholders through the various aspects of HE interoperability, from introducing the use cases addressed by the EDEH interoperability initiative to exploring detailed gap analyses, focusing on essential components and services required for interoperability.

By addressing these critical gaps in detail, this report not only captures the current state but also lays the groundwork for future developments in standards and services. It aims to encourage collaboration of EU-As, European organisations, stakeholders, and EdTech vendors to bridge these gaps. This iterative, workflow-driven approach seeks to progressively refine our collective understanding and operational capabilities across the European HE sectors, supporting the development of a robust, interconnected educational framework.

Table of Content

0 Introduction **10**

0.1 How to read this document 10

0.2 Methodology 11

0.3 Overview of use cases and scenarios 14

0.4 Terminology and diagrams notation 16

0.5 Implementation approaches identified 16

1 Use case 1 – Discovery **22**

1.1 Use case definition 22

1.2 High-level flow 23

1.3 Draft architecture 25

1.4 Interoperability required capabilities 28

1.5 Overview of resources in use 32

1.6 Analysis 35

2 Use case 2 - Apply and get recognition **37**

2.1 Use case definition 37

2.2 High-level flow 37

2.3 Draft architecture 39

2.4 Interoperability required capabilities 42

2.5 Overview of resources in use 46

2.6 Analysis 48

3 Use case 3 – Access tools **50**

3.1 Use case definition 50

3.2 High-level flow 50

3.3 Draft architecture 53

3.4 Interoperability required capabilities 55

3.5 Overview of resources in use 57

3.6 Analysis 59

4 Use case 4 - Manage educational resources **61**

4.1 Use case definition 61

4.2 High-level flow 61

4.3 Draft architecture 64

4.4 Interoperability required capabilities 68

4.5 Overview of resources in use 70

5 Use case 5 - Generate data **74**

5.1 Use case definition 74

5.2 High-level flow 74

5.3 Draft architecture 79

5.4 Interoperability required capabilities 80

5.5 Overview of resources in use 83

6 Use case 6 - Earn a credential **87**

6.1 Use case definition 87

6.2 High-level flow 87

6.3 Draft architecture 89

6.4 Interoperability required capabilities 93

6.5 Overview of resources in use 94

6.6 Analysis 97

7 Use case 7 - User identity **99**

7.1 Use case definition 99

7.2 High-level flow 100

7.3 Draft architecture 102

7.4 Interoperability required capabilities 105

7.5 Overview of resources in use 110

7.6 Analysis 113

8 Use case 8 - Institutional identity **116**

8.1 Use case definition 116

8.2 High-level flow 117

8.3 Draft architecture 120

8.4 Interoperability and required capabilities 121

8.5 Overview of resources in use 123

8.6 Analysis 124

9 Key data standards **126**

9.1 Learning data standard 126

9.2 Agreements standards 128

9.3 Tools and assets data standard 130

9.4 Educational resources standard 132

9.5 User identity standard 133

9.6 Institutional identity standard 134

9.7 Mapping services 135

10 Annex I – Inventory of tools and services **137**

11 Annex II – Inventory of standards and protocols **151**

0 Introduction

This document outlines the current technical landscape within European University alliances (EU-As) and the Higher Education Institutions (HEIs) that constitute them. The purpose of this report is to provide an insight into the tools used by the different alliances to create their virtual campuses, identify gaps left unaddressed by existing tools, and the alliances' most relevant interoperability challenges.

Below image illustrates the components of the HE Interoperability Framework. This mapping report is a technical document that supports the reference architecture defined in the blueprint. It is an inventory of the existing solutions and standards in place in alliances that have been identified throughout the project.

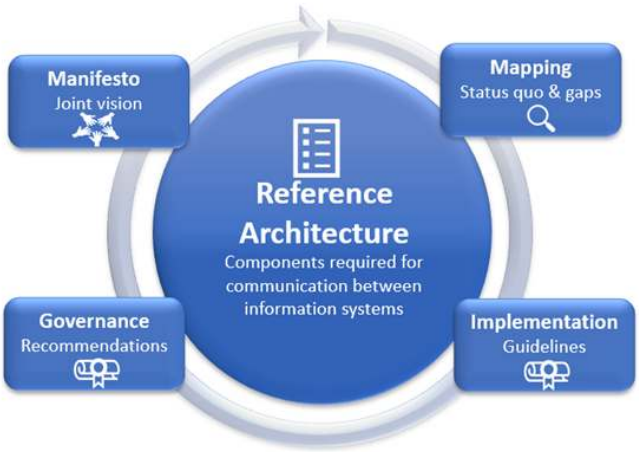


Figure 1 - Overview of the interoperability framework.
© 2025 European Union

0.1 How to read this document

Each use case is described in a dedicated section. In every section, the use case's objective and scope set the scene for the challenges faced. Each use case is further refined through the high-level process flows, which provide an overview of the steps and actors involved in the process. High-level diagrams facilitate the reading of the draft architecture diagrams. For this report's scope, simplified versions of the draft architecture diagrams were included, focused on the main components and services required to send and receive information between different systems. Each diagram component is described, and the required capabilities are listed and detailed prior to moving to the gap analysis.

The required capabilities are key to performing the gap analysis. To this end, a matrix containing the set of systems and services outlined in the reference architecture and the subset of available tools collected during the sessions with the alliances has been set up. Most prominent tools were analysed considering the required capabilities. The gap analysis concludes each use case with a summary of technology gaps, an overview of the solutions proposed by the alliances and the challenges faced or forecasted.

Key terminology used in the context of this project and in this report is elaborated on in the report to ensure common understanding. A comprehensive glossary of terms can be consulted here.

0.2 Methodology

Data included in this report has been collected during fourteen sessions conducted from February to June 2024. This inventory presents insights gathered from 41 alliances[1] that took part in at least one session or provided internal documentation relevant for the mapping session.

All the information collected has been thoroughly reviewed and standardised in a unique table incorporated as an annex to this report. Sessions with the alliances have also served to identify challenges faced by different alliances during their interoperability journey. The findings were analysed in more detail in the synthesis report.

The use cases in focus were refined during the first months of this higher education interoperability assignment and challenged during the first design thinking workshop (January 2024, Potsdam, Germany). Outcomes include the high-level data flows included in this report.

Additionally, at the beginning of February 2024, eight squads were established to work on each use-case until the end of October 2024. Squads were led by an expert from the consortium and supported by a squad co-lead selected from the core group of experts. Members of the wider group were invited to join as many squads as they wish to test, validate, and propose changes to high-level flows and architecture diagrams in a series of working sessions held online. Most squads had a similar number of experts signed up, ranging from 20 to 30 members, while actual attendance at squad meetings was slightly lower. The use case 7 (user identity) squad needs to be highlighted as the one with the highest level of participation, with 32 different people participating between the two sessions. This possibly reflects the foundational nature of this use case, underpinning most of the use cases 1 – 6 in one way or another.

[1] Arqus, CHARM-EU, CIVICA, CIVIS, E3UDRES2, EC2U, EDUC, ERUA, EPICUR, EU-CONEXUS, EU GREEN, EUGLOH, EUniWell, EUPeace, EuroTeQ, INVEST, NeurotechEU, T4EU, UNIC, UNITA, Unite! and other alliances that have preferred not to be named or are in the process of giving permission to be mentioned.

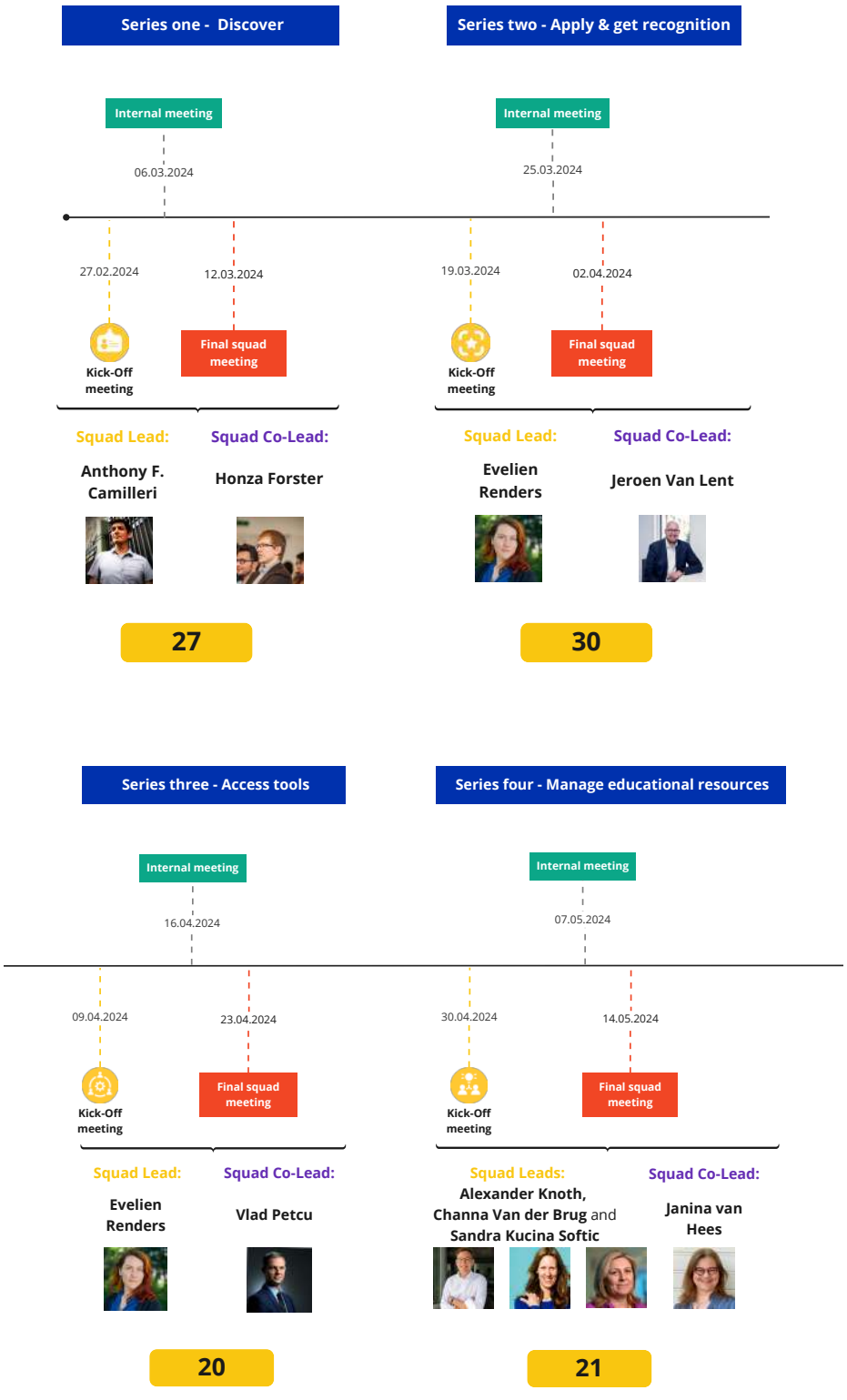


Figure 2 - Timeline of squad series.

© 2025 European Union

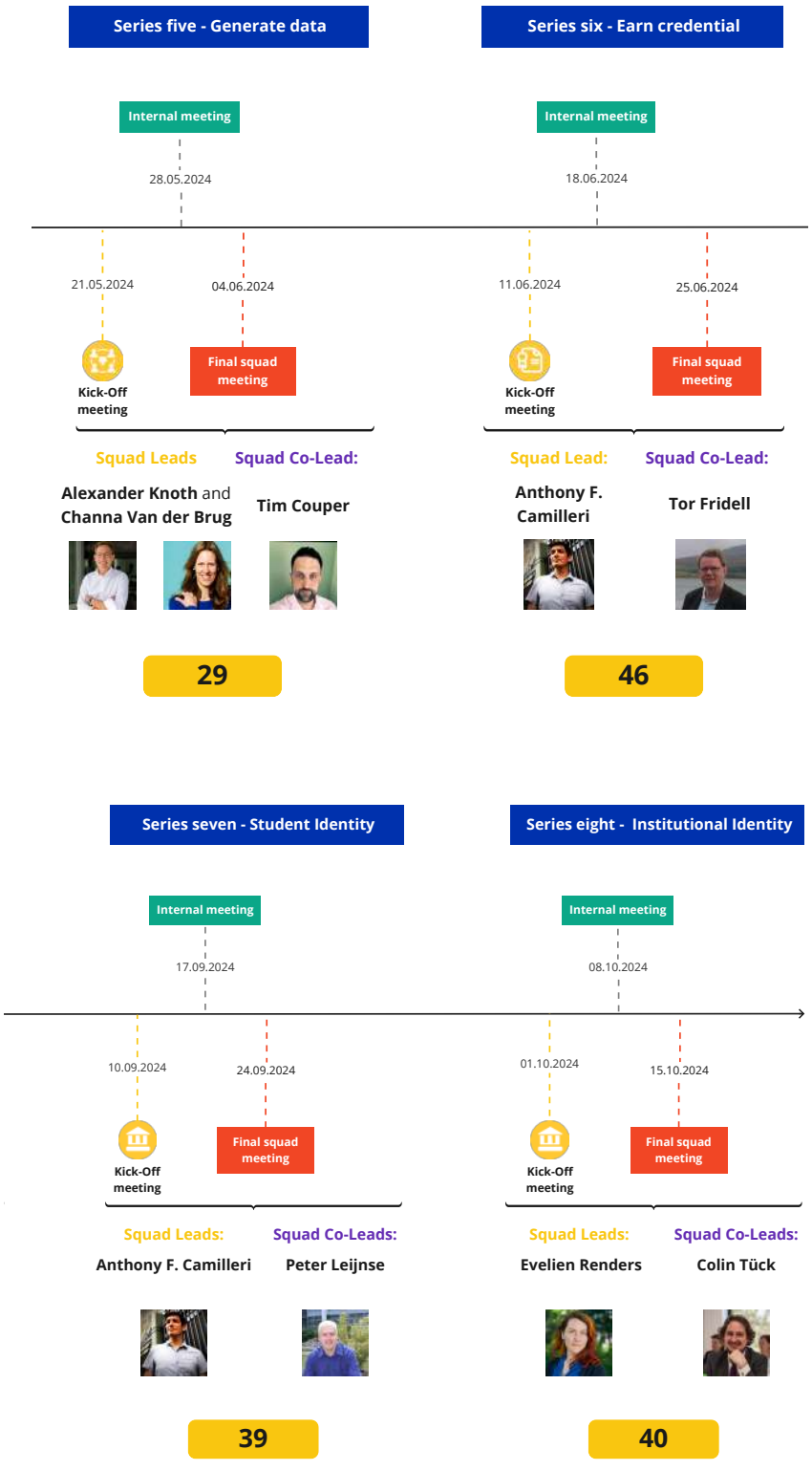


Figure 3 - Timeline of squad sessions II.

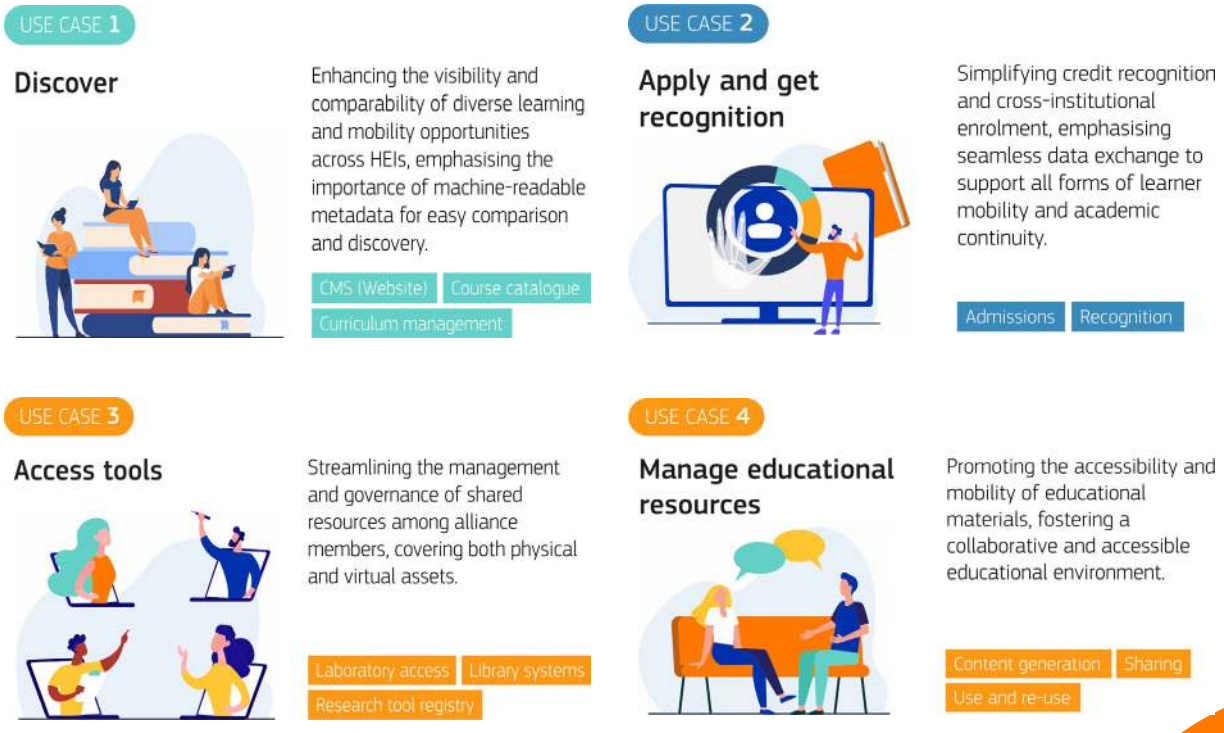
© 2025 European Union

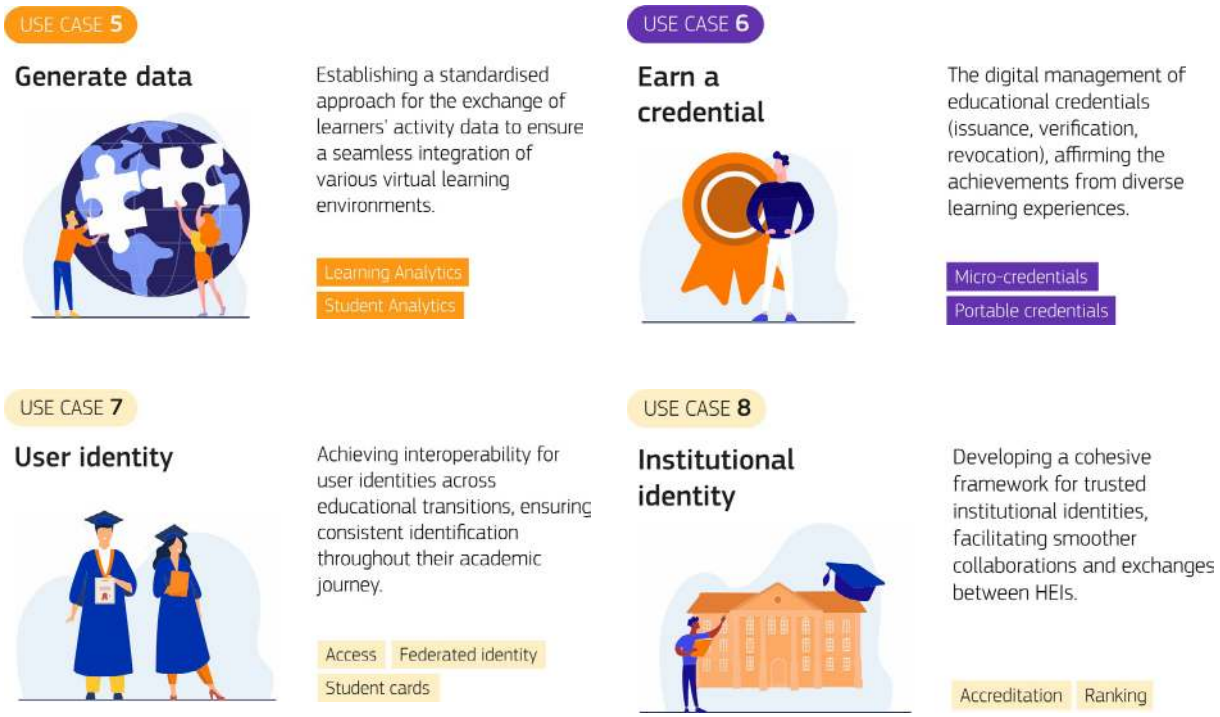
Squads worked on sprints of three weeks duration. Each squad kicked off with an introductory session in which the squad lead and squad co-lead presented the scope of the use case through a series of user stories. Once the workgroup had a clear view of the boundaries, the high-level flow and draft architecture diagrams were reviewed, and feedback was collected for further refinement. Further, the diagrams were revised in an internal meeting with members of the consortium and the squad co-lead. In a third and final session with the squad participants, the changes made were presented and final thoughts and key considerations were gathered.

0.3 Overview of use cases and scenarios

The Design Thinking workshop (January 2024) led to the categorisation of the use cases into two main types: Core processes and supporting processes. In addition, for some use cases, different scenarios are accounted for.

The first six use cases, as displayed below, define core processes in the learner journey. These use cases cover the essential steps in that learner journey through the virtual campus of an EU-A: it begins with the learner discovering available learning opportunities (UC 1), enrolling into those (UC 2), using various tools and resources during their studies (UC 3 & 4), tracking their progress (UC 5) and receiving a credential upon completion (UC 6). The remaining two use cases (use cases 7- User identity and 8 - Institutional identity) support the previous ones.





© *2024 Freepik*

Three scenarios account for different interoperability challenges encountered by alliances:

- **Joint programme:** full degree/programme across different institutions. Also including double degree.
- **Credit mobility/programme:** short module/courses across different institutions. Includes, but not restricted to, Erasmus mobilities.
- **Open programme**: full degree or module or course mobility at one institution different from the learner's home institution.

Such interoperability challenges were exposed by the Erasmus+ programme and are addressed by projects, such as Erasmus Without Papers (EWP)[2] or the European Student Card (ESC)[3]. In addition, alliances have expressed during the squad sessions and the inventory sessions that joint programmes and other collaboration scenarios have brought further interoperability challenges to light that impact on certain use cases.

[2] Erasmus Without Paper | Erasmus+ (europa.eu)
[3] European Student Card Initiative | Erasmus+ (europa.eu)

0.4 Terminology and diagrams notation

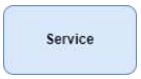
Diagrams included in this report use the following notation:



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[4].



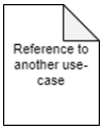
Service: Defines systems required capabilities. Services share or expose data and must be interoperable.



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.

0.5 Implementation approaches identified

In this section the different general implementation approaches that can be applied to the different use cases are outlined. The proposed architecture is designed with the necessary flexibility to accommodate ideal implementations that lead to interoperability while also supporting the creation of a system of systems that considers existing solutions already implemented by HEIs. This approach facilitates both the modernisation of systems and the adoption of solutions that complement current infrastructures. This section provides an overview of the identified approaches without recommending one over another but highlighting potential pros and cons. There is no single solution, the most prominent ones have been identified and are presented as tools available for alliances to adopt or create hybrid versions adapted to their specific needs in each use case. It is possible to adopt more than one approach in parallel or use hybrid models of these within the complex systems found across EU-As. The selected approach should be agreed in an interoperability agreement signed by the institutions forming an EU-A.

[4] https://pubs.opengroup.org/architecture/archimate31-doc/chap08.html#_Ref412713032

0.5.1 Data sharing implementation

As a result of the inventory process, various strategies have been identified for implementing interoperability between different systems. Each strategy has some implications for the scalability of the system, for data privacy and for consistency. These strategies serve as a foundation or tool for building an interoperable solution. They are versatile enough to be applied in different uses cases and, as a basis, can be adapted or even combined to meet the specific needs of a given use case or institution. In the chapters corresponding to each use case, information is provided on the most prominent strategy. The strategies are as follows:

- Collect data in a **central system**. This strategy implies designating a central system that will store a copy of the data. The master record is kept in the local system that created it. TThere may be consistency issues depending on the time needed to propagate changes from the local systems to the central one. Storing a copy of the data in another system can be challenging when doing so does not comply with the privacy standards of institutions or alliances.
- Offer central services that **collect information on demand**. This strategy offers a central interface querying all the local systems to present the information to the end user. This strategy allows collecting/accessing data on demand without storing it and is the most privacy friendly, while also avoiding data duplication. At the same time, it depends on the stability of all local systems.
- **Broadcast** changes and store a copy of every record in every local system, i.e., a form of peer-to-peer synchronisation. This strategy allows users to use their local systems to query data stored in any other system. While reliability is high, the, the consistency risk increases due to the large number of copies.

Synchronisation of data plays a key role to avoid or, at least minimise, data inconsistency. On the other hand, it may expose a scalability issue. This problem only applies to central system and broadcast strategies.

Given that EU-As have less than 10 members, all approaches are feasible in this setting. It should be noted that some approaches would, however, not be scalable to larger groups of institutions.

For the central system approach, there are also two distinct approaches within regarding the actor that triggers the data transfer between systems. These are detailed below, outlining the interactions between systems.

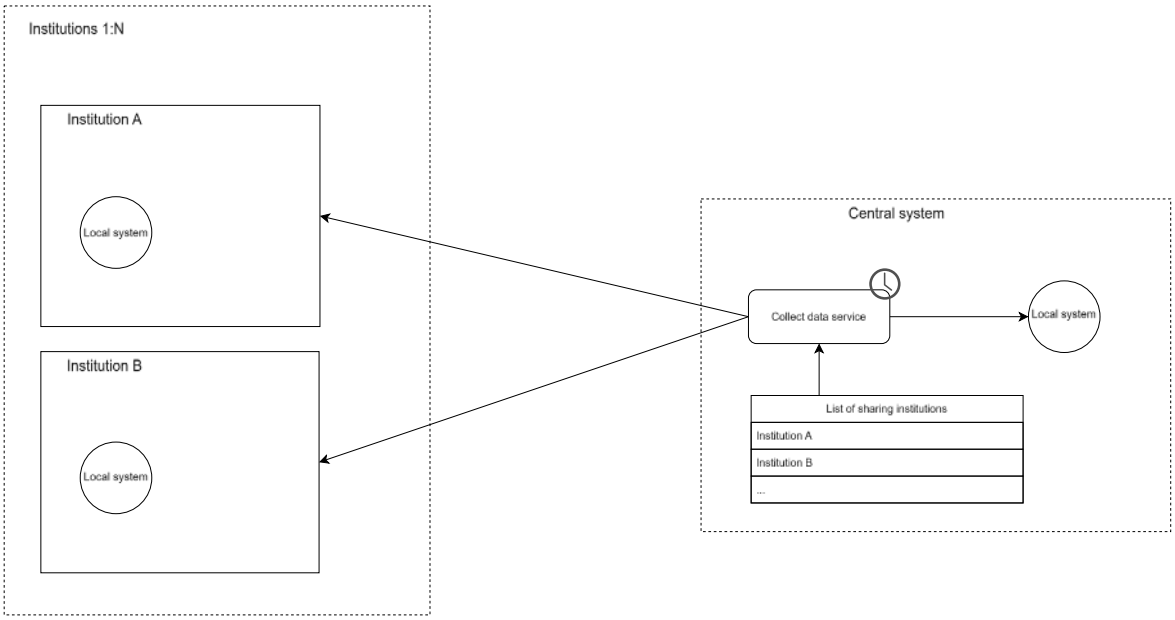


Figure 4 - Receiving system synchronisation approach.

© 2025 European Union

Receiving system ("pull"): Requires that local systems implement a publishing service that can be called on demand. Since the central system is calling all connected systems, it is easier to schedule updating tasks to accommodate available resources needed to process the data. On the other hand, updating tasks might be called even if there are no updates and depending on the updating frequency, data may remain outdated longer than desired. This may lead to either wasting resources or data consistency problems.

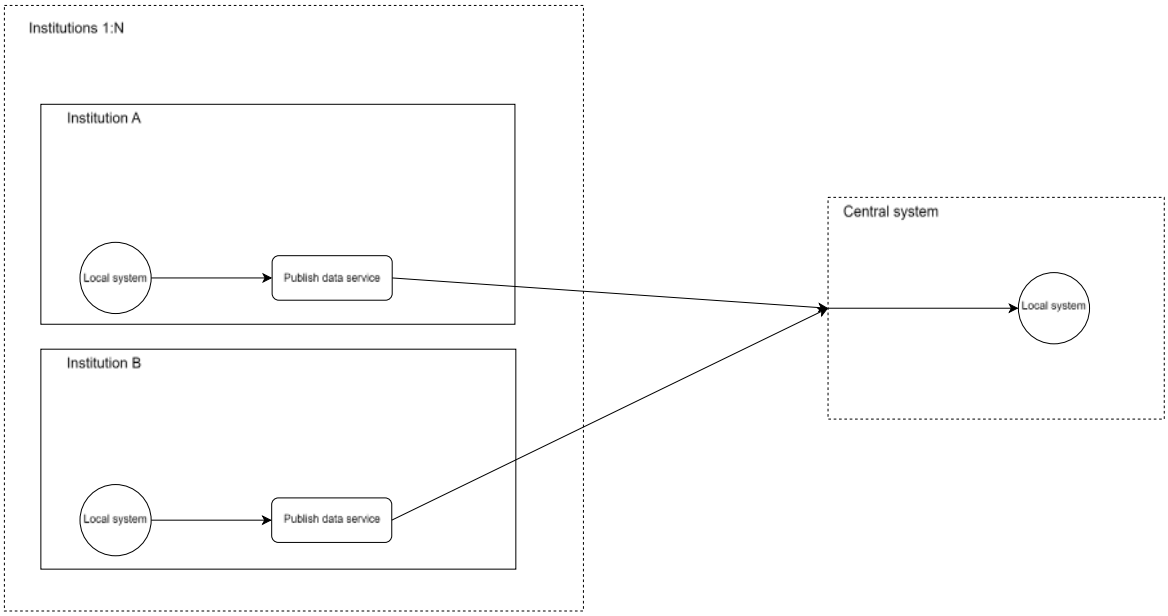


Figure 5 - Sending system synchronisation approach.

© 2025 European Union

Sending system ("push"): In this approach local systems send updates to the central catalogue system whenever they find an update. This is not always possible since some existing systems cannot implement the required mechanisms to trigger the synchronisation process based on update events. This approach has a drawback, central systems do not control when local systems are connecting to synchronise data. This exposes a scalability challenge depending on the communication protocol used. If is a synchronous protocol the central catalogue must be able to scale out to manage request peaks. Such problem can be avoided either at the organisational level by including in the agreements when should each institution synchronise data or leveraging an asynchronous protocol such as message queues.

0.5.2 Mapping implementation

Local systems work with their own data models. Semantic interoperability is key to allow sharing information between different systems and being able to present coherent data from different system to the user. Mapping services are building blocks providing translation capabilities. They work based on a semantic interoperability agreement specifying the data standard to be used. Depending on who implements the mapping service we have the following approaches:

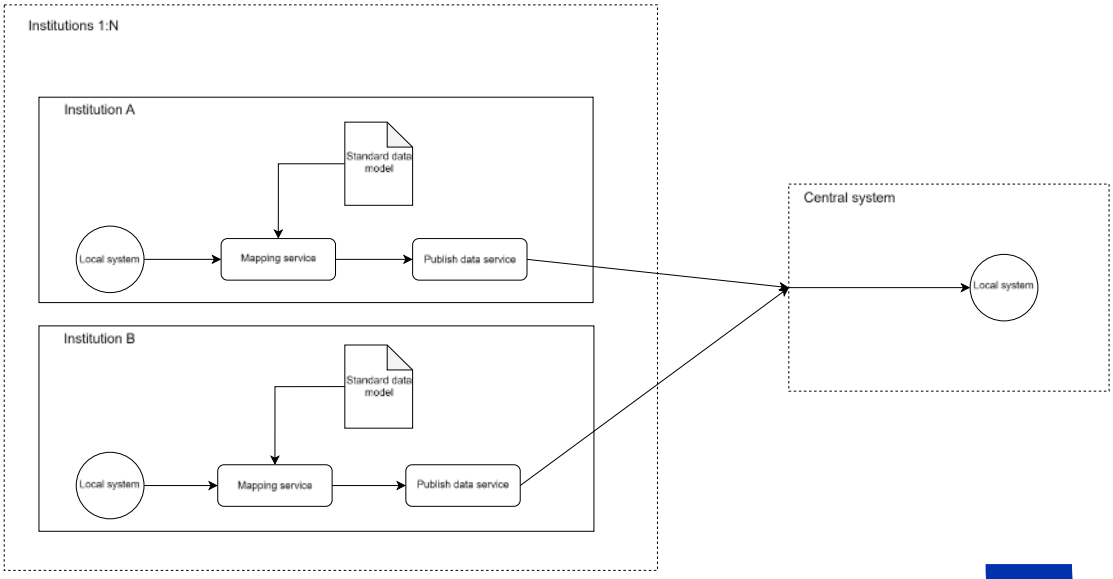


Figure 6 - Sending system mapping approach.

© 2025 European Union

Sending system: In the central system strategy each institution publishing to the central system should adhere to the central standard. That is, each institution oversees the implementation and management of mapping services required to communicate their data to the central system. This approach is easier for catalogue operators since they only must validate received data based on a single data model and maintain a single communication protocol. This poses a scalability issue for institutions publishing opportunities to different catalogues since they must implement one mapping for each of the different data models and publishing services for each communication protocol. This challenge becomes even more crucial in the broadcast strategy, having to develop and maintain as many mapping services as connected institutions. Another approach in the broadcast strategy is to implement a mapping service translating from the central standard to the local data model.

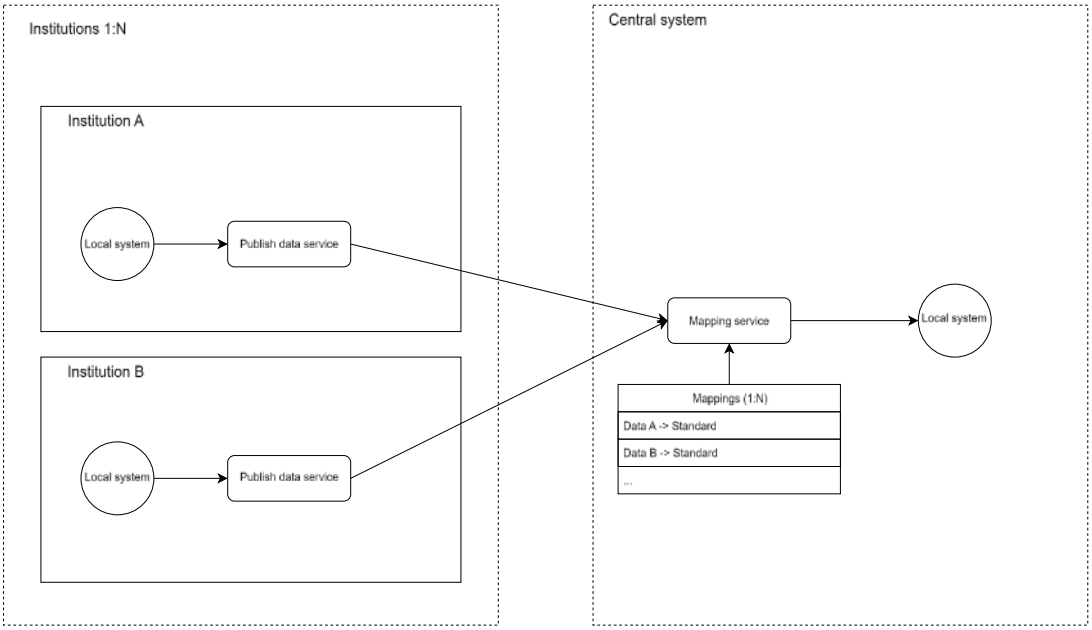


Figure 7 - Receiving system mapping approach.
© 2025 European Union

Receiving system: In the central system strategy this approach is easier for the institution, on the other hand the central system must support every data model. Some alliances find this approach more suitable and faster to implement than waiting for the members to implement their own mapping services. The broadcast strategy shares the same problem with both approaches. Implementing a two-way mapping service may help diminishing this problem.

In chapter 9 - Mapping and Data Standards, the mapping of local data to standards that promote interoperability between institutions and alliances is described in greater detail.



PART 1

Use case 1 – Discovery

1 Use case 1 – Discovery

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

© 2024 Freepik

1.1 Use case definition

This Discovery use case lies at the start of the learner's journey. The chosen scope of the use takes a specific focus on the concept of a course catalogue, which is the key information tool that higher education institutions and EU-As provide to prospective students. Whereas the broader phase of discovery might also involve the learner gaining insight into the demands of the labour market or using tools to discover one's own preferences and talents, these are not necessarily in the remit of EU-As.

The course catalogue is a tool for the management of various learning opportunities offered by an institution, an alliance, or any other form of collaboration between HEIs. Educators design learning opportunities, prepare learning activities and assessments to be incorporated into the catalogue. Learners interact with course catalogues to appraise and compare learning opportunities.

A joint course catalogue assembled by many EU-As, enhances the visibility and comparability of diverse learning and mobility opportunities across HEIs. In the use case the importance of aligned metadata of courses is emphasised so that learning opportunities can easily be collected for comparison and discovery.

1.2 High-level flow

The discovery use case is defined by two main processes: the design and publication of a learning opportunity, and the search of relevant opportunities. This use case has the following stakeholders involved:

- **Catalogue user:** An individual looking for learning opportunities. Can be an educator, a learner already registered in an institution, or a potential learner looking for the most relevant learning opportunity.
- **Publishing institution / HEI:** An institution sharing one or more learning opportunities. Includes different stakeholders overseeing steps of the process such as educators or administrative staff.
- **Catalogue operator:** An organisation or unit designated to manage and operate a central catalogue. Oversees validation processes and overall quality of the catalogue contents.
- **Qualification standards body (Economy):** A designated body defining skills required to practice regulated professions[5].
- **Joint degree consortium:** Steering body managing the organisational tasks required to design, develop, and deliver a joint degree. Usually with representatives from the institutions involved.

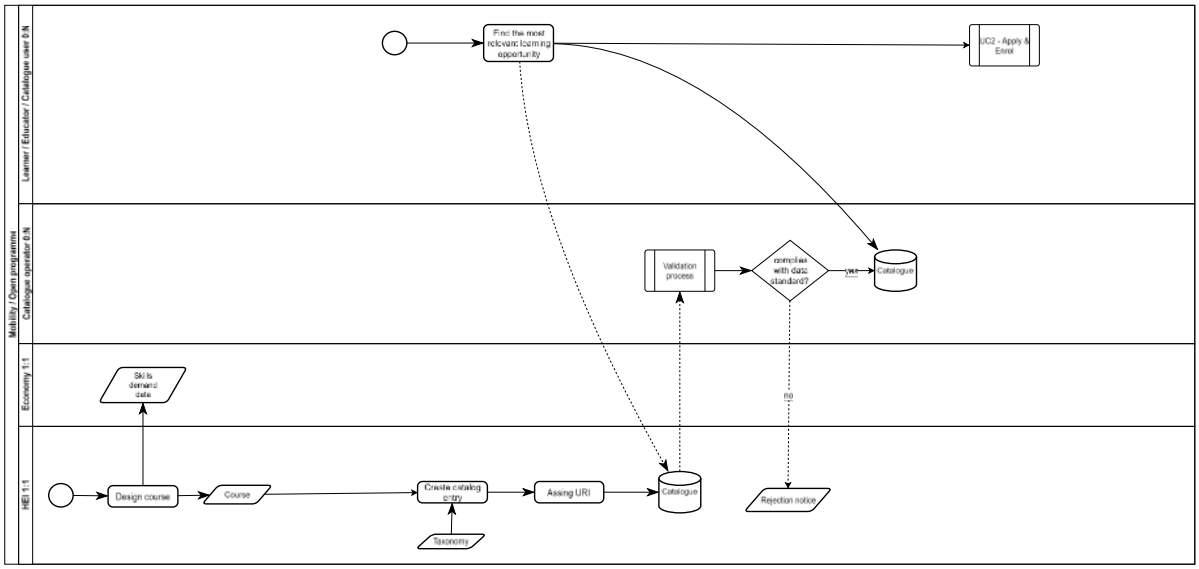


Figure 8 - Design and search of learning opportunities in mobility and open programmes scenarios.
© 2025 European Union

Educators in their institution design a learning opportunity that is based on a skillset sought after. This process has been kept abstract since processes differ by institution. This project does not intend to modify existing processes, but rather to propose general processes that can be easily adapted to local ones. Along these lines, quality assurance processes that are sensitive and locally managed processes, are excluded from the scope of this data flow. Once the learning opportunity has been designed, it is incorporated into the local

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

catalogue. As will be shown later, there exists a myriad of tools that can be used to store opportunities, each of them involving specific changes to the steps of creating an entry into the catalogue and generating the uniform resource identifier (URI)[6] to access them. In some cases, the URI will be the outcome of creating the entry in the catalogue. Once a learning opportunity has been included in the local catalogue, it is possible to publish it in a central catalogue. This part of the flow is optional since there are some approaches without a central catalogue where data is collected in real time from the different local catalogues and presented to the user. With a central catalogue in place, incoming data must undergo a validation process to ensure that the information complies with the required format and all required attributes have been properly included prior to incorporating it into the central storage.

The second process depicted in Figure 8- Design and search of learning opportunities in mobility and open programmes scenarios focuses on discoverability of available learning opportunities. The search process may lead to the potential learner applying to an opportunity, therefore a link to the use case 2 – Apply and get recognition has been included at the end of the search process.

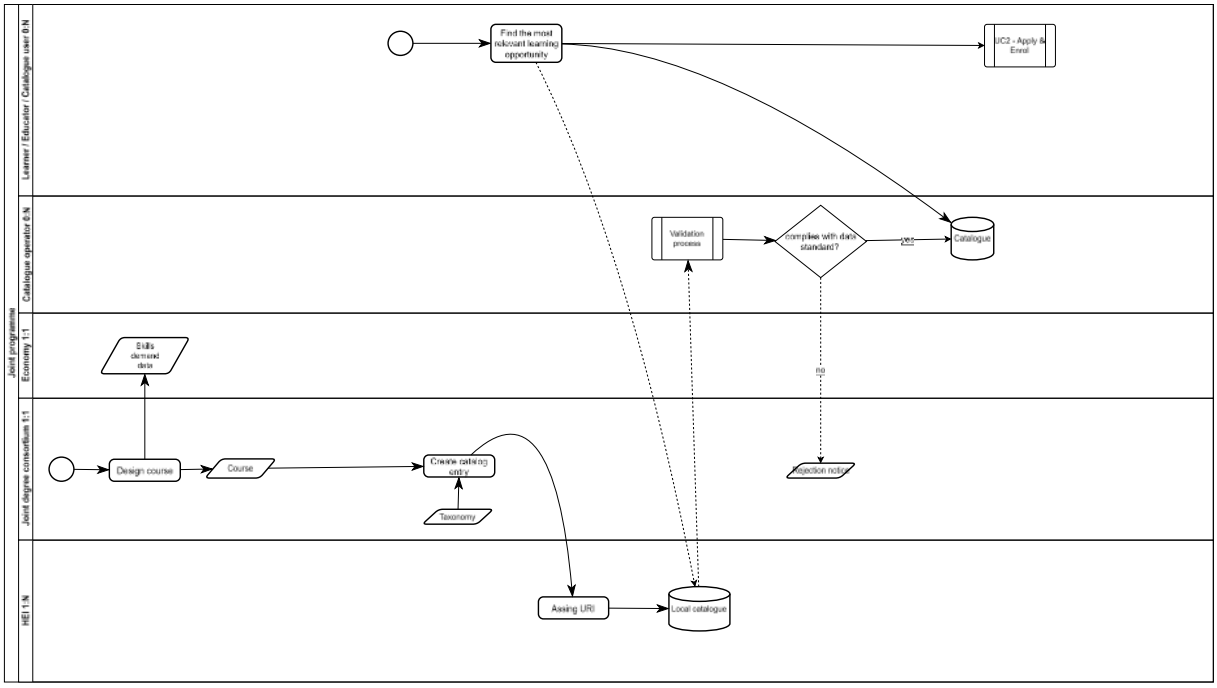


Figure 9 - Design and search of learning opportunities in joint programmes scenario.
© 2025 European Union

[6] Brown, M, McGreal, R RFC 3986: Uniform Resource Identifier (URI): Generic Syntax (rfc-editor.org)

The joint programmes scenario poses some particularities. Institutions involved jointly design the learning opportunities offered. In this scenario, the specification must follow a common schema that can be included later into the local catalogues, exposing the first technical interoperability challenge. Once the specification has been incorporated into the local catalogues, the institution overseeing a specific offering to the learning opportunity includes it in its local catalogue prior to publishing it to the central catalogue with its specific URI. The rest of the process remains the same and no further changes are required.

1.3 Draft architecture

The original draft architecture has been challenged and revised during the squad sessions, resulting in below diagrams. All three scenarios outlined previously impact the reference architecture of this use case. All three share the same basic components that are outlined in Figure 9 - Design and search of learning opportunities in joint programmes scenario. The joint programme and mobility diagrams include additional components required to cope with the nuances of their scenarios.

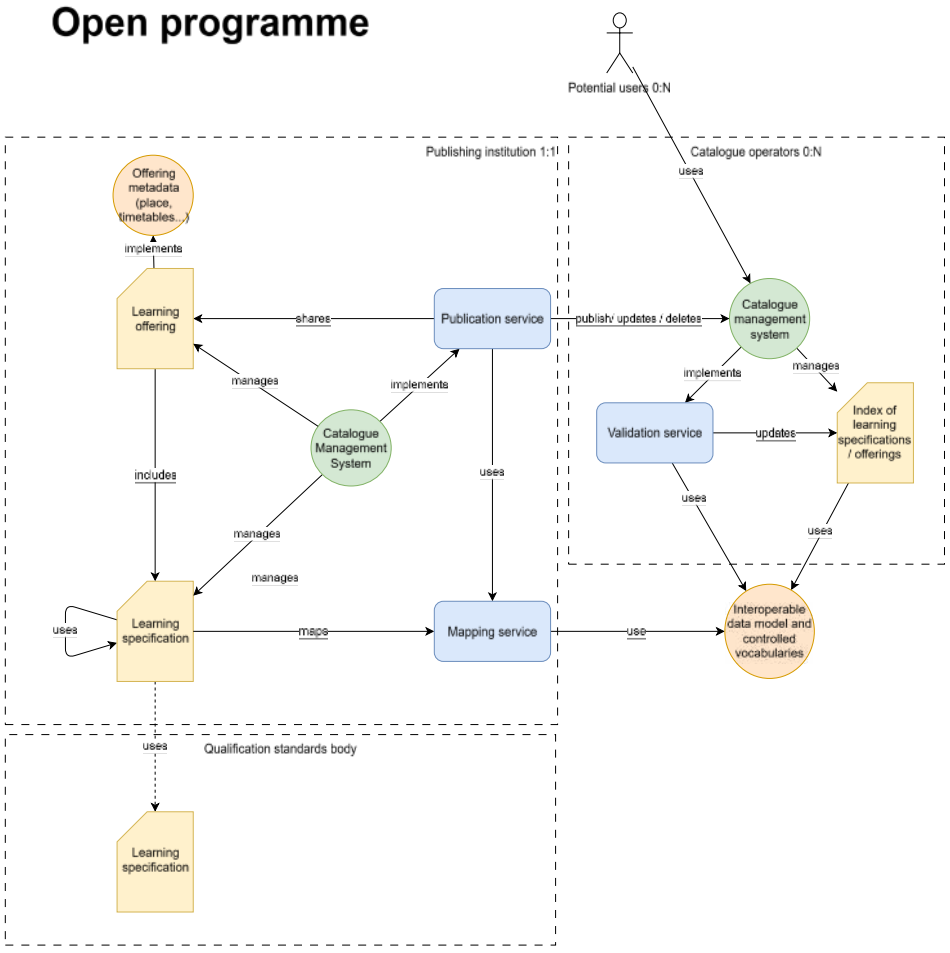


Figure 10 - Main components required to manage a central catalogue of learning opportunities.
© 2025 European Union

Main components inherent to this use case are:

Business objects

- **Learning specification:** Definition of a learning opportunity, includes the description of the different learning activities that will be conducted, the set of requisites to enrol, the specification of the learning assessments and learning outcomes achieved upon completing the opportunity.
- **Learning offering:** A specific instance of a learning specification that takes place in a specific academic calendar. Includes scheduling information. Even if the European Leaning Model (ELM)[7] standard does not differentiate between learning specification and offering, most alliances' management systems clearly differentiate. This differentiation is reflected accordingly in the architecture to support existing implementations. Throughout this report, specifications and offerings will be referred to as 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:** Service in charge of collecting information from management systems that do not offer publishing or exporting mechanisms. Harvesters usually scrape data from existing systems and prepare it to be sent to the central catalogue. Another usage of harvesters is to collect and merge information from different services to facilitate the mapping between different data models or standards.
- **Publication service:** Service sending information from a local catalogue to the central one. Publication services should be using the same communication protocol than the catalogue ingesting service.
- **Validation service:** Service to check that data received adheres to the data standards and complies with the minimal required fields agreed beforehand. Validation services are not intended to interfere nor overlap with quality assurance processes and focus only on data structures compliance.

Systems

- **Catalogue management system:** System to manage the catalogue of learning opportunities.

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

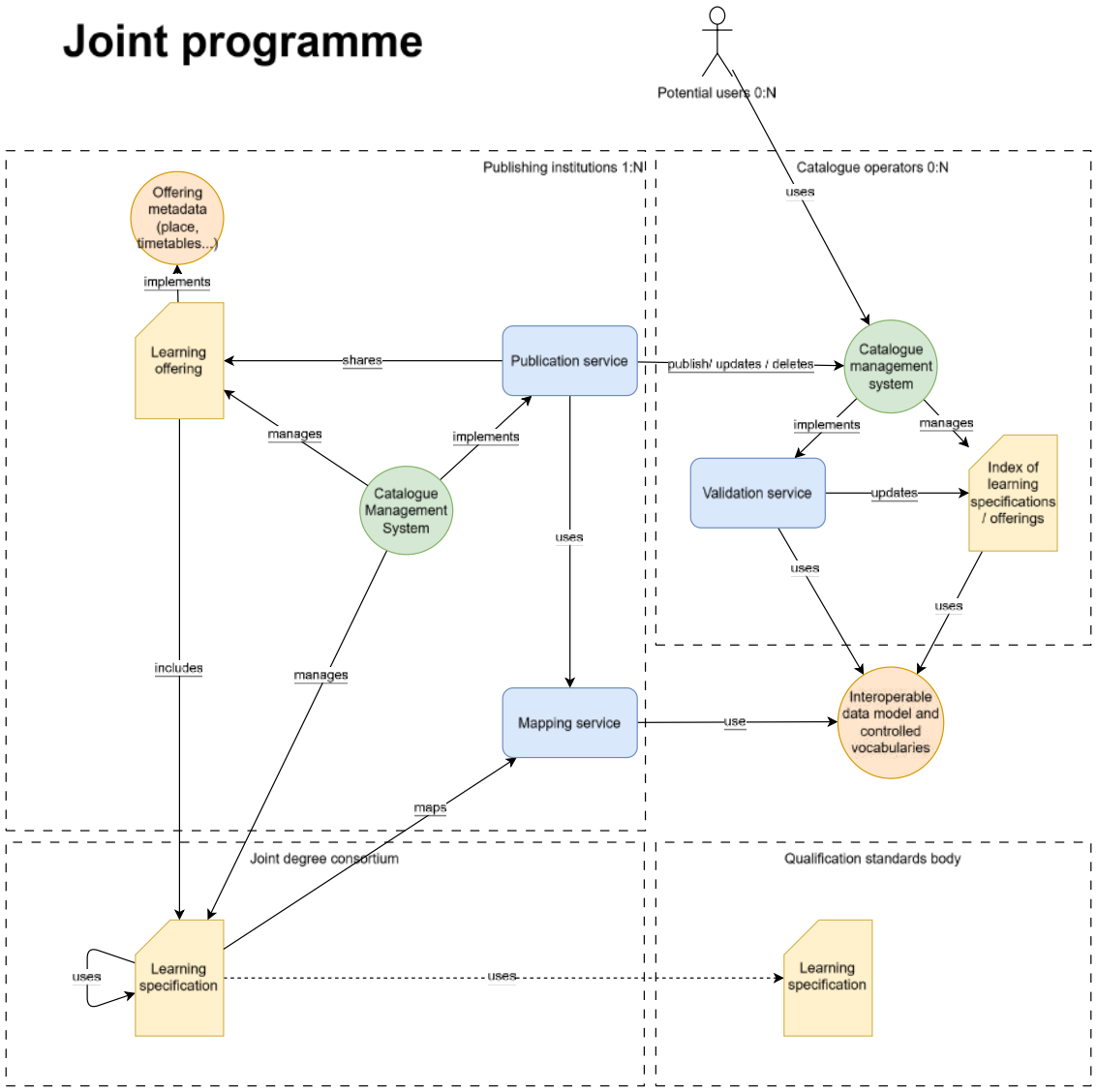


Figure 11 - Specific components required to work with a central catalogue managing opportunities belonging to a joint programme.
© 2025 European Union

This scenario focuses on learning opportunities of joint programmes. Institutions involved in the joint degree design the curriculum delivered. This leads to a shared learning specification that may or may not be compatible with all the different local data models. To overcome such a challenge, the mapping service can be leveraged to translate specifications to the local models.

Learning specification can be stored in every local catalogue managed by an institution involved in the joint programme. On the other hand, offerings are managed by the local catalogue of the institution delivering a particular instance of the opportunity. The rest of the process remains untouched, and components behave as depicted in Figure 10 - Main components required to manage a central catalogue of learning opportunities.

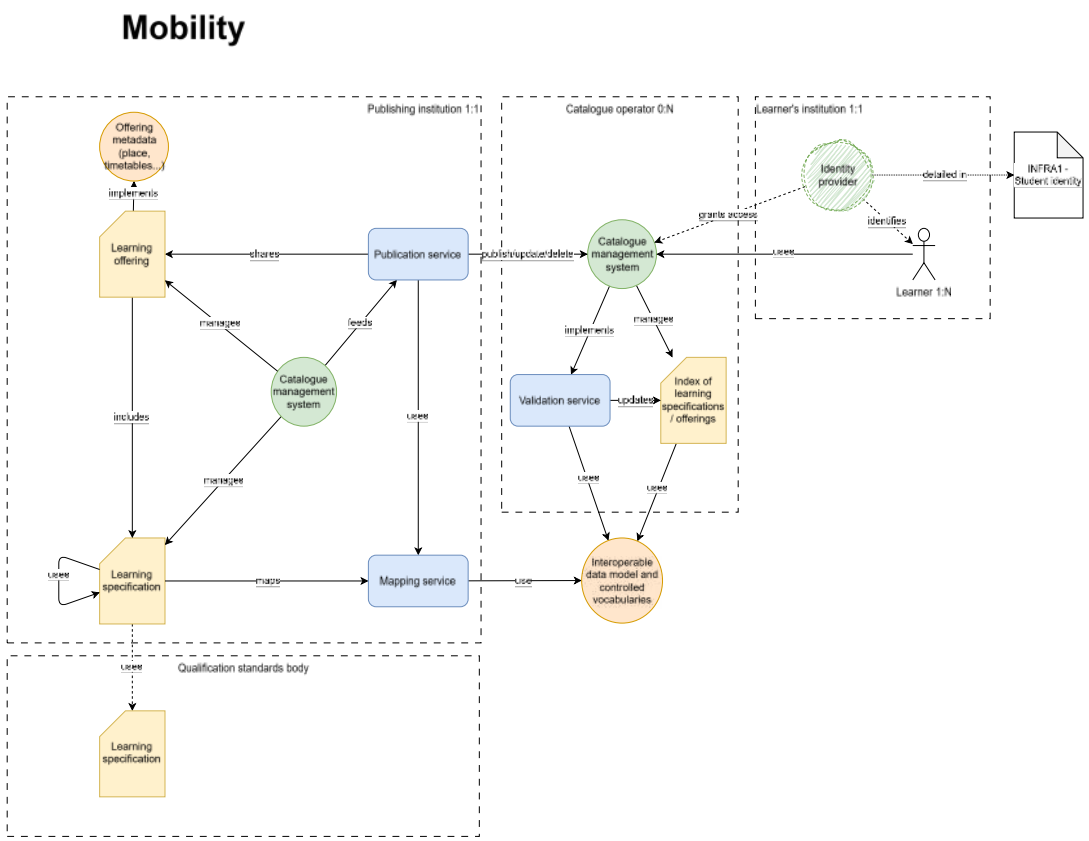


Figure 12 - Optional identity provider to filter opportunities available for a mobility.
© 2025 European Union

In a mobility scenario, the only particularity is that an identity provider can be optionally included to allow filtering learning offerings available to the learner based on previous agreements.

1.4 Interoperability required capabilities

The definition of learning opportunities offered by institutions has proven to be crucial. This definition should be guided by a set of best practices that not only facilitate interoperability but also enhance the visibility of the offered opportunity. These best practices include the use of controlled vocabularies and standards.

Following a solid data standard to facilitate interoperability in terms of agglutinating learning opportunities across institutions in a common catalogue leads to a smoother discovery experience.

However, the discovery process could also be cumbersome due to the wide range of vocabulary that could be used to refer to the same type of information. The heterogeneity of the vocabulary used by the different HEIs was identified as a major obstacle. This means that a standard should be followed not only in the data models, but also in the vocabulary. Homogeneous vocabulary and learning opportunities organised with common, appropriate tags significantly increases productivity and the ease of finding relevant learning opportunities from both a learner and educator perspective.

Given the absence of a common standard for vocabulary and taxonomy at the HEI level, the need for an intermediary arises. This role is fulfilled by the mapping service in the draft architecture. It is tasked with transforming each unique HEI learning opportunity into a standardised one.

1.4.1 Communication

This section covers the communication capabilities related to the publication of learning offerings in virtual catalogues through the identified implementation approaches. These approaches serve as a foundation for developing more complex solutions that adapt to the specific needs of each institution's internal architecture within an alliance. Two main pathways are defined: centralisation and decentralisation in the storage and exposure of data. These approaches, being foundational, can be modified, even creating hybrid models, combining both centralised and decentralised elements.

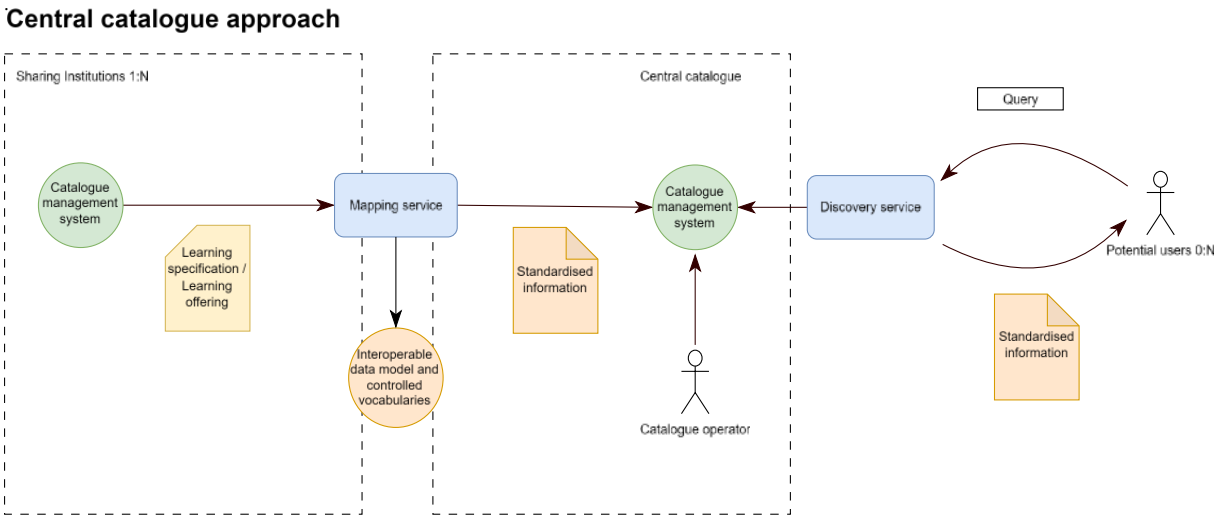


Figure 13 - Central catalogue approach dataflow with architecture components.
© 2025 European Union

All relationships between components in the data flow should be secured. The Central Catalogue Management System should be accessible from different connection sources. The catalogue operator needs direct access to this system to validate and incorporate new incoming learning offerings. The learning opportunities should be discoverable by potential users through a discovery service, including providing open and secure learning offerings. Discovery service may or not be implemented by the central catalogue.

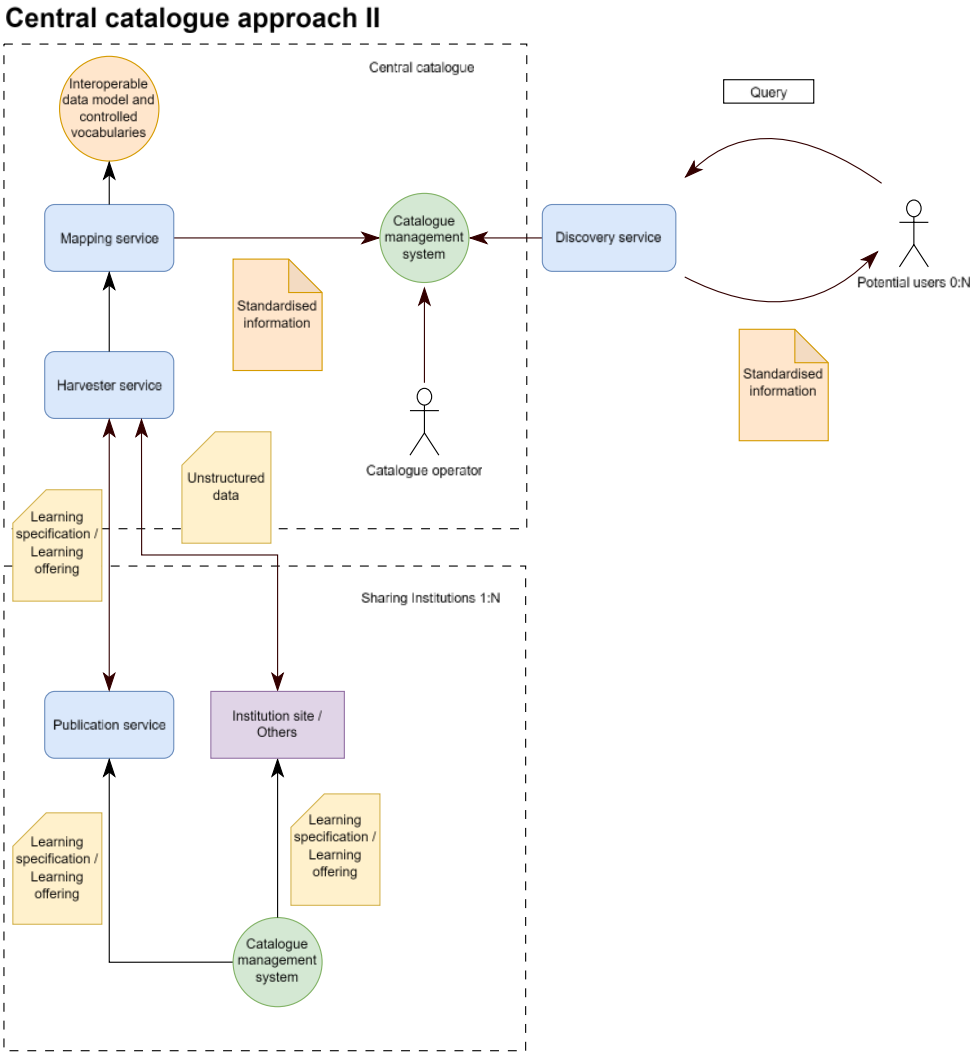


Figure 14 - Central catalogue approach dataflow with architecture components – no sharing service provided by HEIs scenario.
© 2025 European Union

A harvester service on the central catalogue side is required if HEI without a sharing service is to be included in the catalogue. Harvesting offerings data from various sources results in heterogeneous data, resulting in the need for implementation of a mapper service in the central catalogue. With this service, unstructured data can be standardised and stored in the central catalogue.

Collecting opportunities in a central catalogue leads to delicate synchronisation scenarios. The capabilities to manage these scenarios are described in section 0.6.

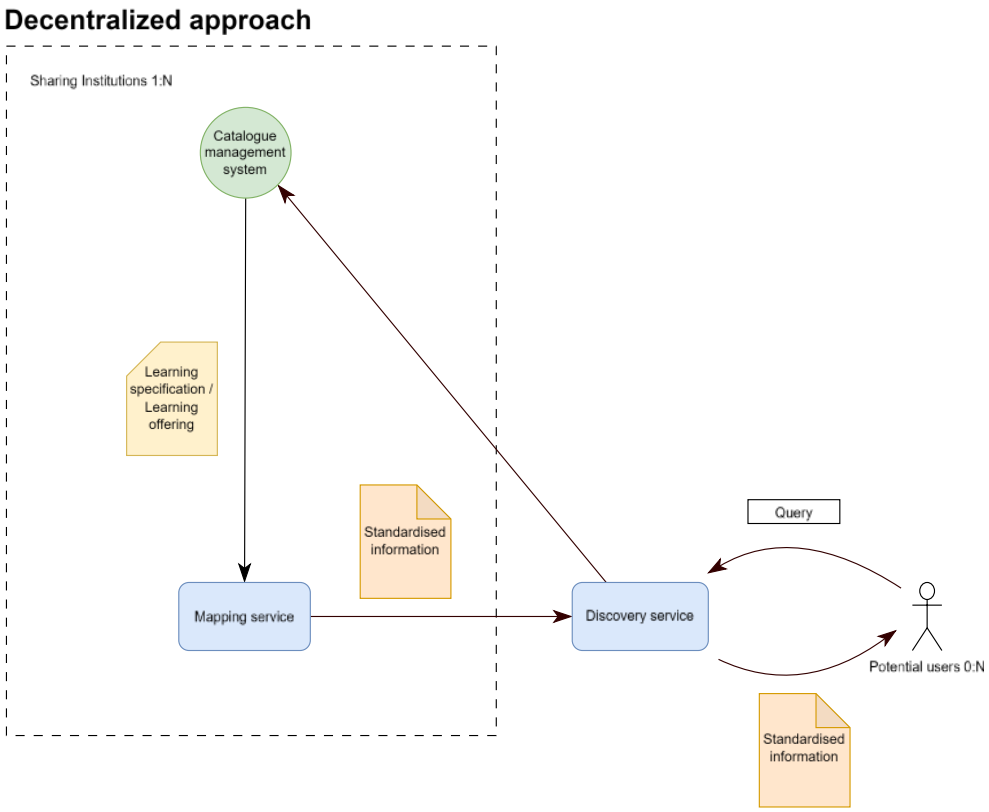


Figure 15 - Decentralised approach dataflow with architecture components.
© 2025 European Union

HEIs store their defined learning offerings in Local Catalogue Management Systems managed by themselves. On the condition of openly sharing opportunities (decentralised approach), external secured communication with the local offerings catalogue is required.

Regardless of the implementation approach chosen, a scalability plan should be planned in the exposed systems and services. This would prevent communication congestion and platform availability issues. Also, a security layer should be included to protect the systems from possible malicious attacks (e.g., Distributed Denial of Service[8]).

[8] DDoS: https://csrc.nist.gov/glossary/term/ddos

1.4.2 Boundaries

Use case 2 (apply and get recognition)

Within the definition of a course, the specification of learning outcomes plays a crucial role, especially in Use Case 2. A standardised definition of these learning outcomes, using controlled vocabularies, is a practice that facilitates not only the understanding of the course outcomes, but also the subsequent recognition of credentials issued by third parties. This approach also increases the transparency of course content and helps to build trust between institutions.

Use case 7 (user identity)

In this use case, it is essential to differentiate the user accessing the course catalogue to provide an appropriate user experience. Therefore, the user's identity on access must have a minimum set of defined attributes that allow the system to identify their origin (whether they are from the same institution or from another institution with which they have mobility agreements), their role and, ideally, their previous experience. With this identity information, it will be possible to pre-filter and display the most relevant learning opportunities for the learner, and to restrict access to those that are not relevant to them. In addition to identity, an appropriate level of assurance (LoA) must be defined to ensure the credibility of the identity provided before access to the catalogue is granted.

1.5 Overview of resources in use

Many of the solutions attempted by alliances are yet in planning or development. This has two implications: systems implemented may change and new interoperability features may be implemented. The gap analysis resulted in a portfolio of applications, ranging from home-made solutions to off-the-shelf solutions to such solutions that originally were not designed as catalogue management systems.

After the sessions held with the alliances, more than half of the registered tools have been developed by the institutions themselves to meet the needs of this use case. This suggests that there may not be a commercial or open-source tool currently available that fully meets these needs. Among the tools, the open-source solution EduXchange is the most chosen. The open standard that could satisfy the needs of this use case is OOAPI. Both services and standards are described in the following tables.

1.5.1 Standards

This section includes a table that contains most used data standards, protocols, standardised APIs or similar identified in the project, which can be implemented by tools and services.

Excludes: purely internal, unpublished standards used only by a specific tool.

Name	Information	Capabilities covered		Open standard	Owned / maintained by
		Learning opportunity standard	Publication service		
EWP Courses API	API specification used for sharing Course Catalogues in connection with Erasmus+ mobility Learning Agreements.	✓	✓	✓	EWP consortium on behalf of DG EAC
ELM	European Learning Model	✓		✓	DG EMPL
Edu-API	Specification for the standardised exchange of data between the transactional systems that manage higher education administration, teaching, and learning.		✓		1EdTech
CASE	Technical specification that establishes a standard way to exchange information about academic standards, competencies, and learning outcomes across platforms and applications.	Sharing competences and skills acquired upon completing a learning opportunity		✓	1EdTech
LIS	Learning Information Services (LIS) specification defines how systems manage the exchange of information that describes people, groups, memberships, courses, and outcomes within the context of learning		✓		1EdTech
ESCO	European Skills, Competences, Qualifications and Occupations (ESCO) is the European multilingual classification of Skills, Competences and Occupations.	Sharing competences and skills acquired upon completing a learning opportunity			1EdTech
OOAPI	It is an open API for HEIs to share educational data in a structured and efficient manner. It enhances the management of various software systems within the institution, promotes the reusability of software components, and improves the student experience.	✓	✓	✓	SURF

OneRoster	The OneRoster standard defines data models for the core elements necessary for digital teaching and learning. OneRoster defines information about people (users), courses, enrolments, organisations, and grades.	✓		✓	1EdTech

1.5.2 Services and tools

This section provides a table listing the main inter-institutional networks (e.g. Europe-wide, national, regional, alliance-wide), services, software, federations, platforms, etc. that institutions (or alliances) can connect to for data exchange or aggregation. It includes both open and commercial options that are of minimum relevance for this use case.

A complete list of identified services and tools could be found in Annex I – Inventory of tools and services.

Name	Information	Offered / managed by	Openness	Standards used
EduXchange	Open-source catalogue solution adapted for international use, which implements a custom identity provider. This centralised catalogue is filled with information from the local course databases via SURFeduhub using the OOAPI standard. It makes application seamless thanks to MyAcademicID login service.	SURF	Existing deployments for NL & alliance, but reusable as open source.	OOAPI, MyAcademicID
BLOOM Hub	EDigital infrastructure to link local software of universities.	OpenU project	Open access	LTI
EWP Network	Erasmus Without Papers is a network for exchanging data related to Erasmus+ student mobility. It is based on a collection of standardised APIs that are implemented by HEIs individually, through third party-systems integrating EWP APIs or the EWP Dashboard, and a central registry service.	EUF for DG EAC	EWP consortium	EWP Courses API
QDR	The Qualification Dataset Register (QDR) serves as a central portal for qualifications, learning opportunities and accreditations. It enables different governmental institutions and awarding bodies to publish their information to the European infrastructure.	DG EMPL	Open access	ELM
ILIAS	It is an open-source learning management system. It has features like course calendar, class reservation, automatic mails on application and certain actions...	Free Software Foundation	Open access	SCORM, LTI, LOM metadata

1.6 Analysis

Alliances have identified that a significant challenge lies in implementing a centralised or global catalogue due to the differing data models of each alliance, hampering data portability and standardisation.

To address these gaps, alliances have adopted scraping solutions to collect all courses from their websites for inclusion in their centralised catalogue. Although this method is cost-effective and may seem practical, it lacks validation or mapping services. Mostly, the raw data is directly entered into the catalogue, which hinders both comparison and the maintenance of data quality.

Above tabular comparison shows that there is no solution that fully implements all required services. Yet, some of the solutions possess features that simplify the implementation of the remaining services or are compatible with other existing tools.

There are alliances that already have implemented their solutions to achieve their goals.

Knowledge Hub is a project that aims to maintain and further develop a knowledge sharing facility based on open W3C Semantic Web Standards. Even though this solution is yet in development, it allows for posting of courses in a standardised way, which fills the Publication Service gap. This solution does not implement a Mapping Service nor a Validation Service but since its data model is standardised, machine-readable and implements some enumerations, the mapping between data models and controlled vocabularies can be easily developed[9]. The alliance implementing Knowledge Hub intends not to replace their local data but to map it on the centralised catalogue.

VURS[10] is a catalogue solution adopted by the EPICUR alliance, based on the open source Student Information System, UniverSIS[11], adapted for international use, that interoperates with any OpenIDConnect identity provider (including SSO services provided by GEANT). This centralized catalogue could be filled with information from the local course databases via OneRoster Standard, CampusConnect and other Rest Interfaces. It makes application seamless thanks to MyAcademicID login service. Also, all courses follow the same template. VURS can support hybrid architecture (including centralised and decentralised bidirectional services). The implementation of standards in solutions facilitates filling of gaps or revealing of missing components.

Other alliances have approached the problem of a centralised catalogue by developing a new joint catalogue. Yet, this approach requires students to apply to the courses in the original HEI catalogues.

[9] As stated on https://data.ec2u.eu/datasets/courses
[10] VURS information can be found here: https://epicur.auth.gr/vurs/
[11] UniverSIS information can be found here: https://universis.gr/en/ - https://gitlab.com/universis



PART 2

Use case 2 – Apply and get recognition

2 Use case 2 - Apply and get recognition



© 2024 Freepik

2.1 Use case definition

The Apply and get recognition use-case focuses on enrolment for a learning opportunity and the creation of the online learning agreement. Getting recognition refers to the appraisal of the learner's previous credentials, which is critical for an admission decision. Thus, the use case aims to simplify credit recognition and cross-institutional enrolment, emphasising seamless data exchange to support all forms 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 can be split into two main processes, the application which implies the identity validation, and the evaluation of the application, which may imply some requisite validation and the signing of an agreement.

This use case has the following stakeholders involved:

- **Learner:** An individual who may get enrolled in a higher education programme. These learners pursue various degrees, such as bachelor's, master's, or doctoral degrees, and 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. E.g., may be presented as a web or mobile application.

- **Sending / Receiving HEI:** In a mobility programme the Higher Education Institutions involved.
- **Designated registrar:** one of the institutions in a joint programme consortium, or an additional unit/ body (e.g., at alliance-level), that coordinates the admission and enrolment process.
- **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 that belongs to an alliance. They can be N per each alliance. On the joint programme scenario are the ones that manage application.

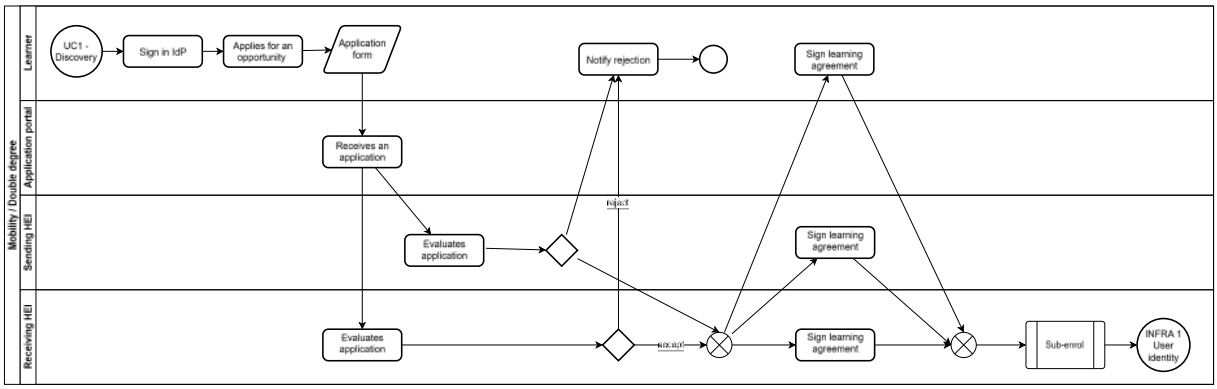


Figure 16 - High-level data objects, steps, and responsibilities to evaluate an application in a mobility scenario.
© 2025 European Union

Mobility scenarios have some particularities inherited from the Erasmus+ programme. Learners are already registered in the sending institution and there is a learning agreement signed by all three parties, sending institution, receiving institution and learner. The Learning Agreement sets out the programme of the studies to be followed in the receiving institution and ensures that the learner will receive automatic recognition of all credits gained for learning outcomes satisfactorily achieved during the mobility[12]. In any scenario within the flow, if a single institution rejects the learner's application, the application process is aborted. This is because, for the flow to proceed, there must be agreement among all parties involved.

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.

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

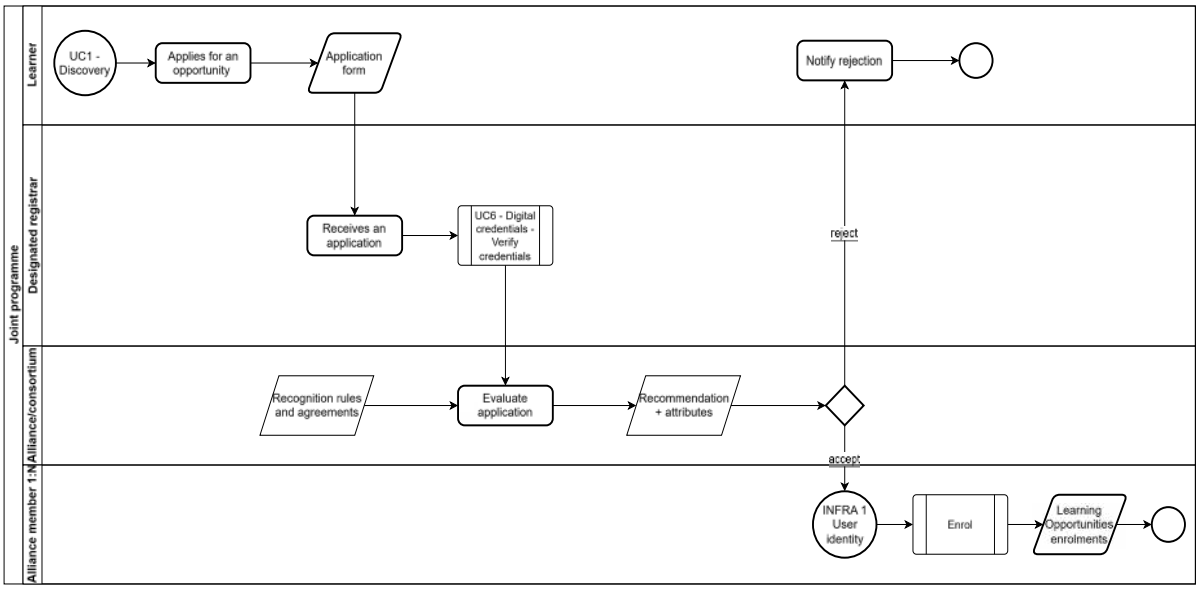


Figure 17 - High-level data objects, steps, and responsibilities to evaluate an application in a joint programme scenario.
© 2025 European Union

2.3 Draft architecture

This use case requires the following main components:

Business objects

- **Identity attributes:** Attributes required to verify the identity of a learner. This data object will be explained in detail in the use case focused on user identity.
- **Credentials:** Physical or digital credentials certifying previous learning achievements or claims presented by a learner.
- **Application:** Includes all the required data to validate and verify the eligibility of a learner to participate in a learning opportunity.
- **Recognition rules and agreements:** An organisational interoperability agreement including rules to recognise previous achievements presented by a learner.
- **Learning offering:** A specific instance of a learning specification that takes place in a specific academic calendar. Includes scheduling information.
- **Learning specification:** Definition of a learning opportunity, includes the description of the different learning activities that will be conducted, the set of requisites to enrol, the specification of the learning assessments and learning outcomes achieved upon completing the opportunity.

Services

- **Validation service:** Service to validate the information from an application.
- **Requisite compliance check service:** Service overseeing the verification of learner's previous achievements match the required skills to enrol in an opportunity. In some scenarios the scheduling constraints of a specific offering must be considered.

Systems

- **Identity provider:** System managing learner identity. Described in detail in the use case focused on user identity. Oversees the identification of learners and manages identity attributes required to authenticate and authorise access to the required systems.
- **Catalogue management system:** System to manage the catalogue of learning opportunities.

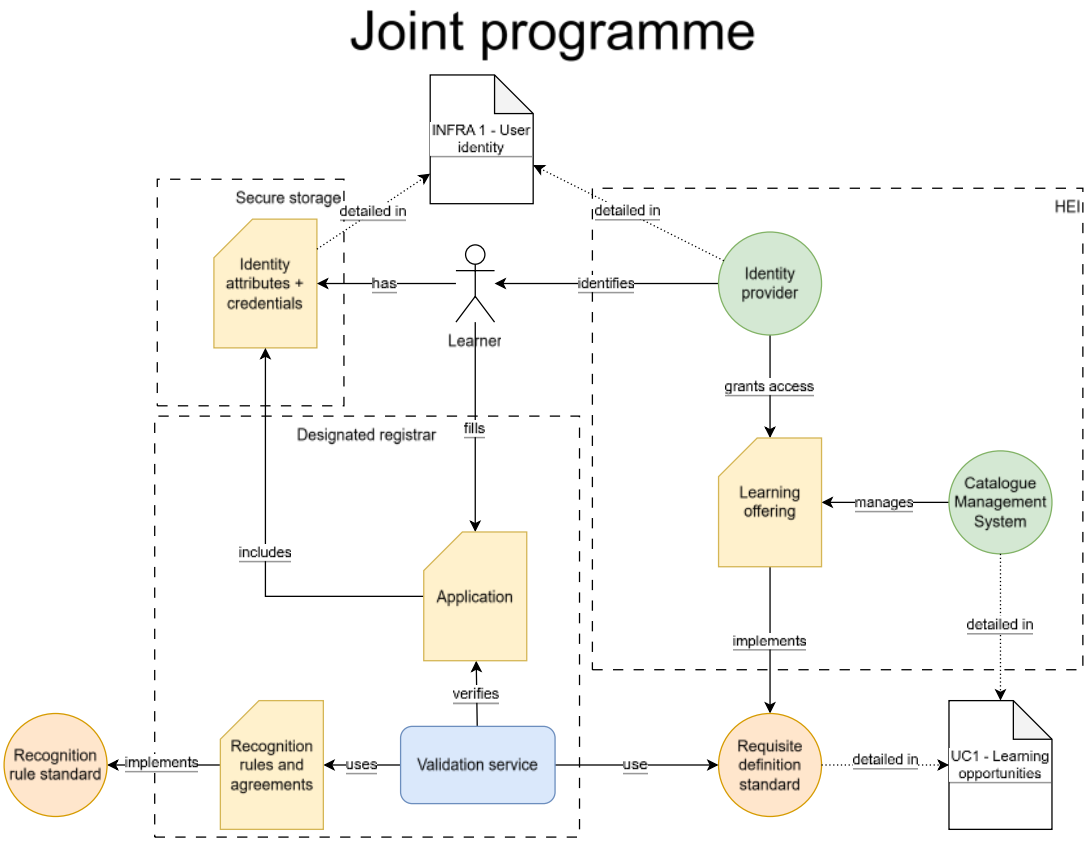


Figure 18 - Main components required to evaluate an application in a joint programme scenario.
© 2025 European Union

The mobility scenario is heavily influenced by the existing Erasmus+ process. In this scenario learners are already registered in their home institution and have an identifier available. Both institutions have previously assessed the quality requirements of the other institution, exam committees have verified the assessment policies, and an inter-institution agreement has been signed.

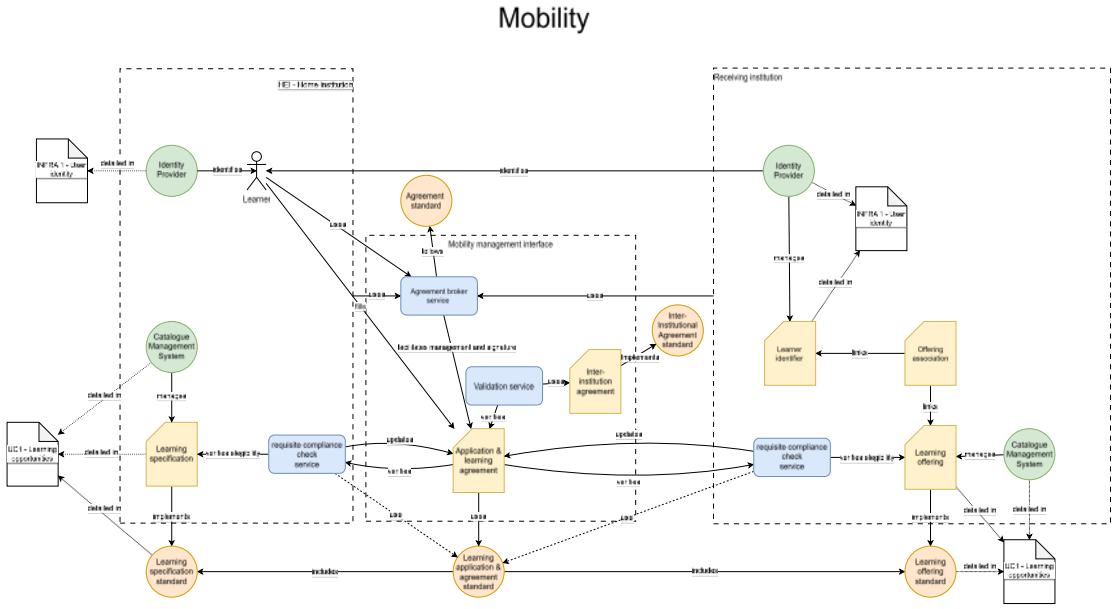


Figure 19 - Main components required to share learner data in a mobility scenario.
© 2025 European Union

The process begins with an application form filled by learners, including the list of learning offerings they wish to take in the receiving institution and the list of learning specifications to be recognized upon successful completion in the receiving institution. The application must be validated in both institutions. To make this validation process interoperable learning agreements should adhere to a data standard facilitating the requisite compliance check process. There are three main concepts to verify:

- The application complies with the inter-institutional agreement.
- The home institution verifies that the learner can enrol in the learning specifications. This process involves matching the specified requisites of the learning specification with previous learning achievements.
- The receiving institution verifies that the incoming learner can enrol in the specified offering. This process includes scheduling checking on top of meeting the requisites defined in the specification.

Once the application has been approved a learning agreement is signed by all the interested parties: learner, sending institution and 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 Interoperability required capabilities

Adapting to the above proposed approaches requires certain interoperability capabilities that are detailed in the following chapters. First, all the data objects requiring (data) 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 being mapped with the requisites of the learning offering.

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

2.4.1 Communication

All component relationships in the data flow need to be secured. Furthermore, this applies to the communication of the application process, as it may contain confidential and personal information. This is particularly important in the mobility scenario where both the application and the learning agreement need to be transferred between different systems.

As can be seen in the image below the application & learning agreement signed on the mobility management interface receive information transfers from the two institutions, the home institution, and the receiving institution. Both update and verify the content of the agreements, so it is important to establish a secure (as it contains personal information of the learner and agreements of the institutions) and reliable communication.

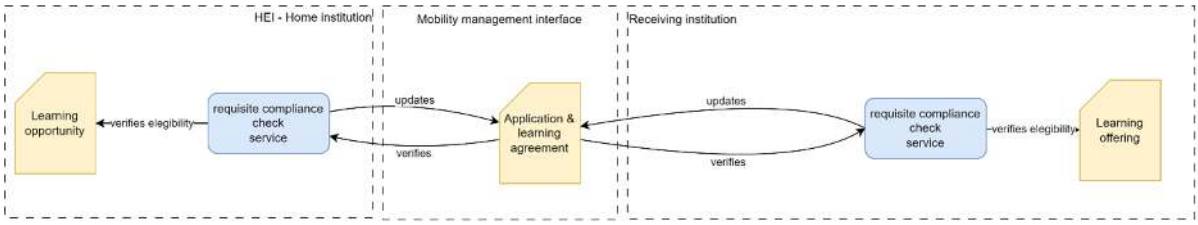


Figure 20 - Communication between Institutions when applicating.
© 2025 European Union

Broker also plays a key role in communications in this use case. Brokers are intermediary software or service that facilitates the exchange of data between different educational systems, applications, or platforms. In this regard, brokers convert data from different formats and standards used by various educational systems into a common, interoperable format. This ensures that data from one system can be accurately interpreted and utilised by another. Although the implementation of these brokers is out of scope, here is a picture of the role they would play in the interoperability architecture.

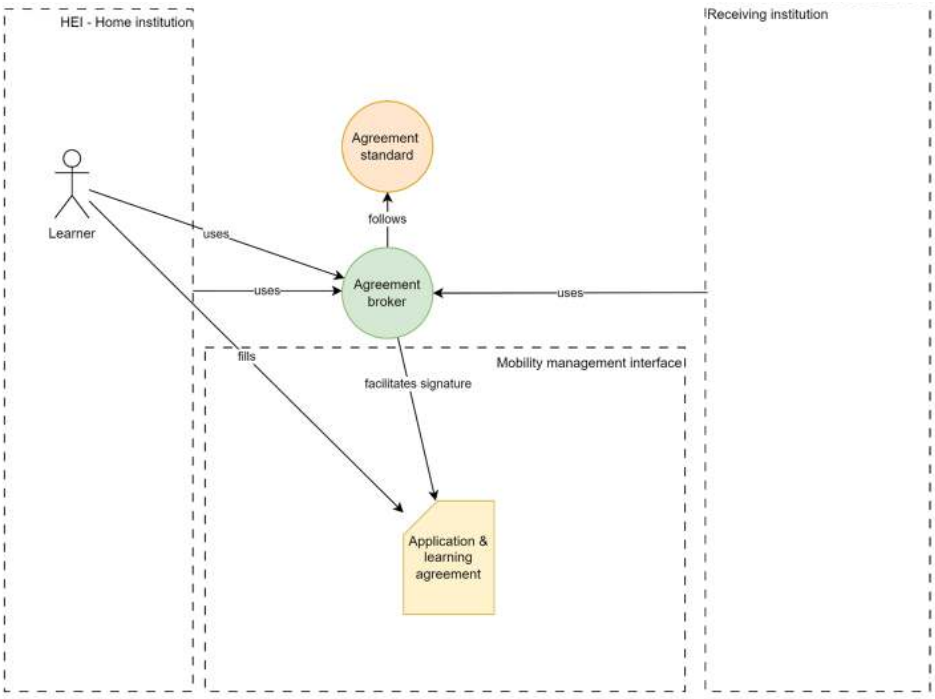


Figure 21 - Role of the agreement broker in Use Case 2.
© 2025 European Union

2.4.2 Data protection and licensing

Similarly, while most user identity data is managed by the identity provider and therefore addressed in the Identity use case, there will also be identity fields included in the application, again especially in the case of mobility. Therefore, it will be important to consider user privacy and data protection. For these reasons, the use of secure communications throughout the process is mandatory, using protocols such as HTTPS. This ensures that communications are protected by encrypting data in transit. Additionally, certain legal aspects may need to be addressed in compliance with laws such as GDPR, as user data may be transferred to systems outside their home institution. This may include agreements between all parties (origin institution - learner - destination institution) regarding data handling in cases of mobility.

2.4.3 Boundaries

Use case 1 (discovery)

The standardised definition of learning outcomes has become a crucial aspect within the educational domain, particularly in the creation of courses and training programmes. As outlined in the boundaries section of use case 1, learning outcomes are linked to the proper structuring of courses. The use of controlled vocabularies and recognised standards not only enables a clearer understanding of the objectives of each course but also facilitates their recognition by third parties, a significant challenge in the current higher education landscape.

The educational community has emphasised the importance of having a standardised definition of these outcomes, as many of the challenges institutions face today stem from the difficulty in aligning their own courses with those offered by other institutions. A clear and uniform definition of learning outcomes not only promotes transparency and clarity in educational offerings but also fosters trust between institutions, which is essential for creating recognition agreements and educational partnerships.

Furthermore, this harmonisation encourages an environment where students can navigate more easily between different institutions, with the assurance that their learning outcomes will be recognised and valued fairly and consistently.

Use case 6 (earn a credential)

The credential recognition flow described in this use case is related to use case 6, which outlines the process by which credentials are issued to learners. To ensure effective recognition of these credentials between institutions, it is crucial that they are generated with the appropriate information and in a standardised format.

The key is for the credential to accurately identify the holder, which requires the use of secure mechanisms to verify the identity of the learner. This is essential to ensure that the credential belongs to the correct individual and is being used legitimately.

Moreover, the credential should include the essential fields for recognition, such as learning outcomes, the issuing institution, the number of credits earned, and any other relevant data that allows institutions to compare and establish the necessary equivalencies. Standardising the elements of the credential not only facilitates its interpretation and validation by third parties, it also helps create an environment of trust between institutions, enhancing mobility processes and recognition of learning in higher education.

Thus, both use cases are intrinsically linked, as the recognition flow depends directly on how credentials are issued and structured. This, in turn, ensures that students' learning is recognised and valued consistently on an international scale.

Use case 7 (user identity)

Use case 7, being foundational for many other use cases, also has a close connection with the credential recognition flow. The learner's identity at the institution conducting the recognition must contain the necessary attributes to enable a match with the identity specified in the credential. This is crucial to ensure that the holder is indeed the rightful owner of the credential.

This process becomes even more complex when the credential in question bears multiple signatures from external institutions, such as in mobility programmes involving universities. In these scenarios, the recognition process must validate each signature to confirm the legitimacy and validity of the document.

A key challenge in the credential recognition flow relates to the mutability of identity. There are instances where a learner's identity may change, for example, if the individual changes their name, which could leave their previous credentials outdated. Additionally, there can be cases where multiple learners share the same full name, further complicating the recognition process.

To address these challenges, efforts are underway to define identifiers that could be either centralised or decentralised, providing a more robust mechanism for unequivocally linking the learner's identity with their credentials. These identifiers would ensure the integrity and security of recognising academic achievements across different institutions, regardless of any changes in the learner's identity.

Use case 8 (institutional identity)

Similarly to user identity verification, when verifying a credential, it is crucial to confirm the authenticity of the issuing institution. For this, the institutional identity attributes associated with the signature on the credential must be well-defined and sufficient to be validated accurately.

This validation process ensures that the credential's issuing institution is legitimate and recognised, adding an extra layer of trust to the credential's authenticity. This is particularly important in scenarios where the credential may be used in various contexts or across different countries.

The process of institutional identity validation is addressed in greater detail in the section dedicated to use case 8.

2.5 Overview of resources in use

In this use case, after the sessions held with the alliances, it was determined that half of them have developed their own tool to meet the needs of this use case. This suggests that there is currently a lack of tools that really apply to this use case. The tools/services and standards used are detailed below.

2.5.1 Standards

This section includes a table that contains most used data standards, protocols, standardised APIs, or similar standards identified in the project, which can be implemented by tools and services.

Excludes: purely internal, unpublished standards used only by a specific tool.

List of capabilities:

- LOS: Learning opportunity standard
- IDS: Inter-institutional agreement data standard
- ECDS: Educational credentials data standard
- ABS: Agreements broker service

Name	Information	Covered capabilities				Open standard	Owned / maintained by
		LOS	IDS	ECDS	ABS		
EWP Courses API	API specification used for sharing Course Catalogues in connection with Erasmus+ mobility Learning Agreements.	✓				✓	DG EAC
EWP Interinstitutional Agreements API	This API allows partners to compare their copies of interinstitutional Erasmus+ mobility agreements with each other.		✓				EWP consortium
Interinstitutional Agreements Approval API	This API allows HEIs to approve agreements sent by their partners in the Interinstitutional Agreements API.				✓		EWP consortium
ELM	European Learning Model	✓		✓		✓	DG EMPL
Openbadges	Project maintains the specification of digital badges packaging information of skills and achievements that can be issued, presented, and verified.	✓		✓		✓	EWP consortium on behalf of DG EAC

2.5.2 Services and tools

This section provides a table listing the main inter-institutional networks (e.g. Europe-wide, national, regional, alliance-wide), services, software, federations, platforms, etc. that institutions (or alliances) can connect to for data exchange or aggregation. It includes both open and commercial options that are of minimum relevance for this use case.

A complete list of identified services and tools could be found in Annex I – Inventory of tools and services.

Name	Information	Offered / managed by	Openness	Standards used
EduXchange	Open-source catalogue solution adapted for international use, which implements a custom identity provider. This centralised catalogue is filled with information from the local course databases via SURFeduhub using the OOAPI standard.	SURF	Existing deployments for NL & alliance, but reusable as open source	OOAPI, MyAcademicID

EWP	Erasmus Without Papers is a network for exchanging data related to Erasmus+ student mobility. It is based on a collection of standardised APIs that are implemented by HEIs individually, through third party-systems integrating EWP APIs or the EWP Dashboard, and a central registry service.	EUF for DG EAC	Open access	EWP Courses API
CampusNet	CampusNet is a campus management system designed to support administrative, academic, and organisational processes within higher education institutions. It provides tools to manage student data, course scheduling, grades, examinations, and various communication channels between students, faculty, and administrative staff.	Datenlotsen Informationssysteme GmbH	Neither open source nor free	No information available on standards used.
Fullfabric	It is a software solution for HEIs that supports digital transformation in admissions.	Fullfabric Ltd.	Neither open source nor free	No information available on standards used.

2.6 Analysis

Alliances have identified that a significant challenge lies in implementing a centralised or global catalogue Alliances have identified a significant challenge in linking course catalogues (see use case 1 - Discovery) to applications and recognising credentials, as the recognition process is closely linked to application. Ensuring compatibility between catalogues, curriculums, and application forms is problematic due to differing data models.

To address these gaps, alliances have implemented forms that allow students to apply for courses listed in the catalogues. Other alliances have adopted integrated systems that automate processes and fully digitise operations. However, as indicated in the table above, no tool currently offers a validation service as described in this use case. Regarding the agreement broker service, we adhere to the Erasmus Without Paper initiative's philosophy. For that reason, we have defined interactions between the different components to facilitate connection to the Erasmus Without Paper project.

Moreover, the compliance check for requirements appears to be another significant gap. In the current landscape of solutions, this process is typically managed outside system interfaces and is often conducted manually.



PART 3

Use case 3 – Access tools

3 Use case 3 – Access tools



© 2024 Freepik

3.1 Use case definition

The ability to access tools is fundamental to learning. The 'access tools' use case is closely related to traditional IT Service Management (ITSM). As such, the use case's scope is to streamline the procurement, management, and governance of shared resources among alliance members, covering both physical and virtual resources. The use case heavily relies on use case 7 - User identity.

Work done so far has exposed that the discoverability is not a priority for alliances right now since the amount of request done is still manageable following local and manual processes. As alliances continue their interoperability journey, sharing tools; especially on joint programmes scenario, will become increasingly common. Yet, being able to expose the assets can be important for institutions and alliances focused on research as part of their institutional identity.

3.2 High-level flow

This use case focuses on mechanisms to share and get access to resources. To fully describe this use case, it is necessary to define processes related to the management of the catalogue of resources available for sharing, and the steps to discover and get access to those resources.

Scenarios described at the beginning of this document affect mostly the steps required to manage access to users with specific roles or enrolled in opportunities specifying a set of tools that should be used to complete

learning activities. Since access rights management is covered as part of use case 7 – User identity on user identities, high-level flows and reference architecture diagrams do not depict such scenarios in detail but instead refer to use case 7 – User identity. There are two main approaches, the first one being creating a central catalogue that stores metadata of the tools shared by each institution, the second one following a decentralised approach.

The central catalogue approach involves a new stakeholder, the catalogue operator, overseeing the management of the information that describes the tools. Institutions sharing resources are still in charge of managing the requests and granting access rights to end users. The peer-to-peer approach requires additional steps to make tools searchable since the discovery service must broadcast requests to every institution sharing service, collect, and merge the results before presenting them to the end user. As will be shown in the architecture subsection, each solution has strengths and weaknesses.

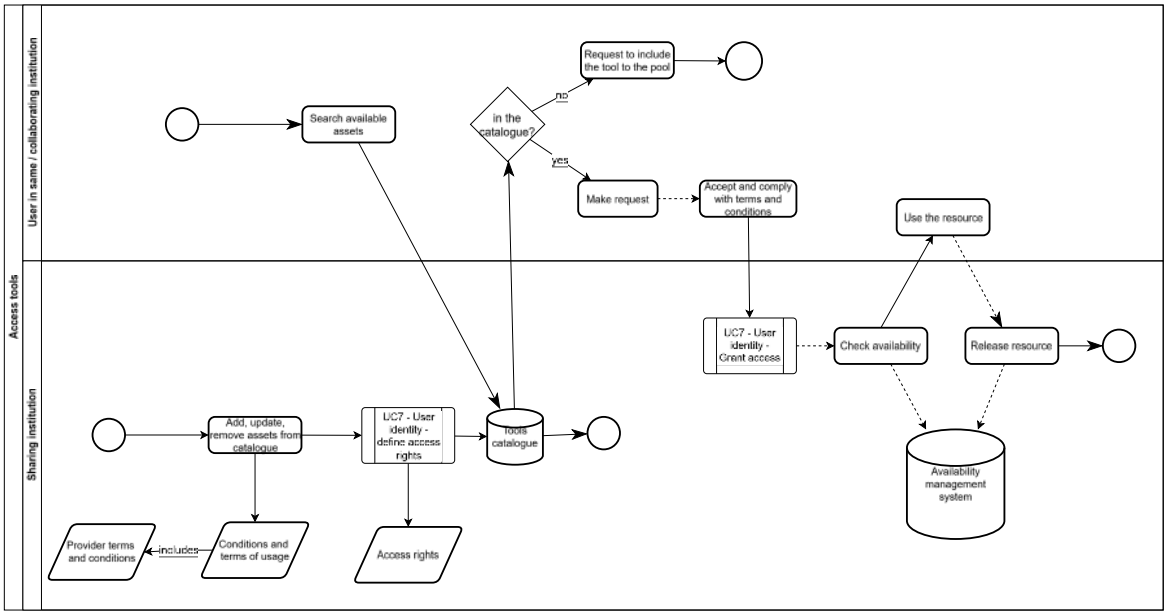


Figure 22 - Steps required to share and manage access to shared resources.
© 2025 European Union

First, steps required to make a resource available will be presented. Sharing institutions may select a subset of tools to share. Tools usually come with a license describing the terms and conditions of their use. On top of this, sharing institutions may want to incorporate access rules. Sharing a resource requires defining the set of access rights. Once the resource has been accurately described, it can be incorporated to the tools catalogue.

If the selected approach includes a central catalogue, the sharing institution will send the tool description to the catalogue for publication. Otherwise, once the tool has been included in the local catalogue, it should appear in subsequent searches.

A user looking for tools or assets makes use of the discovery service that will either broadcast the request to the local catalogues or access the central one, depending on the selected approach. This process should remain transparent to the end user. A new tool can be included in the pool through the local request process. Since this process is local to each institution and hence does not expose any interoperability challenges it is considered out of the scope for this project.

Once a user has found the tool of interest, the sharing institution oversees managing the request and granting users access to the tools. There are multiple scenarios at this point in the data flow. Some of them will require the evaluation of the individual request, for example, educators may request access to evaluate the suitability of a specific tool when designing a learning opportunity. Other scenarios may not require individual evaluation and might hence be automated. For example, software tools available to all registered users, or learning specifications and assessments, which may rely on the usage of a specific tool with a particular role. Learners enrolled in an offering associated with such specification must be granted access to the required tools. The specifics of managing user permissions and roles are described in detail in use case 7 on user identities.

Availability management and availability steps are local processes that do not require seamless communication. Yet, these steps are included in the diagram to stress that some tools may require undergoing certain local processes upon access to the resource is granted, such as quota restrictions.

3.3 Draft architecture

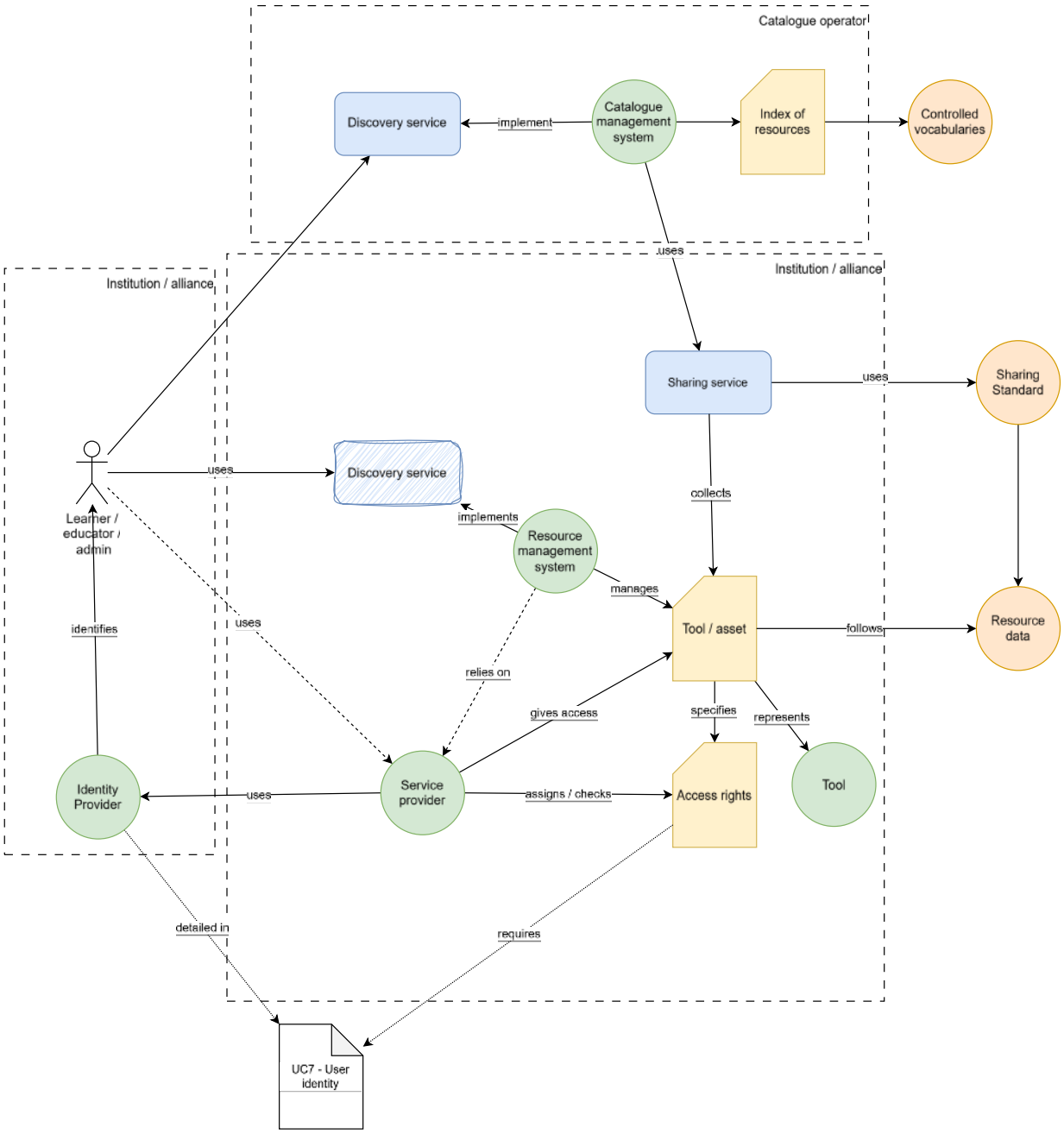


Figure 23 - Overview of components required to manage a repository of discoverable and shareable assets.
© 2025 European Union

Main components inherent to this use case are:

Data objects:

- **Tool / asset:** Describes a tool, software package, laboratory equipment or any other kind of physical or virtual asset available in an institution.
- **Access rights:** Set of permissions required to use a tool. Different users may need a different set of access rights to manage or use the tool based on their role. i.e., administrators may require specific access rights to manage requests or change configurations, students may require read only access to a tool. Details on access rights and how are they managed is described in detail in Use Case 7.
- **Index of resources:** Collection of assets ready to be shared. Includes information of each tool and how to get access to such tool.

A sharing service collects data from the assets and exposes the information following the sharing standard. This process can be complicated given that certain tools include their own management systems and others rely on manual processes, leading to tailored services that rely on manual processes.

As mentioned previously, some alliances follow a centralising approach, others follow a peer-to-peer approach. Centralising information requires incorporating a central catalogue that will store standardised information. The **catalogue management system** manages an **index of available tools** and exposes a **discovery service** for search. The peer-to-peer approach requires each institution to provide a local catalogue with the discovery service. Currently there are no discovery services as such, educators work based on previous experiences and collaborations with colleagues from other institutions.

Making the request to use a tool follows a local process and thus is not included in the reference architecture. The process of granting access to an asset depends on the type of asset and its specific management system. Physical resources may require getting an access card from a desk service in the facilities of the institution, whereas virtual assets or with a digital access can leverage on the identity use case to grant access rights to the identity.

3.4 Interoperability required capabilities

To make the tools searchable, they must be described in a way that allows them to be uniquely identified. Alliances have expressed the importance of having a data standard to adhere to. Otherwise, institutions must rely on agreements stating the data model to be used. On top of the data model or standard to describe the characteristics of a tool, a sharing standard needs to be in place for users to know how to request access.

To optimise the use of tools, it would be useful to create a common inventory of tools for all the institutions in the alliance. This could, for example, avoid having an excessive number of licences for a tool compared to other cases where the quota of licences required for the expected number of uses would barely be covered. This would also be interesting from the Alliance's point of view, to make known the full potential that can be offered to researchers and learners.

3.4.1 Communication

For this use case, regarding the requirements of communications, it should be noted that, as in use case 1 - Discovery, a series of resources are being exposed to users. This implies from the side of the catalogue operator, having services exposed from which these resources can be discovered and shared securely. If the central catalogue approach is chosen, synchronisation becomes particularly important to maintain consistency in the tools available and published.

There may be tools that require a lock state to manage their use, to prevent their simultaneous use by multiple learners or educators at the same time.

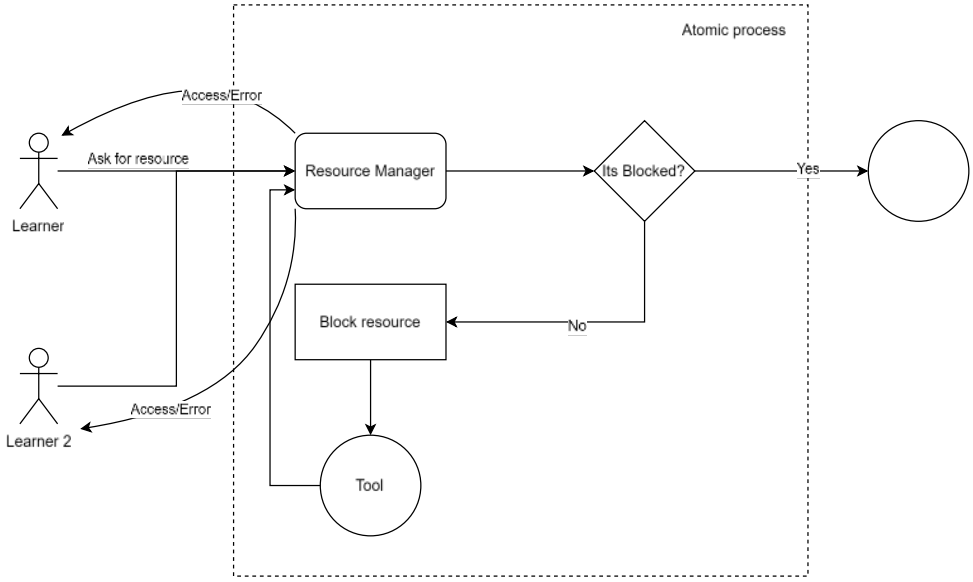


Figure 24 - Synchronization process failure leading to unexpected results.
© 2025 European Union

As the above diagram illustrates, if the state of the tools is not professionally managed, there may be a case where an unoccupied tool has a blocked state, or vice versa, a blocked tool has an unoccupied state, with the conflicts this can cause. The locking of tool states must be done atomically[13] to avoid problems related to race conditions[16] to avoid problems related to race conditions[14].

In addition to the synchronisation in terms of the exposed tools and their states, the synchronisation between the versioning of the tools must also be considered, concretely coherence between the versions of the available tools and the version necessary to be able to complete the learning activities.

Beyond synchronisation, access to the tools must be integrated with the institution or alliance's identity provider. This will ensure that users' access to the tools is correct, preventing misuse

Regardless of the chosen approach (central catalogue, peer-to-peer), a mapper must be implemented to ensure the exchange of standardised data. If the mapper is implemented as part of the catalogue operator, it must be able to transform the data from the tools received from different institutions. This implies a scalability issue that is to be considered if the central catalogue approach is chosen: Tools and institutions are integrated, hence, the number of mappings implemented must grow in parallel. In case of the peer-to-peer approach, the mapping, maintenance and updating is on the side of the sending institution, making the solution more scalable, although it requires a greater number of connections (one per institution aiming to share its tools).

3.4.2 Data protection and licensing

Shared tools could be a heterogeneous range of resources that may or may not have licensing terms. In case that the tools to be shared are not open source, license terms must be considered to avoid legal problems, e.g., with regards to misuse, reuse or publication of content generated by the tools, and others.

In case of sharing a tool that needs a personal license, the institutions should be capable to provide those for the learners and have a thorough tracking mechanism in place to facilitate learning activities and maintain oversight on implied licensing costs.

[13] Atomic action definition
[14] Race condition definition

3.4.3 Boundaries

Use case 7 (user identity)

To provide access to the required tools, validation of the learner's or educator's access rights is required. This process is tightly coupled with and detailed as part of Use case 7 – User identity. This use case prioritises providing learners seamless access to tools and equipment supplied by universities within the alliance. Therefore, tools and equipment supplied by private collaborators working with their institution is out of scope.

The learner's identity at the institution conducting the recognition must contain the necessary attributes to enable a match with the identity specified in the credential. In this regard, it is crucial that the credential contains information on the user's role to ensure that the user only has access to what he or she should have and to prevent misuse of the tools and services.

General boundaries

While procurement and negotiations are acknowledged processes, this use case does not aim to define or implement a comprehensive procurement management system. Therefore, this use case does not cover pricing or financial aspects of the use of those tools nor the negotiation processes for obtaining licences. Legal interoperability is also out of the scope.

While educators can establish usage rules for third parties' software and systems, it is not within the scope of this use case to implement these rules in a technical way.

3.5 Overview of resources in use

For this use case, it has been noted after the sessions held with the alliances that around sixty percent of the alliances use their own developed tools. In this case, there are few open-source tools registered that are being used to meet the needs of this use case. However, nearly a third of the alliances use third-party commercial tools.

3.5.1 Standards

This section includes a table that contains most used data standards, protocols, controlled vocabularies, standardised APIS or similar identified in the project, which can be implemented by tools and services.

Excludes: purely internal, unpublished standards used only by a specific tool.

Name	Information	Capabilities covered				Open standard	Owned / maintained by
		Asset provisioning	Asset discovery	Access management	Availability management		
Dublin Core	The Dublin Core vocabulary is a general-purpose metadata vocabulary for describing resources of any type. Standardised set of metadata elements for describing resources.		✓			Open source and free to use	Dublin Core Metadata Initiative (DCMI)
LTI	Learning Tools Interoperability (LTI) is a standard that enables seamless integration between learning systems and external systems. A (LMS) may use LTI to host course content and tools provided by external or third-party systems on a website without requiring a learner to log in separately on the external systems.			✓		Open source and free to use	IMS Global Learning Consortium
LOM	Learning Object Metadata is a data model used to describe a learning object and similar digital resources, used to support learning. The purpose of learning object metadata is to support the reusability of learning objects, to aid discoverability, and to facilitate their interoperability.		✓			Open source and free to use	IEEE Learning Technology Standards Committee (LTSC)
SCORM	SCORM is a set of technical standards for eLearning products. It provides the communication method and data models that allow eLearning content and LMSs to work together.	✓				Open source and free to use	Rustici software

3.5.2 Services and tools

In the following table there are the most identified prominent tools, for the complete list of related tools check the first annex.

Name	Information	Offered / managed by	Openness	Standards used
BLOOM Hub	Digital infrastructure to link local software of universities.	OpenU project	Free to use and open source	LTI
Edu-sharing	Edu-sharing is an open-source platform designed to facilitate the management, sharing, and collaborative creation of educational content.	German Research Foundation	Neither open source nor free	No information available on standards used.

3.6 Analysis

As becomes clear from the table above, the mapping analysis has led to only a small number of commercial solutions in use by alliances. These solutions focus on the catalogue operator side, less focus is put on the discovery service of the resource management systems.

Some of these solutions offer a consistent catalogue management system focused on interconnecting systems. This is a huge advantage as it is a step further and makes alliances closer to achieve interoperability.



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

© 2024 Freepik

4.1 Use case definition

It is paramount that educational resources can be easily presented on various platforms. Therefore, it is valuable to decouple the resource from the platform. Thus, this use case focuses on the ability to (co-) create a resource, and then the capability to access and share these educational materials. This bolsters collaborative and accessible educational environments. A typical learning management system often has the capability to create, import, and/or export educational resources, while also allowing for modification, deletion, and reuse.

TTo facilitate continuous improvement, resources should be editable by authorised users, enabling updates or adaptations to specific needs or changing curricula. Additionally, resources should be reusable and adaptable for different educational contexts, preserving pedagogical value while allowing flexibility. When resources are no longer relevant, they should be easily erasable, with proper archiving options when needed.

4.2 High-level flow

This use case builds on Use case 3 – Access tools. Educational resources are designed to be used with a specific tool. Educators or learners co-creating content select the tool before creating the content. The specific steps required to create content are not depicted in the high-level flow, since they can differ between institutions.

Once the educational resource has been created, it must be classified and characterised through metadata to make it searchable. Controlled vocabularies and sharing standards play a key role in this process. Educational resources registries, referred as content pools in the diagrams, use a specific data model and potentially store data created long time ago following different methodologies to classify and characterise educational resources. This exposes an interoperability issue, since harmonising existing methodologies might be complicated.

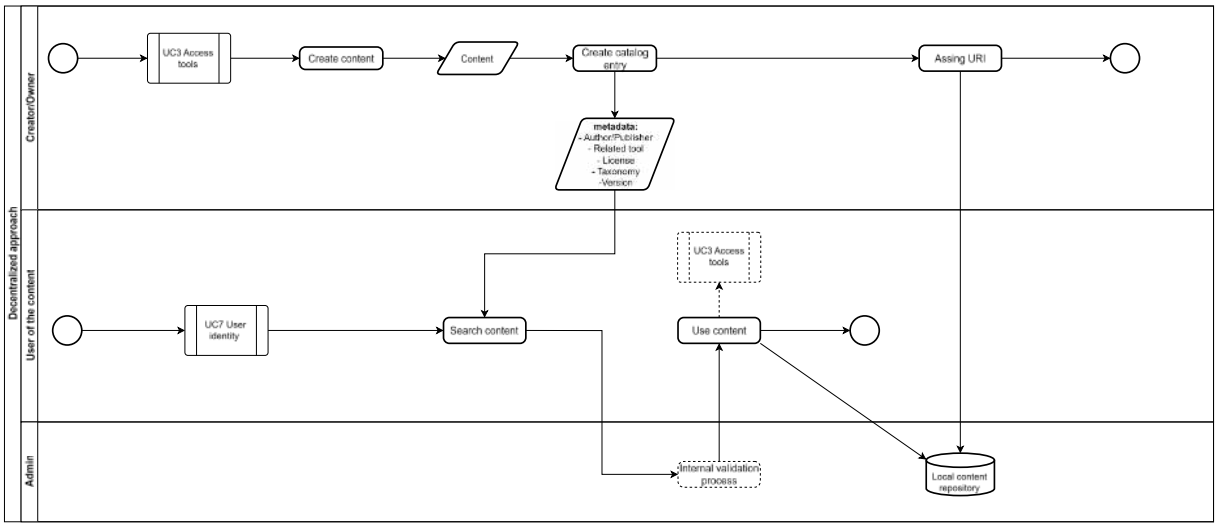


Figure 25 - Overview of the steps required to share and discover educational resources following a decentralized approach.
© 2025 European Union

If the alliance follows the decentralised approach, the process of sharing educational resources starts once the catalogue entry has been created and the content has been incorporated into the registry. This approach adds complexity to the discovery phase: Either users must collect information from different systems or alliances must create a discovery service that collects and harmonises information prior to presenting it to the user. After searching for the content, the user's request to use the content will go through the relevant internal processes of each institution, which will determine whether access to the resource is granted.

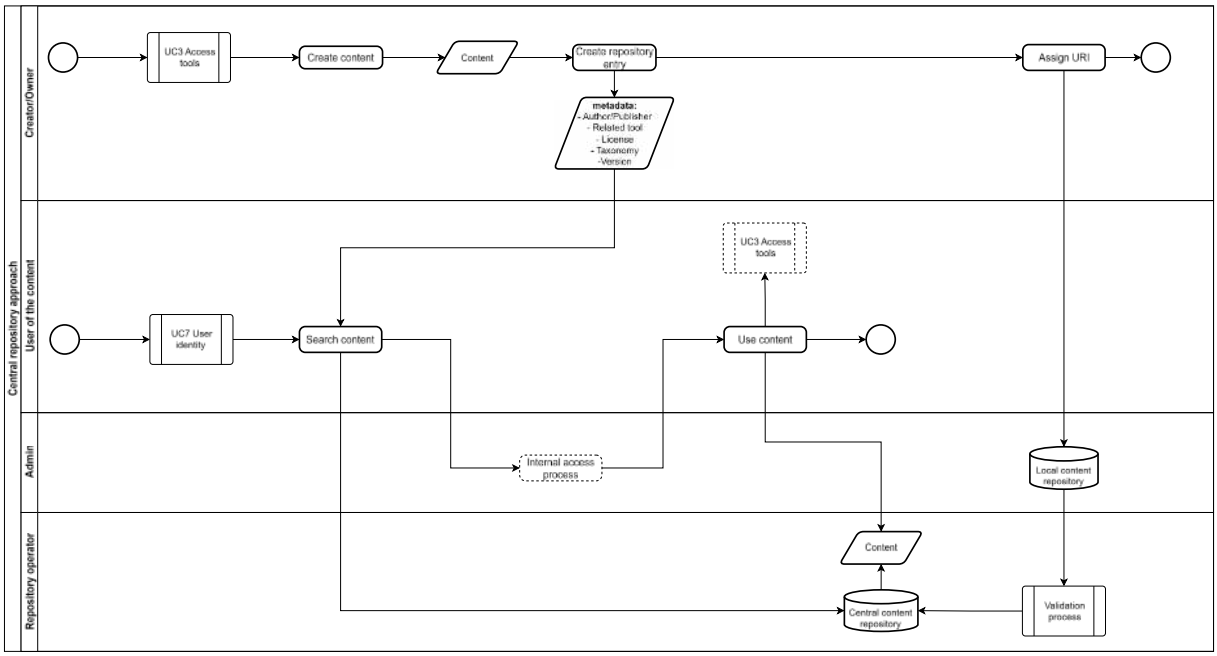


Figure 26 - Overview of the steps required to share educational resources following the central catalogue approach.
© 2025 European Union

Institutions following the central catalogue approach must publish educational resources to the central catalogue. This step requires translating from the local model to the shared standard vocabularies.

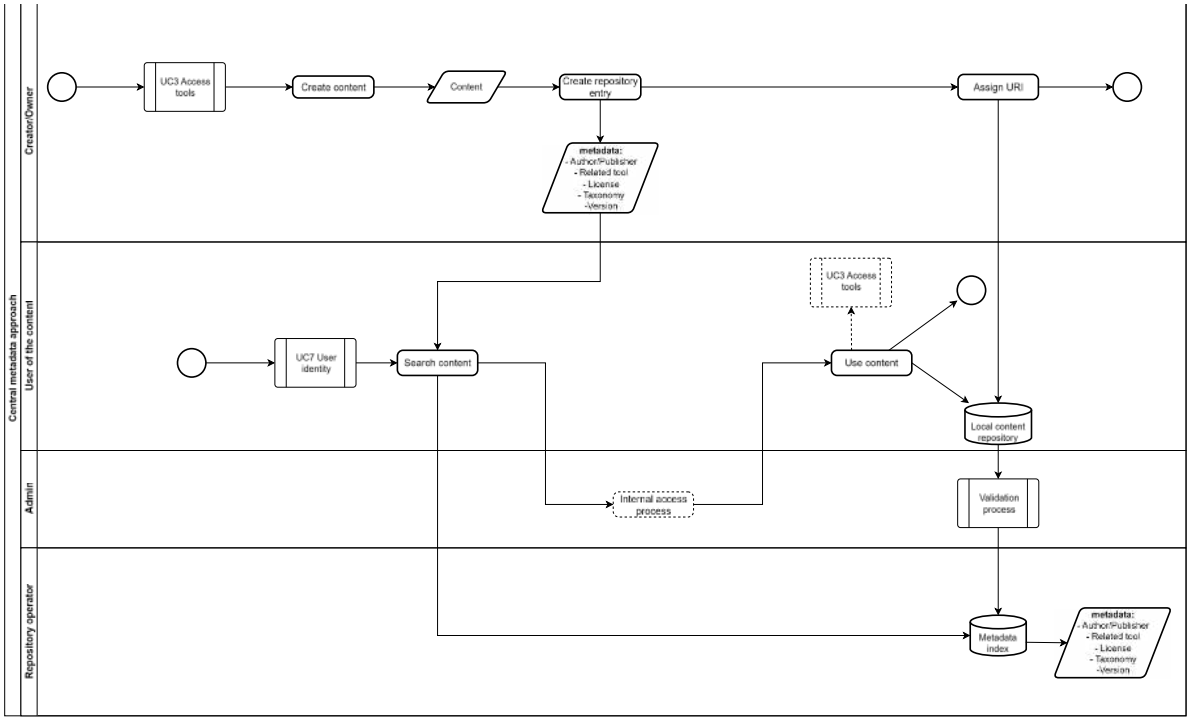


Figure 27 - Overview of the steps required to share and discover educational resources following a decentralised metadata approach.
© 2025 European Union

Another approach that emerged from the central repository during the working sessions of squad 4, is the central metadata repository approach. This central repository will only store the metadata of the educational resources, thereby reducing the storage capacities required for this system, among other benefits. Additionally, this approach is highly compatible with the internal data protection and licensing policies of each institution. By storing only the metadata, the original resource never leaves the local repositories of the institutions. Thus, when a user of the content tries to access a resource after searching for it, the request goes through an internal process within the relevant institution, which grants or denies access.

4.3 Draft architecture

Educators design educational resources for the learning specification in which they are involved. Those educational resources are stored in a registry and discoverable by other educators or learners. To fulfil this use case, the following main components are required:

Data objects and data standards:

- **Educational resource:** Represents any kind of educational material. Includes metadata attributes to fully characterise and classify the resource.
- **Shared index of educational resources:** An index of educational resources.
- **Educational resource standard:** A data standard specifying the attributes and controlled vocabularies used to represent educational resources.

Services and systems:

- **Mapping services** oversee translating from local registry data models to the educational resource standard.
- **Sharing service:** Exposes information from a local registry. Use the mapping service to translate data before exposing it. Depending on the selected approach can play an active role sending the information to a catalogue or collecting data in real time responding to external requests.
- **Validation service:** Checks that information received complies with the data standard and minimum set of required attributes.
- **Search service:** Exposes search capabilities to find educational resources. Relies on the index of educational resources and controlled vocabularies in place to make resources searchable.

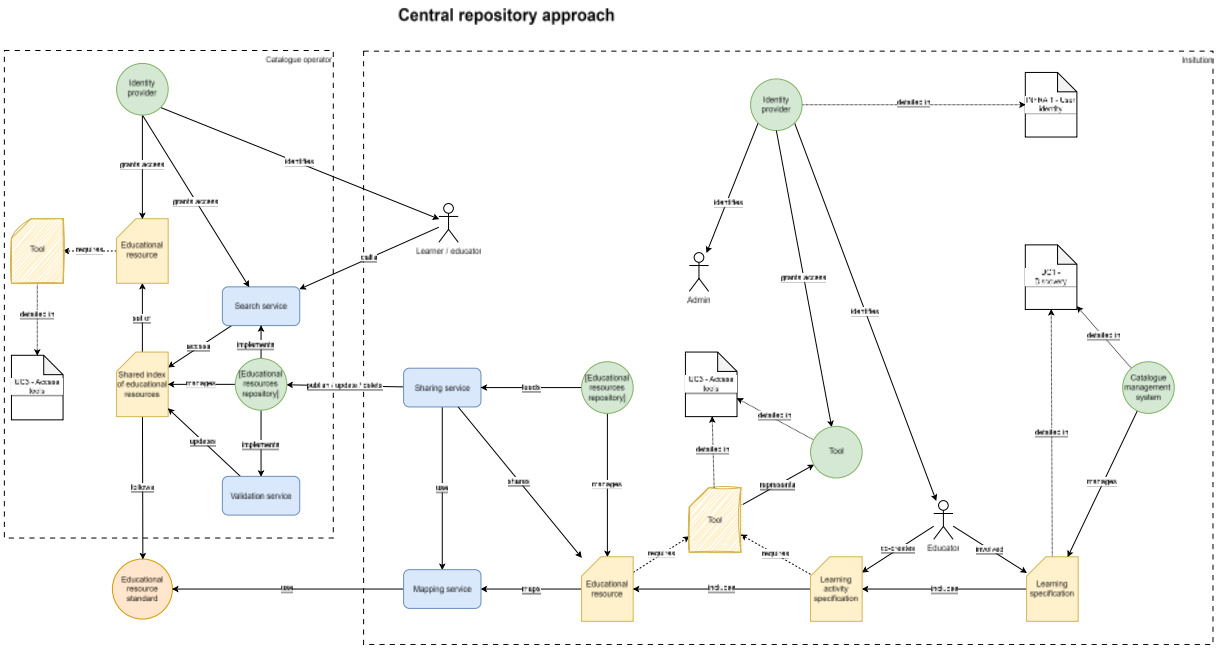


Figure 28 - Main components required to exchange educational resources with a central registry.
© 2025 European Union

The central repositories approach, as shown in Figure 28 - Main components required to exchange educational resources with a central registry above, can be implemented in two ways. If the central repository oversees collecting information from the local repositories, the sharing service must accept the request and expose changes to the central repository. The extent to which the central repository is aware of the HEIs' local repositories sets the limits. Yet, data collection can be scheduled and be based on available infrastructure.

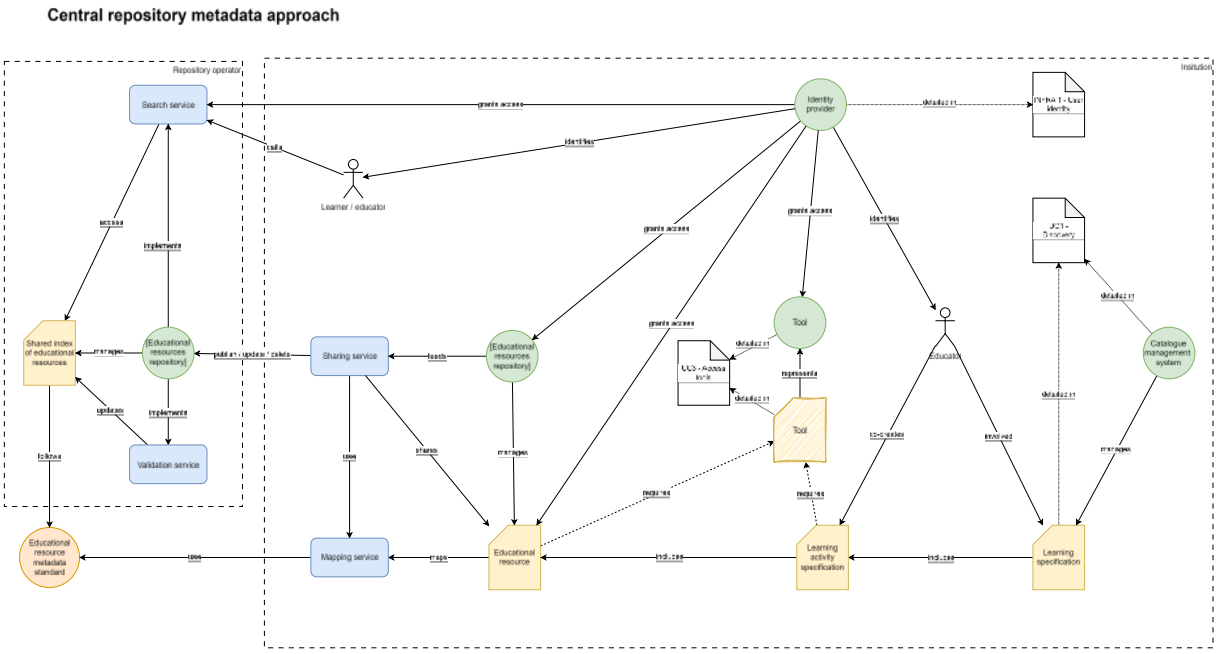


Figure 29 - Main components required to exchange educational resources with a central metadata registry.
© 2025 European Union

The difference between the diagram above and the central repository approach diagram is the management of access to the actual resource. In this case, the identity provider of the central repository is replaced by local identity providers and their internal management of user permissions.

In comparison, decentralised repositories require the local repositories to collect and send data to the central one. This may require scaling the infrastructure of the central catalogue to ingest all the updates.

In this approach, the central repository exposes the search service used by end users.

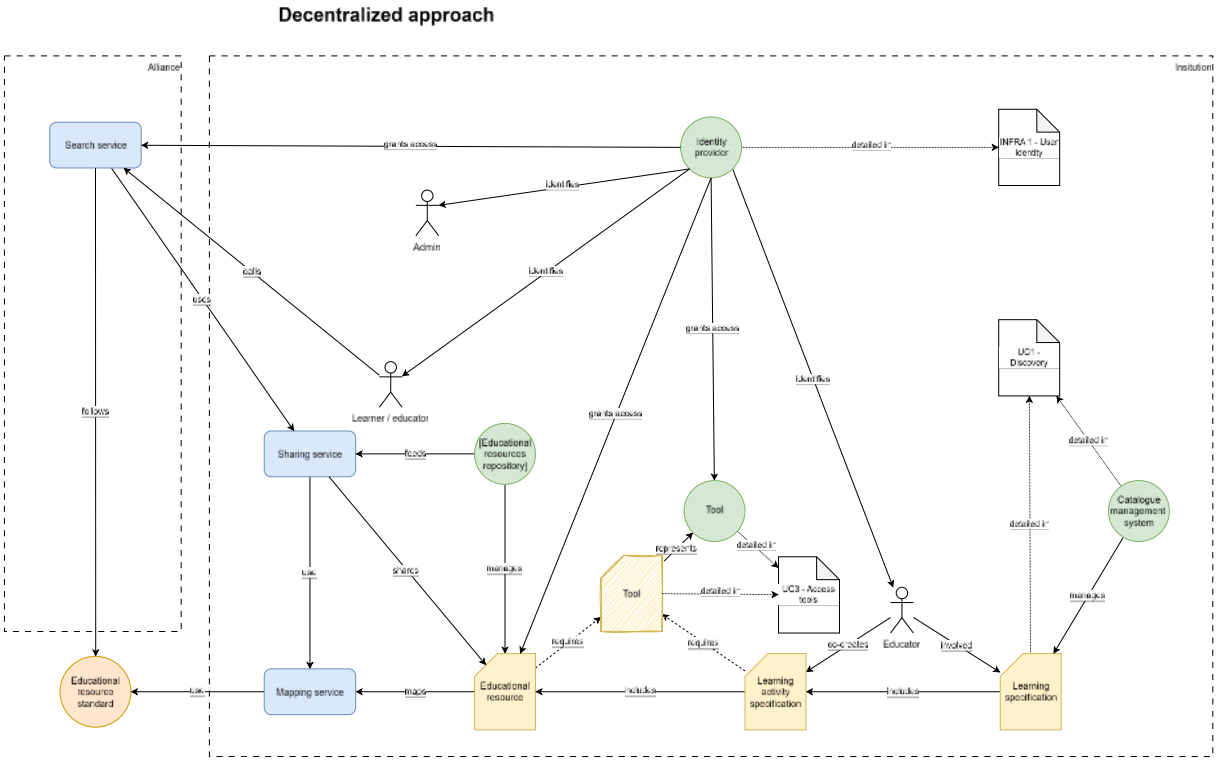


Figure 30 - Main components required to exchange educational resources following a decentralised approach.
© 2025 European Union

.

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.

IIn the decentralised approach each repository must either follow the same data standard or implement the mapping service to send data following the required structure. End users either use the search capabilities of each repository or the alliance exposes a central search service that relies on the local repositories to collect and present the data to the user.

4.4 Interoperability required capabilities

Describing contents of an educational resource is fundamental to make it discoverable. Agreeing on a shared data standard to fully describe educational resources is the first step required to share resources between institutions. Controlled vocabularies provide a solid ground to standardise terms describing contents. Terms defined in a controlled vocabulary should include a set of accepted synonyms and a clear definition. Search services require knowledge on the available attributes to build effective queries. Shared model enables search services.

4.4.1 Communication

Three approaches to interoperability within an alliance have been shown.

IIn central resource repository approach, the communication terms are similar, with the difference that not metadata but the resources themselves are shared with the central server. This implies agreeing and using a different data standard in the mapper service and therefore, sharing a more complex standardised data object. This requires the central repository to have more capacity than in the previous approach to be able to support the possible size of the data. In addition, granting access to the resources is on the side of the central repository: the resources that the end user accesses are those stored in the central repository. This eliminates the need to make extra requests to the institutions' systems. It may be necessary to agree on a mode of data access that can reconcile local internal access processes with the access provided by the central repository. Yet, this adds synchronisation and versioning problems between the data stored in the central repository and the local ones of the institutions. As for scaling and resource collection, it is identical to the previous approach.

In the second approach, the communications established between the institutions and the central repository of educational resources are carried out to share the metadata linked to the resources themselves. To make this possible, there should be a service that actively exposes the metadata of the resources generated in the institution. This service needs to be securely connected with the central resource repository. On the side of the central server, it must enable communications with this service to receive the metadata. In case this service is not implemented by an alliance, the central repository must be aware of the alliances concerned. Through a harvester type service, this will allow collection of the required metadata from different repositories of the institutions. In any case, communications between these components should always be secure.

Due to the possible increasing number of institutions, the central repository must be able to scale its capacity, both to absorb search requests and to store the metadata of the generated resources. This scalability can be carried out on demand or by planning in advance the increase in resources after agreeing to the entry of a new institution. This type of scaling can be done in a simpler manner if cloud technologies are used, as it does not require the acquisition of physical elements with the delay and costs that this may entail. In this approach, by storing only the metadata of the resources, granting access to them is the responsibility of the identity providers of the institutions themselves which possess the complete resource. This process requires that the central catalogue sends metadata of the educational resource (URI should be enough) and user data (institutional attributes).

From the point of view of communications and data storage, the decentralised approach is simpler. The capabilities required in this case are limited to having an agreed standard for the data object model that represents educational resources at the alliance level, and to implementing a service that allows exposing these standardised resources at the institution level. The part external to the institutions and centralised would be limited to a search service, which must be aware of the institutions it must target to obtain the resources. This implies that with the inclusion of new institutions, the service must be updated. As is the case for the central repository approach, granting access to the resources is on the institutions themselves and their internal approval processes. The central search service must communicate securely with the services exposed by the alliances.

4.4.2 Data protection and licensing

Sharing educational resources requires mechanisms to control which resources can be shared and with whom.

The alliances have expressed their concern about GDPR, particularly regarding the intersection of data protection with intellectual property rights. While GDPR is primarily focused on the privacy and security of personal data, it also impacts how intellectual property, such as copyrights of educational resources, is managed and shared. Specifically, if resources created within an institution contain personal data or if they are protected under copyright, sharing them with external systems could create compliance issues. Therefore, establishing a clear legal framework is essential, potentially through agreements between institutions and content creators. These agreements should address both GDPR compliance and intellectual property rights, ensuring that resources are shared securely while respecting the ownership and control over the content.

In practical terms, alliances proposed having specialised repositories in place, each with a specific purpose. For example, a repository for general educational resources and another specific for research-oriented educational resources. This could simplify the management of permissions and access to resources.

4.4.3 Boundaries

Use case 7 (user identity)

To provide access to the required resources, validation of the learner's or educator's access rights is required. This process is tightly coupled with and detailed as part of Use case 7 – User identity. This use case prioritises providing learners seamless access to educational resources supplied by universities within the alliance. Therefore, interoperability between tools is outside the scope of this use case and limited to Use case 3 – Access Tools.

The learner's identity at the institution conducting the recognition must contain the necessary attributes to enable a match with the identity specified in the credential. In this regard, it is crucial that the credential contains information on the user's role to ensure that the user only has access to what he or she should have and to prevent misuse of the tools and services.

4.5 Overview of resources in use

This use case requires a system with multiple capabilities. The following tables includes an analysis of the capabilities of the identified tools/services and standards available for this use case.

4.5.1 Standards

This section includes a table that contains most used data standards, protocols, controlled vocabularies, standardised APIS or similar identified in the project, which can be implemented by tools and services.

Excludes: purely internal, unpublished standards used only by a specific tool.

Name	Information	Capabilities covered			Open standard	Owned / maintained by
		Publish educational resources	Search educational resources	Access management		
Dublin Core	The Dublin Core vocabulary is a general-purpose metadata vocabulary for describing resources of any type. Standardised set of metadata elements for describing resources.		✓		Open source and free to use	Dublin Core Metadata Initiative (DCMI)

LTI	Learning Tools Interoperability (LTI) is a standard that enables seamless integration between learning systems and external systems. A (LMS) may use LTI to host course content and tools provided by external or third-party systems on a website without requiring a learner to log in separately on the external systems.			✓	Open source and free to use	IMS Global Learning Consortium
LOM	Learning Object Metadata is a data model used to describe a learning object, and similar digital resources used to support learning. The purpose of learning object metadata is to support the reusability of learning objects, to aid discoverability, and to facilitate their interoperability,		✓		Open source and free to use	IEEE Learning Technology Standards Committee (LTSC)

4.5.2 Services and tools

In the following table there are the most identified prominent services, for the complete list of related tools check the first annex.

Name	Information	Offered / managed by	Openness	Standards used
Biblioteca do conhecimento online	Digital infrastructure to link local software of universities.	OpenU project	Free to use and open source	LTI
AZON – The Atlas of Open Science Resources	Collect, process, and share science resources in an open digital form to all interested parties.	Consortium of institutions, with the Wrocław University of Science and Technology as the leader	All resources are available openly and free of charge	WCAG 2.0 standards
Dialnet	Educational resources repository. Includes Scientific papers and research material.	Primarily managed by the Universidad de la Roja; coordinated by Fundación Dialnet	Access is free and open	No information available
EDUC8U	Recommend tailored learning pathways aligned with student's career goals and aspirations.	EDUC8 Consortium	Free application but not explicitly labeled as open source	No information available

Educast	Repository of national educational videos.	FCCN (Fundação para a Computação Científica Nacional)	Not open source; free to use for academic institutions	Educast requires user authentication via the RCTSaai Federation, which is aligned with the eduroam network and other institutional services
Open Educational Resources Platform	Repository with open educational resources and courses.	E-learning Division (Dział E-learningu) at Wrocław University of Science and Technology (Politechnika Wrocławska)	Free to use	No information available
OERSI	OERSI stands for Open Educational Resources Search Index - a search engine for free educational materials in higher education. As a central search entry point, OERSI connects OER repositories of distributed state initiatives, institutional repositories of universities and libraries, and subject-specialised repositories for OER.	Hochschulbibliothekszentrum des Landes Nordrhein-Westfalen (hbz) and the German National Library of Science and Technology (TIB)	Open source	LOM, LRMI, schema.org, Dublin Core
InvenioRDM	A research data management repository.	Managed by Invenio Software, which is a part of CERN	Open-source project and free to use	MARC21 (formally); JSON-based system supporting different metadata formats



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

© 2024 Freepik

5.1 Use case definition

This is a use case that focuses specifically on information which resides in a typical Learning Management System (LMS). The key capability is to generate, store and exchange learner data on a more granular level than earning the credential. This use case also enables to analyse meta-data on the learner journey, and thus can help improve platforms, educational resource or even give input for the creation of a new education resource.

5.2 High-level flow

Learners generate experience data as they take part in a variety of learning activities using a heterogeneous set of tools. Such activities are stored in a **learner records storage (LRS)** which can live within a learning **management system (LMS)** or as an independent system.

Regardless of the approach chosen by the institution/alliance to undertake this use case, learners can check their learning progress by collecting their own aggregated records from an LRS. Moreover, educators can collect the same records to monitor the student's progress and assess their activities. The chosen approach should be transparent to learners and educators.

There are four identified approaches for this use case, central operator, decentralised, broadcast, and central metadata operator.

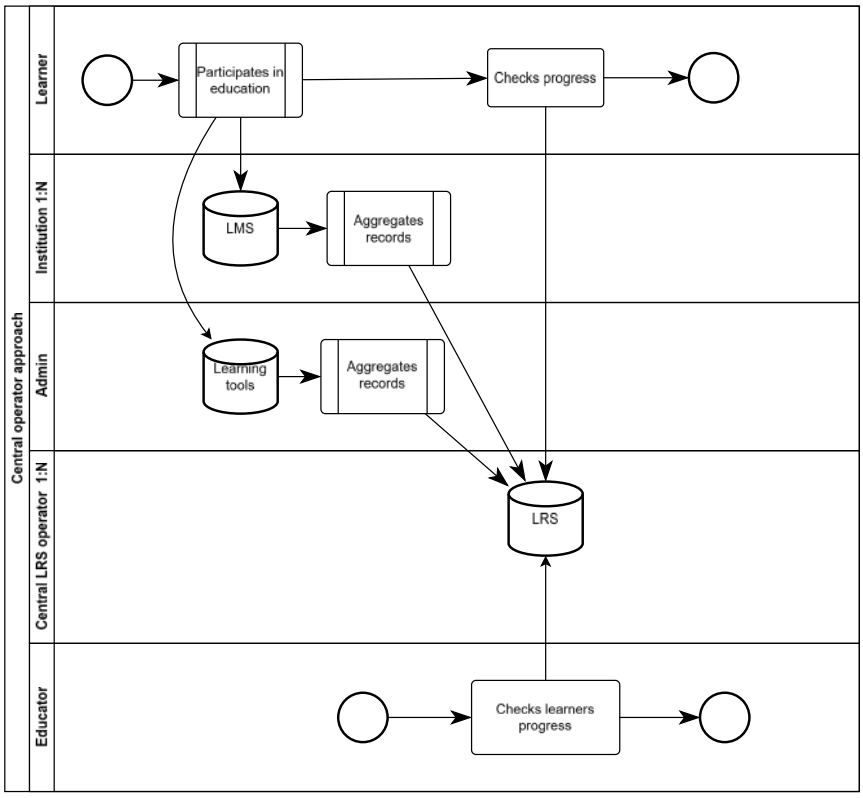


Figure 31 - Overview of the steps required to persist and search the learning records generated by learners following a central operator approach.
© 2025 European Union

The central operator approach forces the LRS to be an independent element that collects all the learning records generated by learners' interaction with 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 synchronises the data with the central LRS. This condition could be plausible due to a network connection issue or a high latency scenario.

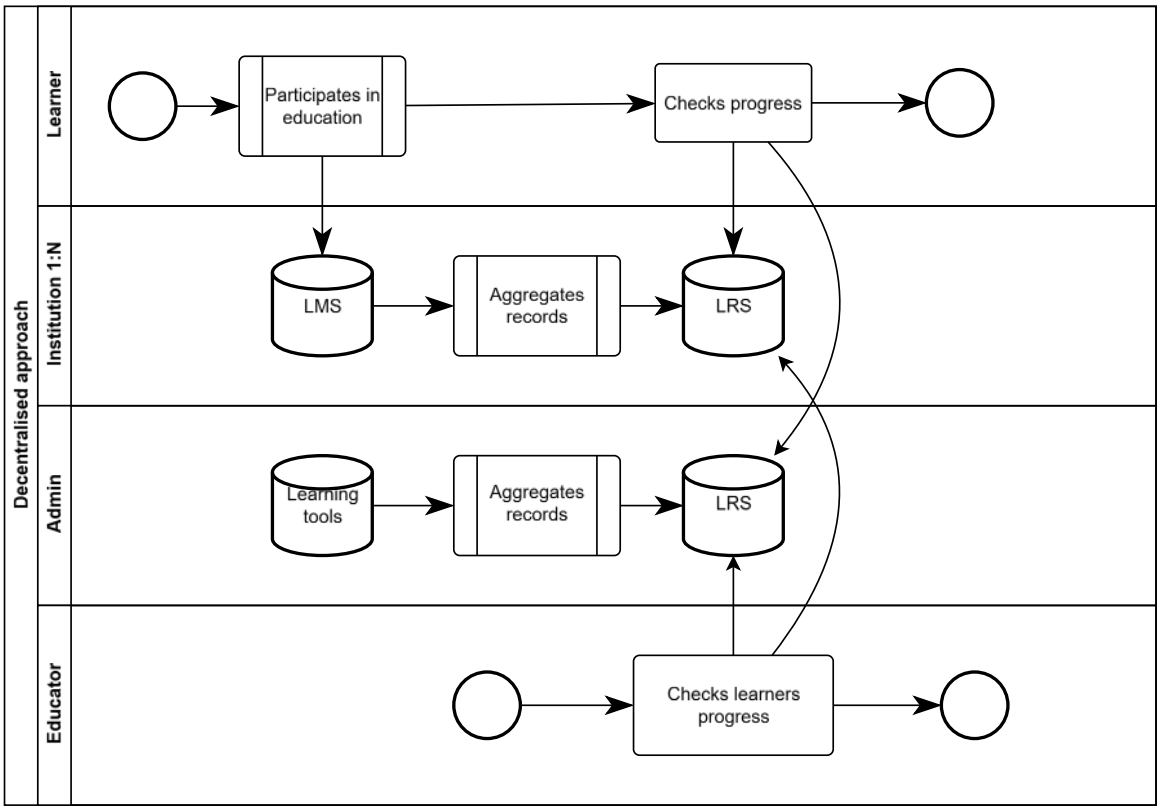


Figure 32 - Overview of the steps required to persist and search the learning records generated by learners following a decentralised approach.
© 2025 European Union

In the decentralised approach, the lack of a common LRS implies a high volume of requests between all the systems involved. This volume of requests could be problematic in terms of scalability. However, this approach avoids duplication of data as no central LRS is needed. Learners and educators should have access to all existing LRS to be able to track the learners progress stored among LMS and learning tools.

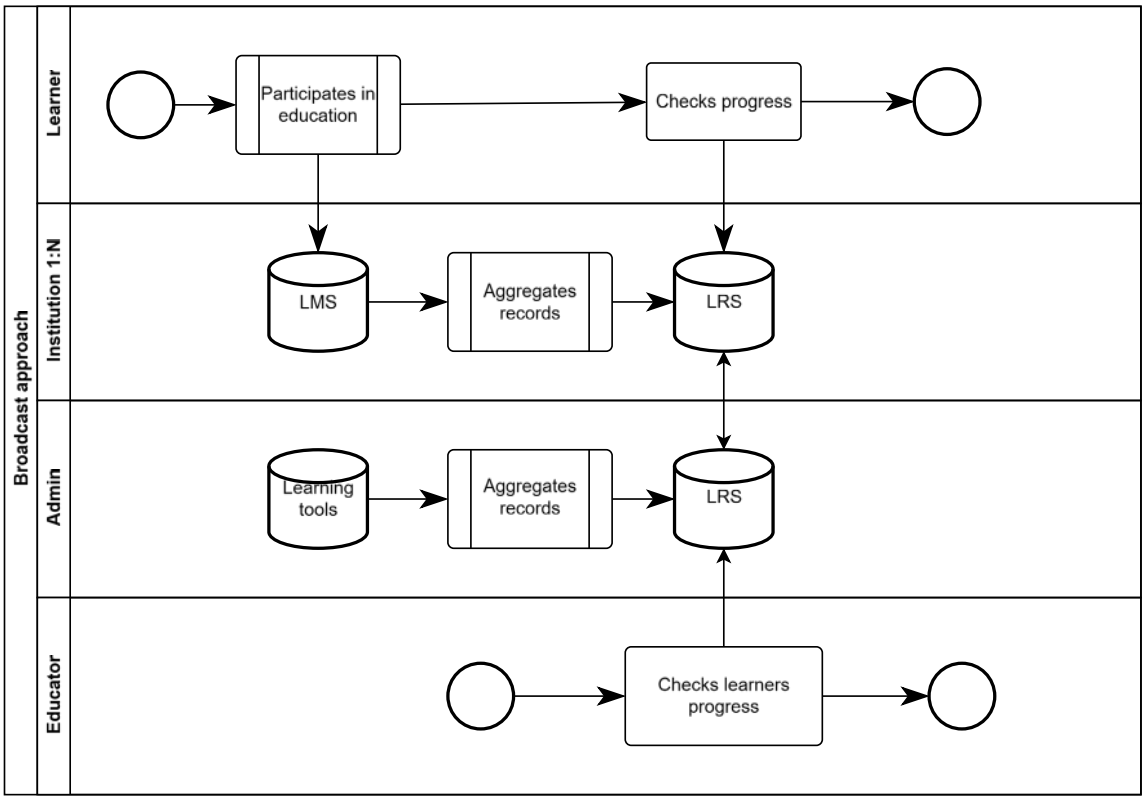


Figure 33 - Overview of the steps required to persist and search the learning records generated by learners following a broadcast approach.
© 2025 European Union

The last approach is broadcasting. This means that each LRS involved must register each other's LRS learning records. Thus, learners and educators can access their learning records from any LRS exposed. As is the case for the central operator approach, also this approach requires a duplication of learning records. In addition, a high volume of requests, as noted in the peer-to-peer approach, is seen. Nevertheless, the great strength of the broadcast approach is the data availability. Although one or more LRS may be unavailable, the learning records remain accessible due to data replication between the LRS.

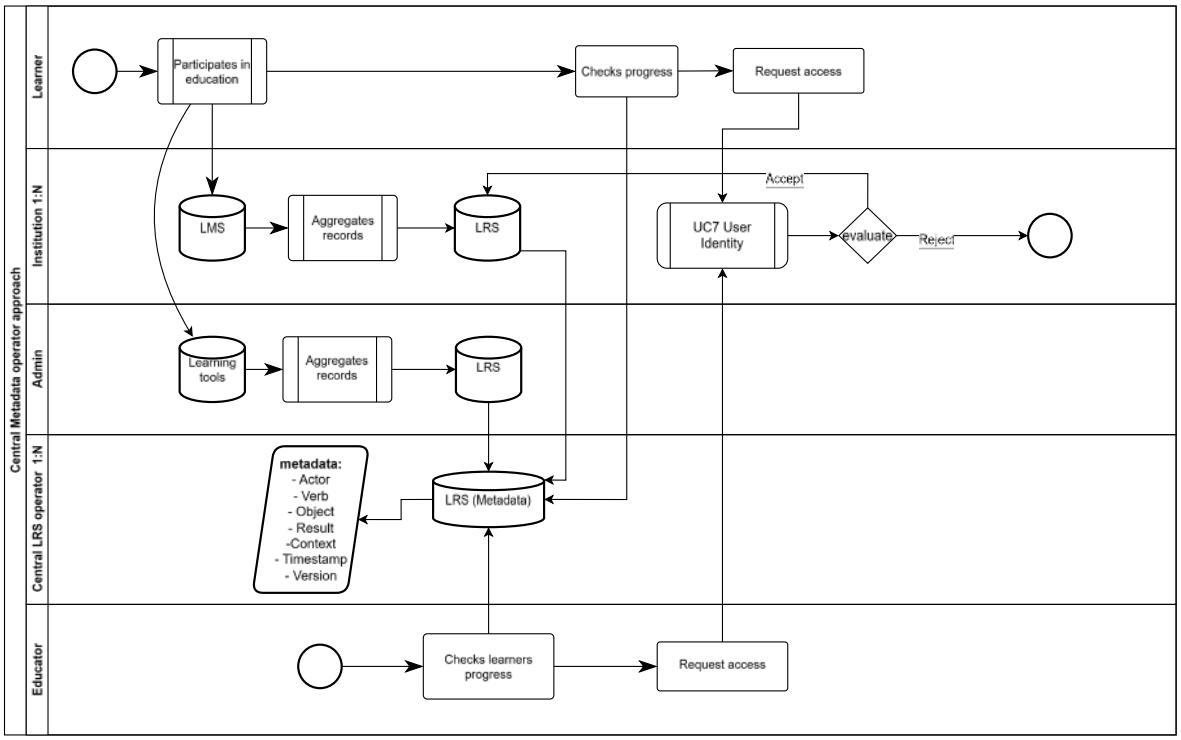


Figure 34 - Overview of the steps required to persist and search the learning records generated by learners following a central metadata operator approach.
© 2025 European Union

As seen during the working sessions in squad 4, squad 5 has identified the use of a central storage system as a metadata repository as a viable approach. Like Use Case 4 - Managing Educational Resources, this approach offers functionalities that can facilitate compliance with licensing policies, privacy, and usage restrictions by not transferring the generated resources themselves between systems.

5.3 Draft architecture

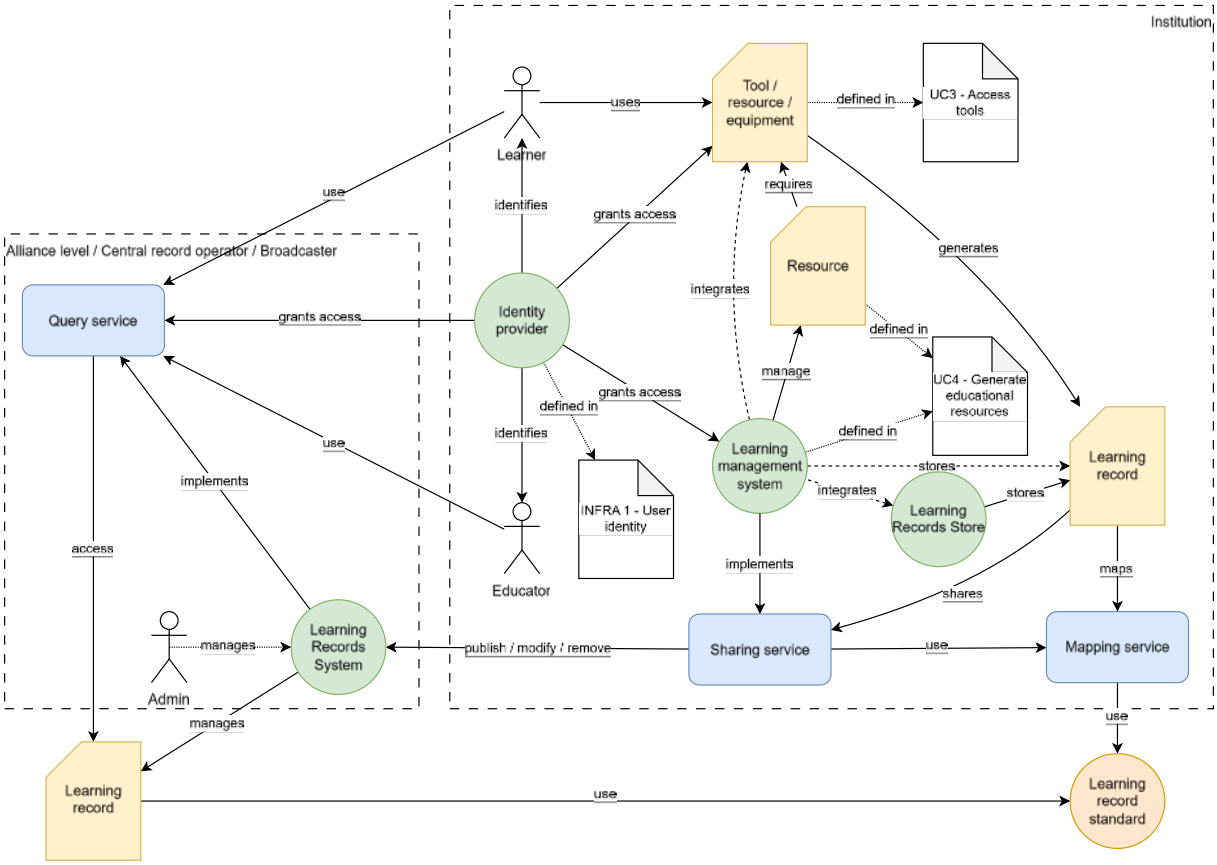


Figure 35 - Overview of main architectural components involved in generating, storing, and sharing learner records.
© 2025 European Union

Business objects:

- **Learning record:** A statement about a learning activity completed by a learner. Includes information about the actor, usually a learner, the action realised, and the result of the action.
- **Resource:** An educational resource designed as part of a learning activity. Educational resources are usually designed and created to be used with a specific tool, resource, equipment, or any other type of asset.
- **Tool:** Any type of asset available to complete a learning activity.

Services:

- **Sharing service** oversees sending local records to externals systems. Depending on the selected approach the service will expose a reading or a publishing interface. Sharing services 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 the learner activities. Depending on the selected approach this service will be implemented in a different manner. Either broadcasting queries to the different systems in a peer-to-peer approach, interacting with the local record system, or interacting with the central record system.

Systems:

- **Learning management system (LMS):** Software application for the administration and delivery of educational processes. In this particular use case, a LMS integrates information on learners' progress related to different learning activities that are part of a learning offering.
- **Learning records system (LRS):** Software application for storing and managing learning records. Learning records systems can be integrated as part of the LMS or be an independent system.

5.4 Interoperability required capabilities

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

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

5.4.1 Communication

In addition to the standardisation of the data generated by the tools, another important challenge noted by the alliances is scalability. For this use case, one of the components that most needs to support scalability is the data mapping service.

Regardless of whether only metadata or learning records as such are stored, in approaches where a central LRS is used, this part must be able to scale to support the presumed load of communications that may cause the storage of this data. It should be able to support as many requests as learning records are generated and stored.

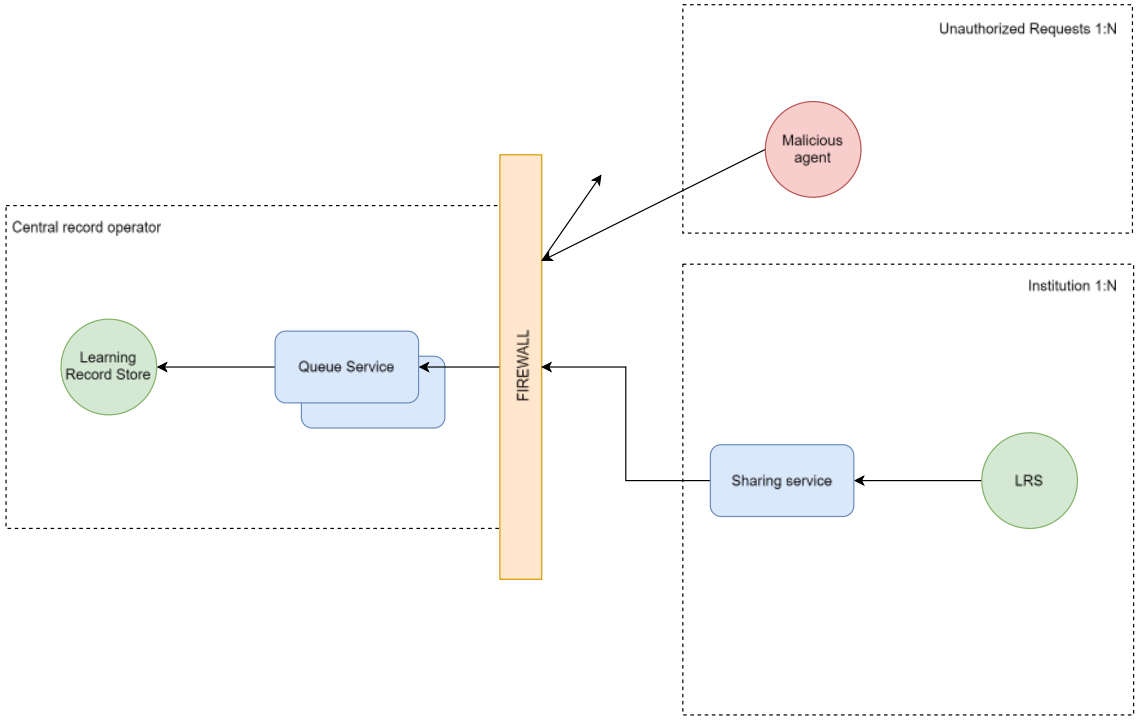


Figure 36 - Role of a strong firewall against request.
© 2025 European Union

.

The above scheme represents a solution to the possible casuistry of extremely high peaks of requests to the central LRS, and before DDoS attacks. Using strict firewall rules, it is guaranteed that only requests from the sharing services of the institutions are accepted. Then, with a scaled queue system, it allows the controlled intake of data received by all institutions, so that in the face of peaks of maximum activity, the system remains stable.

Another option to the queue system would be to perform periodic and scheduled dumps of learning records from local repositories to the central one. Although this guarantees the stability of communication, it means that there is a certain delay between the generation of a learning record and its consultation availability by the teacher/learner.

As for the decentralised approach, the alliance-level query service must be aware of all the local LRSs it needs to target. This implies at the institutional level, enabling secure communication between the exposed LRSs and the service. This service must be capable of incorporating institutions as the alliance requires it to collect their learning records. In this case, scalability falls on the side of the alliances that must expose the services that the centralised search will target.

5.4.2 Data protection and licensing

Regarding data security, all data transferred between the LRSs, and the common service are encrypted using secure protocols. In addition, it is necessary to ensure that the architecture complies with relevant regulations and regulations on data protection and privacy (GDPR). This can be relevant since in the case of opting for the centralised approach, the learning records will be stored, and this can be considered intellectual property. From the alliances, it points out that some type of consent may be needed for students to give permission for their data to travel from a local LRS of the institution to a centralised LRS.

The identity provider of each institution must provide access to the centralised search service for learning records and ensure that it provides this service with the necessary data to send back to the local LRSs sufficient information to restrict the learner's/educator's access to their respective learning records. The details of the identity provider are described in more detail in Use Case 7.

5.4.3 Boundaries

Use case 3 (access tools) and Use case 4 (manage educational resources)

Use case 5 inherently relies on the workflows defined in use cases 3 and 4. To generate learning records, the learner should first have selected an activity, which could be linked to a specific tool. Access to these activities, as well as subsequent access to the necessary tools to complete them, is outlined in use cases 3 and 4, respectively.

Use case 7 (user identity)

Once learners' learning records are generated, these can be accessed for various purposes and levels of access depending on the user profile. For instance, an educator might view an individual learning record to assess performance on a specific activity or examine a set of records to analyse overall progress across a course. Different attributes in the identity of the individual accessing these records, as well as an appropriate Level of Assurance (LoA), will be required depending on the type of query or manipulation performed on these records.

When a learner proceeds to access their own learning records, their identity representation must include the minimal necessary attributes to unequivocally link them to the record. Given that these records contain private information, a high LoA is required to confirm that it is indeed the learner, thereby safeguarding data confidentiality.

On the other hand, if an educator is accessing a learner's records, their identity must include specific attributes that not only allow for personal identification but also validate their role and the necessary level of access to interact with these records. Additionally, they must meet the required LoA to ensure that access occurs under the correct security and authorisation parameters, thereby upholding the privacy and integrity of the learner's educational data.

5.5 Overview of resources in use

This use case, being closely related to the previous two, shares tools/services and standards with them. The following tables present the main standards and tools/services identified in relation to this use case.

5.5.1 Standards

This section includes a table that contains most used data standards, protocols, standardised APIs, or similar standards identified in the project, which can be implemented by tools and services.

Excludes: purely internal, unpublished standards used only by a specific tool.

Name	Information	Capabilities covered				Open standard	Owned / maintained by
		Learning record standard	Data Exchange	SSO support	Legacy support		
xAPI	xAPI is a web service that allows for statements of experience (typically learning experiences, but they could be anything) to be delivered to and stored securely in a Learning Record Store. Includes a data standard to store and share learning records.	✓	✓			✓	Rustici software
ELMO	The ELMO XML format is the basis for the exchange of result information. Elmo is based on the CEN standard EN 15981-2011 EuroLMAI. EuroLMAI is a data model describing assessments.	✓	✓			✓	Vietsch Foundation

SCORM	SCORM is a set of technical standards for eLearning products. It provides the communication method and data models that allow eLearning content and LMSs to work together. SCORM has limitations as it does not allow recording data of learning activities taking place out of the SCORM environment.	✓	✓		✓	✓	Rustici software
Cmi5	Cmi5 enables the packaging and delivery of distributed learning resources, including both traditional courseware and content that sits outside of a web-browser.	✓	✓			✓	Advanced Distributed Learning
LTI	This standard really applies to this use case?	✓	✓	✓		✓	1EdTech
CASE	Technical specification that establishes a standard way to exchange information about academic standards, competencies, and learning outcomes across platforms and applications.	✓	✓			✓	1EdTech

5.5.2 Services and tools

This section provides a table listing the main inter-institutional networks (e.g. Europe-wide, national, regional, alliance-wide), services, software, federations, platforms, etc. that institutions (or alliances) can connect to for data exchange or aggregation. It includes both open and commercial options that are of minimum relevance for this use case.

A complete list of identified services and tools could be found in Annex I – Inventory of tools and services.

Name	Information	Offered / managed by	Openness	Standards used
SCORM Cloud	eLearning platform that allows users to test, play, and distribute SCORM-compliant courses while providing detailed reporting and integration capabilities via its API.	Rustici Software	Not open. For extensive use, various paid plans are available.	SCORM Cloud supports various eLearning standards, including SCORM, AICC, xAPI, and cmi5
Rustici Engine	Rustici Engine can be used to translate SCORM data to xAPI or cmi5 data standards.	Rustici software	Not open access, it requires a term license that includes initial and annual fees for usage, support, and maintenance.	SCORM 1.2, SCORM 2004, xAPI, cmi5, LTI 1.1, LTI 1.3, PENS and AICC

EMREX	Enables efficient exchange of student academic records and transcripts across European higher education institutions.	Vietsch Foundation	Open access	ELMO
ILIAS	It is an open-source learning management system. It has some features like course calendar, class reservation, automatic mails on application and certain actions...	EDUC8 Consortium	Free application but not explicitly labeled as open source	No information available
Moodle	Moodle is an open-source learning management system designed to provide educators, administrators, and learners with a single integrated system to create personalised learning environments.	Free Software Foundation	Open access	SCORM, LTI, LOM metadata



PART 6

Use case 6 – Earn a credential

6 Use case 6 - Earn a credential

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

© 2024 Freepik

6.1 Use case definition

The credential is all about communication with the job-market or enrolling into further learning opportunities. For the scope of this use case, it can be both digital and physical. The fundament of any credential is trust. The use case covers issuing the credential, sharing it, and verifying the credential with trust data.

6.2 High-level flow

Learners successfully completing learning activities can request issuing a credential asserting the completion and acquisition of a set of skills or learning outcomes. Credentials can be either physical, such a signed diplomas or digital, such as a signed PDF or following more mature and machine-readable technologies such as verifiable digital credentials.

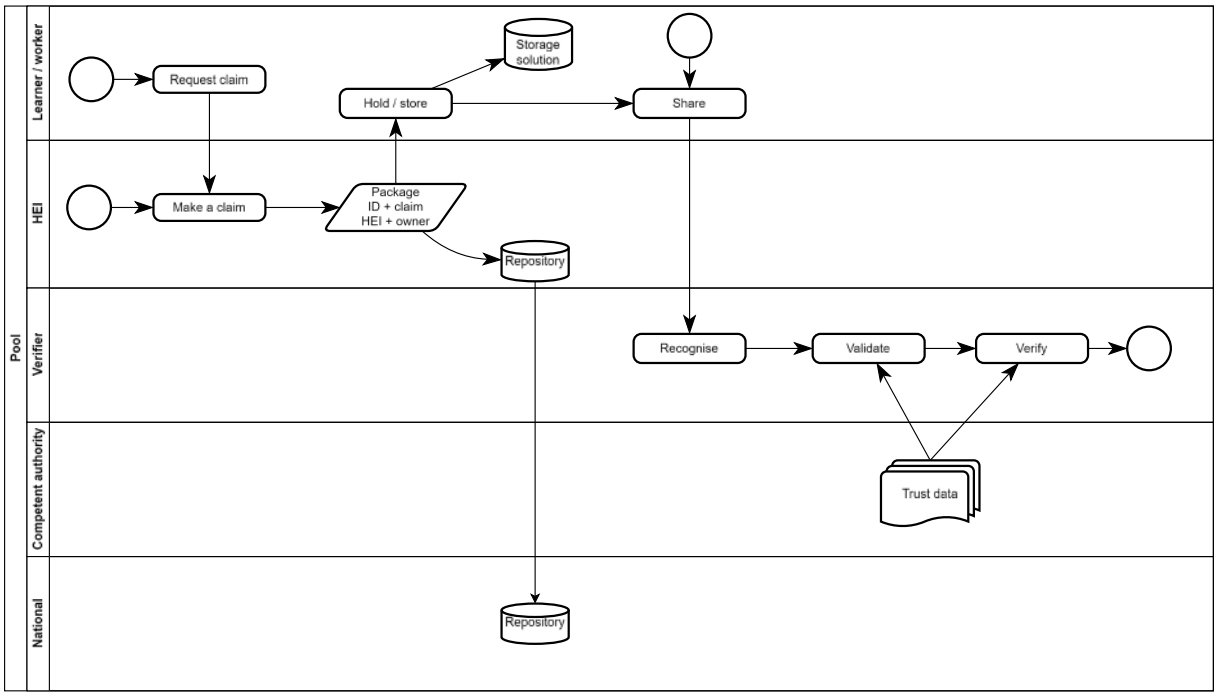


Figure 37 - Steps to issue, store, present and validate educational credentials.
© 2025 European Union

Institutions oversee generating claims incorporating, as a minimum, the set of attributes required to identify the learner getting the credential, the set of learning achievements accredited, and the set of attributes required to identify the issuing institution. The actual set of attributes and format depends on the standard or technology selected.

Issuing institution store a record of expedition for validation and verification purposes. Leaners receiving the credential store the credential in their own storage solution. Digital storage solutions are not mandatory for this data flow to work. For example, printed copies of a credential can be stored in a folder and manually managed. There are projects, such as DC4EU[15], working on standardising the processes required to store and share digital credentials or Open Badges[16] (among others) focused on providing a standard for digital credentials.

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

[15] Digital Credentials for Europe | DC4EU
[16] Home | 1EdTech Open Badges

The mandatory use of national centralised credential repositories for higher education or vocational training institutions has already been implemented in certain European countries, such as Norway and the Netherlands. Other EU countries are in the process of developing national systems as part of the European digital credential interoperability framework. For this reason, this component has been included in the high-level flow defined.

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.[17]
- **Trust data:** Data used to validate and verify a set of claims.
- **Revocation list:** This object represents 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:** Consent signed by an institution granting authority to a third party to use its signature as a certificate authority for future credentials within a joint programme's framework.

Services:

- **Credentials storage service:** Stores a copy of the issued certificates and a register of their status. Can be used to check the status of a previously issued certificate.
- **Credential issuing service:** Given a set of learning achievements and records, generates a certificate with a set of claims. Relies on the identity provider to attach information of the subject obtaining the certificate.
- **Credential sharing service:** Credentials storage solutions provide mechanisms to share previously stored credentials.
- **Credential revocation service:** Service in charge of revoking a credential, manages the revocation list.
- **Signing service:** Given a credential, this service oversees signing it with the institution signing private key.
- **Credential verification service:** Service checking the veracity of a claim. Verification processes involve getting information about the status of a claim.

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

Systems:

- **Student information system (SIS):** Manage student data, including grades and records of the student needed to issue a claim about the achievements obtained.
- **Learning record store:** Software application for storing and managing learning records. Learning records stores can be integrated as part of the LMS or be an independent system.
- **Identity provider:** An identity provider, sometimes abbreviated as IdP, is a system for creating, maintaining, and managing identity information for holders, while providing authentication services to relying party applications within a federation or distributed network[22].
- **Credentials storage solution:** System to store and manage the certificates issued to the user. Is owned by the subject receiving a credential.

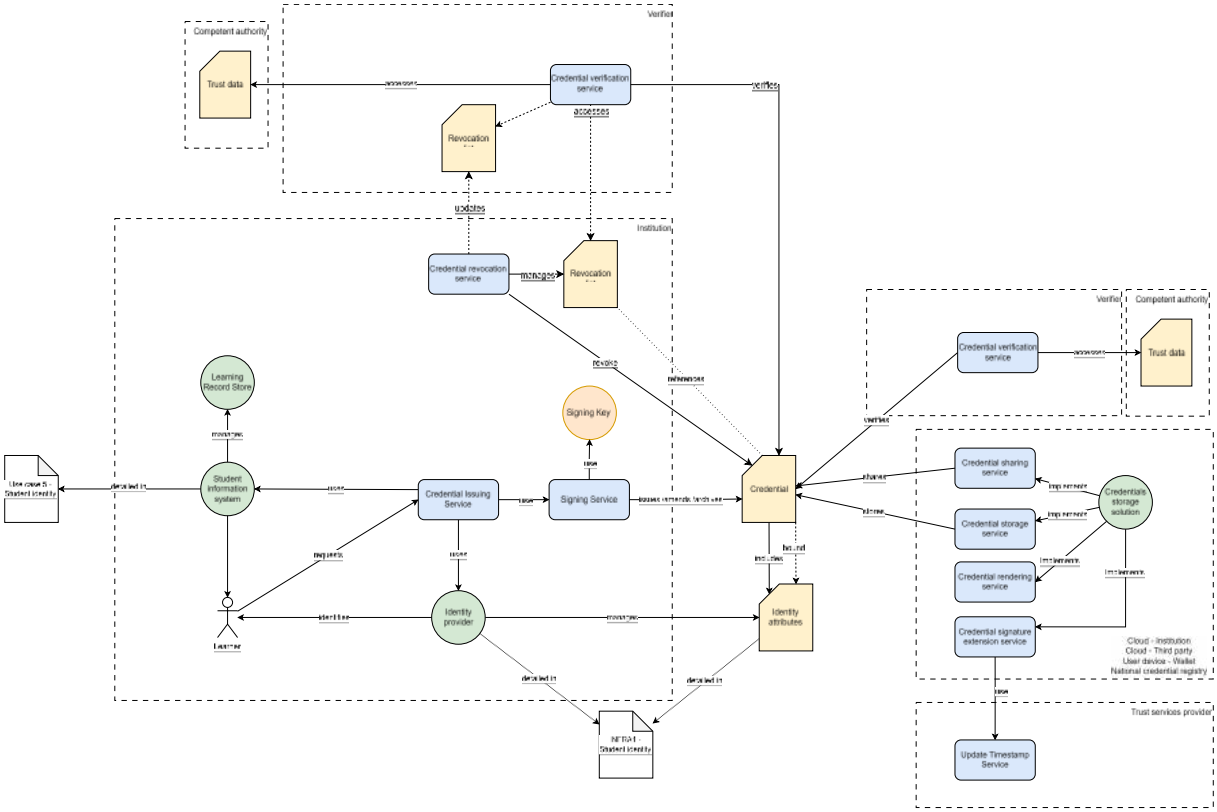


Figure 38 - Overview of components required to issue, store, share and recognize educational credentials.
© 2025 European Union

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

In the diagram above, the draft architecture is presented for the scenario where an institution is responsible for issuing a credential to a learner. This credential is signed with the institution's signing key, and the necessary identity attributes of the user are linked to it so that the credential can be recognised in the future. The credential is stored in a credential storage solution, which in this case is defined in a generic manner. Therefore, it can represent modern solutions like wallets, as well as more traditional ones, including national repositories. This storage solution will be 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, 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 approach could involve an agreement that permits the home institution, in addition to signing with its own signing key, to sign with the signing keys of the other institutions, resulting in a credential that is multi-signed by all of them. Both cases are represented in the diagram.

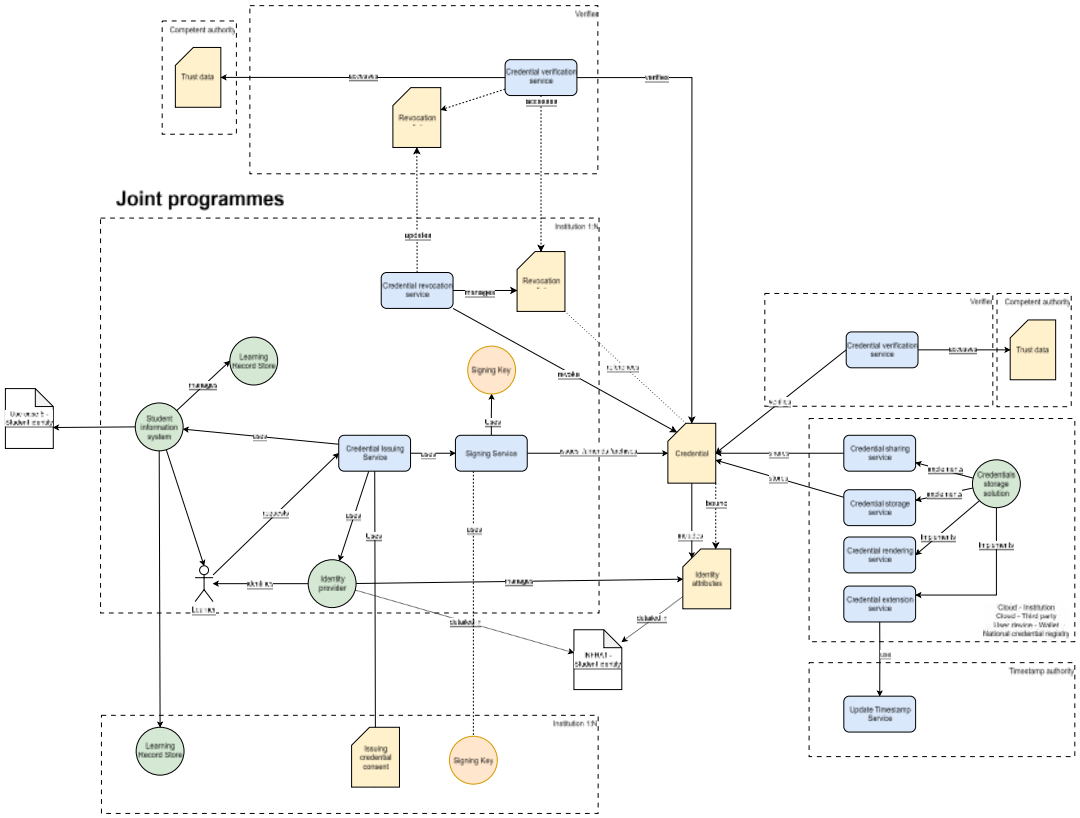


Figure 39 - Overview of components required to issue, store, share and recognize educational credentials - Joint programme.

© 2025 European Union

Finally, the following architecture diagram represents a mobility scenario outside the framework of joint programmes. To achieve a common credential in this case, during the credential creation process at the learner's home institution, the credentials issued and signed by third parties are embedded in a credential signed by the home institution itself. This process of embedding external credentials requires a sub-process of credential verification, confirming not only the validity of the credential, but also that it belongs to the learner who holds it. This entire process is reflected in the architecture of this scenario.

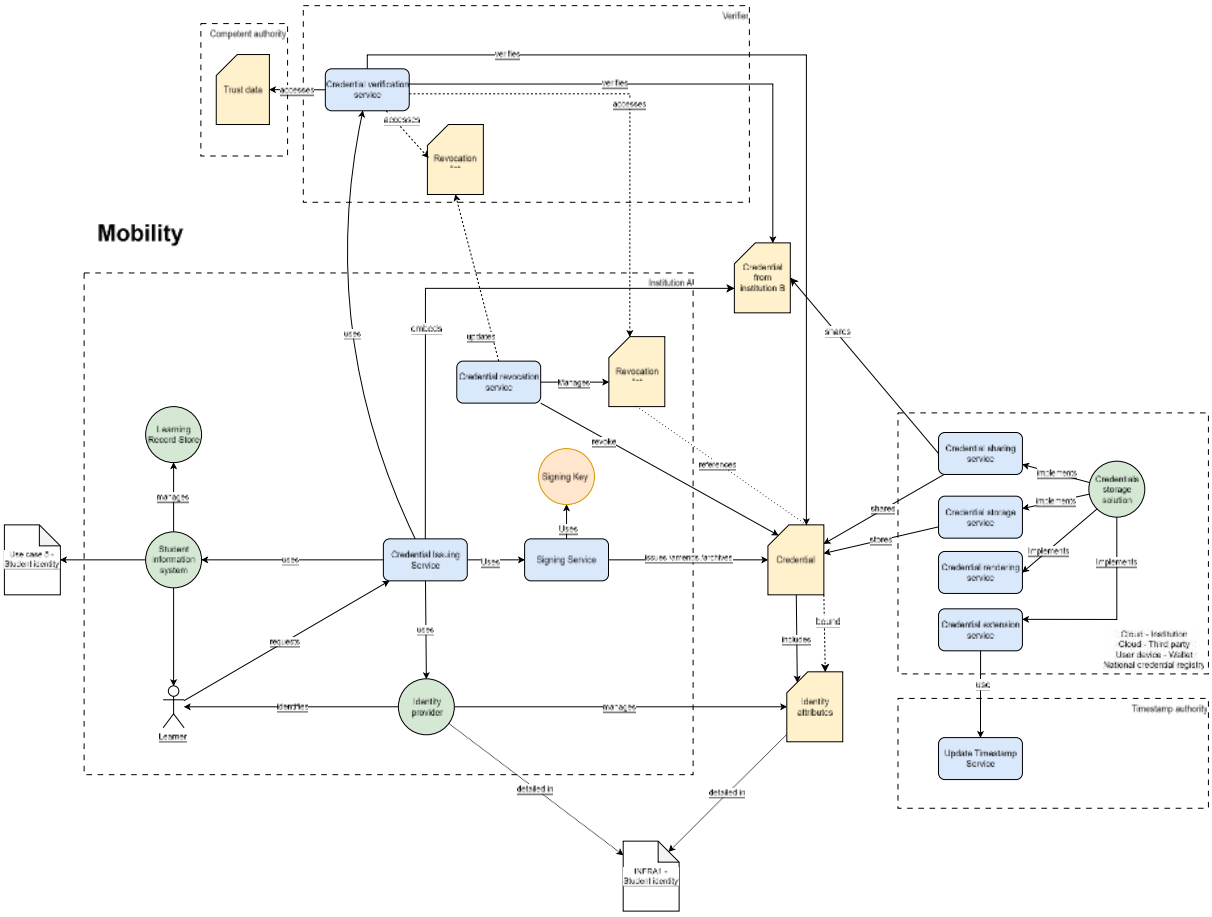


Figure 40 - Overview of components required to issue, store, share and recognise educational credentials - Mobility scenario.
© 2025 European Union

6.4 Interoperability required capabilities

The interoperability between HEIs to generate and manage student credentials involves several steps and the use of standards and technologies that ensure the validity, security, and recognition of these credentials.

Once the learner has completed a learning assessment, thus obtaining a learning achievement, they can claim a credential that includes the claims of the obtained learning achievement. For a claim to be recognised by different institutions, there must be a prior agreement that establishes standards of learning outcomes that ensure that the result of the learning achievement is as expected by all parties.

The issuing institution must collect the necessary data from the student and the achievement it is going to certify. This includes fields such as the student's name, the learning assessment completed, the results and competencies acquired, the date of issue and validity of the credential, and the identification of the institution itself. To access the student's data, the service that generates the credential must have access to the SIS. The generated credential will contain the previously described metadata and 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:** Secure storage of credentials, including both student and institution data and credential details, is a necessity. 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 unauthorised 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.

6.4.1 Boundaries

Use case 5 (generate data)

This use case is linked to use case 5, as issuing a credential to certify a learner's acquisition of skills or knowledge relies fundamentally on the prior completion of a series of activities. These activities, recorded in learning records, serve as the evidence supporting the creation of the credential. Therefore, for this use case, it is essential to have learning records that document and validate the learner's achievements, enabling the issuance of an authentic and verifiable credential.

Use case 7 (user identity)

For credential issuance, it is essential to carefully consider the identity of the user to whom the credentials are issued. This identity provides certain key attributes that will be bounded in the credential, and these attributes must be sufficient to ensure both the accurate issuance and subsequent validation of the credential. This means that the linked attributes should enable the unequivocal identification of the credential's owner, thereby supporting its authenticity and ensuring that the credential faithfully represents the achievements and competencies of the user to whom it belongs.

6.5 Overview of resources in use

The creation and validation of digital academic credentials has become critically important to support student mobility, skills recognition, and interoperability between educational institutions. Various tools, services, and standards have been developed to provide a reliable and secure infrastructure for issuing, storing, and verifying these credentials. These mechanisms align with policies on data transparency and portability, while also promoting trust and mutual recognition of academic achievements across countries and institutions.

The following tables summarise the main tools and standards implemented in Europe for managing academic credentials.

6.5.1 Standards

This section includes a table that contains most used data standards, protocols, standardised APIs, or similar standards identified in the project, which can be implemented by tools and services

Excludes: purely internal, unpublished standards used only by a specific tool.

Name	Information	Capabilities covered				Open standard	Owned / maintained by
		Learning assessment support	Completion award	Information security management	Student record maintenance		
Verifiable credentials	Standard proposed by W3C exposes mechanisms to issue, present and validate digital credentials. **Status list**[19] is another standard proposed by W3C to maintain the status of previously issued verifiable credentials.		✓	✓		✓	W3C
Openbadges	Project maintains the specification of digital badges packaging information of skills and achievements that can be issued, presented, and verified.	✓	✓			✓	1EdTech
Blockcerts	An open standard for creating, issuing, viewing, and verifying blockchain-based certificates. These digital records are registered on a blockchain, cryptographically signed, tamper-proof, and shareable.	✓	✓	✓		✓	Hyland Credentials
European Digital Credentials standards	A set of standards, services and software which allows institutions to issue, store, verify, share, and identify digital, tamper-proof credentials within the European Education Area. It allows for the identification, verification, issuing, storage, and sharing of digitally signed credentials in cross-border context.	✓	✓	✓	✓	✓	European Commission
CLR	Is the new generation of secure, verifiable learning and employment records supporting all academic and workplace recognition and achievements, including courses, competencies, skills, and employer-based achievements and milestones developed by 1EdTech.	✓	✓		✓	✓	1EdTech

[19] Bitstring Status List v1.0 (w3.org)

6.5.2 Services and tools

This section provides a table listing the main inter-institutional networks (e.g. Europe-wide, national, regional, alliance-wide), services, software, federations, platforms, etc. that institutions (or alliances) can connect to for data exchange or aggregation. It includes both open and commercial options that are of minimum relevance for this use case.

A complete list of identified services and tools could be found in Annex I – Inventory of tools and services.

Name	Information	Offered / managed by	Openness	Standards used
Europass Digital Credentials Infrastructure (EDCI)	The EDCI is an infrastructure provided by the European Commission that enables educational institutions to issue, store, and verify digital credentials. It is designed to enhance the portability and transparency of educational credentials across Europe, facilitating their recognition and use by institutions, employers, and other organisations.	European Commission	Open access	EDCI, Verified Credentials (W3C) compatible
EMREX	EMREX is a network that facilitates the transfer of academic records between higher education institutions in Europe.	EMREX Consortium	Open access	ELMO
Edubadges	Edubadges is a Dutch digital badge platform developed by SURF for the higher education sector in the Netherlands. It enables educational institutions to issue badges that certify specific achievements, skills, or competencies acquired by students.	SURF	Open access	Openbadges
EBSI	EBSI is a blockchain infrastructure developed by the European Commission and the European Blockchain Partnership (EBP) to promote interoperability and security in public digital services. In the educational sphere, EBSI facilitates the verification of digital credentials, allowing these to be issued and validated securely across the European Union.	EBP	Open access	EDCI, Verified Credentials (W3C) compatible

6.6 Analysis

There are multiple projects and standards supporting this use case, which is a good sign. The standards are advanced and general adoption has started thanks to the big 'badge' platforms from the US. Some standards are more focused on tackling the 'trust' aspect of credentials, while others focused first on the content. They have been aligning increasingly over the last years.

Although digital credential standards such as EDCI, Verifiable Credentials (W3C), and Open Badges exist, not all universities in Europe have adopted these standards, preventing full interoperability. Current systems in many universities are institution-specific or country-specific and are not always compatible with common European infrastructures.

Moreover, many universities' IT infrastructures are not yet equipped to integrate digital credential technologies or decentralised identity systems. Implementing these standards may require investment in systems, training, and organisational change management that some institutions may struggle to support. Managing digital identities for students, particularly in mobility programmes, remains a significant challenge. Systems like EBSI and MyAcademicID aim to address this issue, but adoption is uneven, with some universities lacking the identity attributes necessary to ensure authentication and authorisation on interoperable platforms.



PART 7

Use case 7 – User identity

7 Use case 7 - User identity

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

© 2024 Freepik

7.1 Use case definition

This use case is the first of two supporting use cases, meaning that interoperability in this use case is a basic prerequisite for most of the core use cases (1 – 6). The importance of this use case for many others also becomes visible in the numerous references that can be seen in the flowcharts and architecture diagrams above.

A single and interoperable user identity not only means seamless identification and access to tools and services. Such an identity also gives the learner insight in how their data is used and by who. Steps have already been taken by higher education institutions, alliances and at the European level to achieve this.

However, there is still work to be done to achieve full interoperability for learner identities across educational transitions, i.e., consistent learner identification throughout their academic journey. In this use case we aim to facilitate transferring 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 authorising users is crucial for every other use case. In the Design Thinking workshop experts discussed the concept of verified profiles. Verified profiles incorporate identity attributes of a person alongside institution-specific attributes such as the person's roles or access rights.

Verified profiles may thus include a myriad of attributes that can be shared, updated, and removed by different institutions. A verified profile extends the information managed in the student information system and can be used to create local accounts, while local authorisation processes can remain the same.

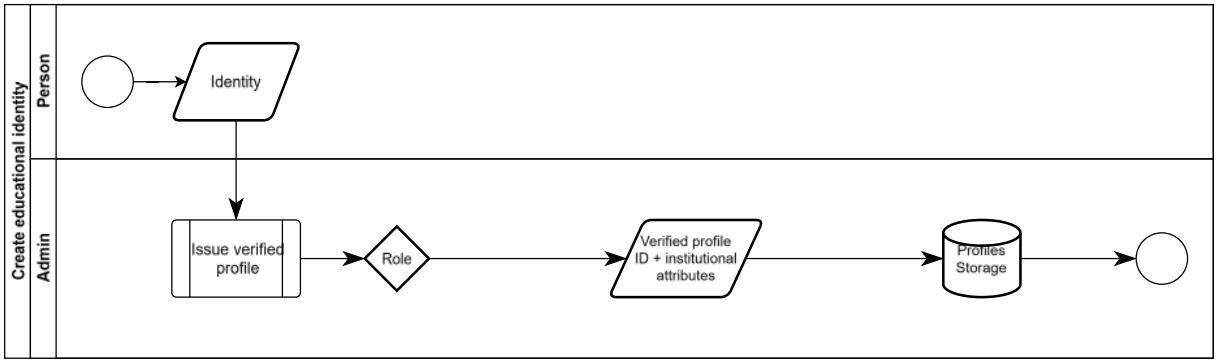


Figure 41 - Steps required to issue a verified profile based on identity attributes.
© 2025 European Union

People **joining** an institution provide their identity attributes and details required to verify their identities. With that information, their verified profile is created. Depending on their role, specific institutional attributes are incorporated into the verified profile. Institutional attributes may determine access rights required when interacting with the different systems, amongst others. Access rights can be the result of internal processes, such as being successfully enrolled in a learning offering or becoming a staff member, or as the result of being granted access to a specific tool or asset as depicted in Use case 3 – Access tools.

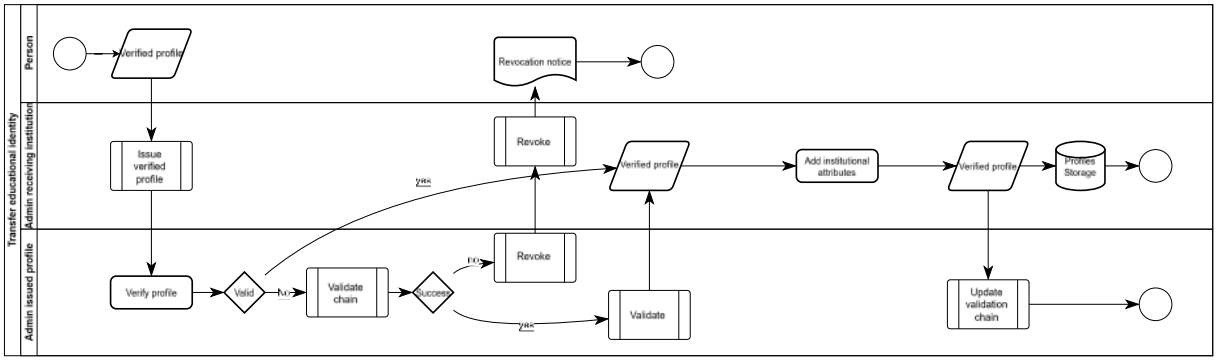


Figure 42 - Steps required to transfer a verified profile between institutions.
© 2025 European Union

People **moving** between institutions may present their existing verified profiles to get access to local systems of another institution, e.g., when using a tool that is managed/offered by another institution within their EU-A. This process relies on trust relationships between institutions. The receiving institution may accept only profiles from institutions in their trust network.

The issuing process of 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 succeeds a new record is stored in the local profiles' storage. This record will incorporate the additional local institutional attributes based on the role of the user 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 of all the profiles issued based on that verified profile. This information is later used to notify and propagate changes on the validity of the original profile. If the verification process fails, a new verified profile must be issued as described in Figure 41- Steps required to issue a verified profile based on identity attributes.

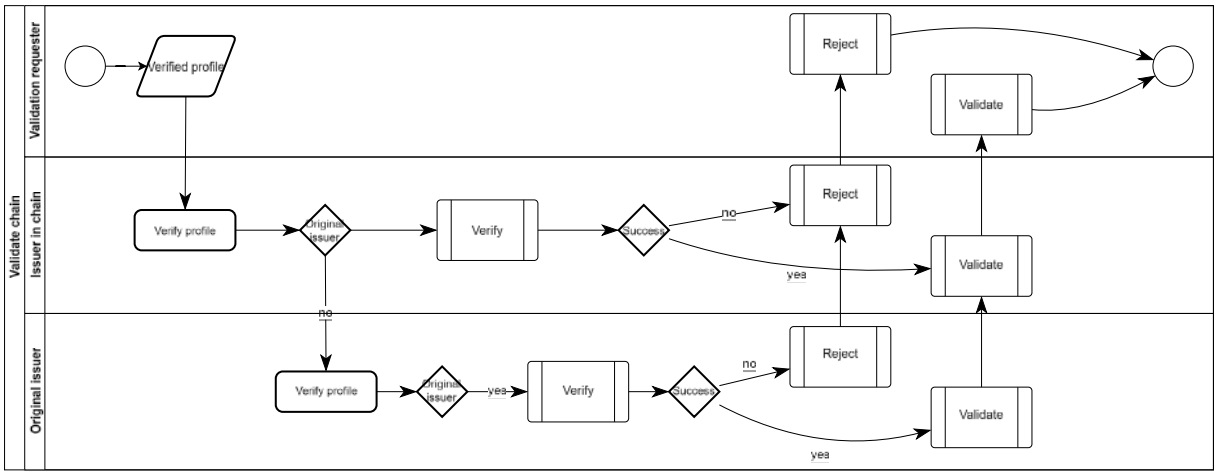


Figure 43 - Validation of an existing profile process.
© 2025 European Union

Institutions receiving a verified profile must validate it before accepting the data included on it. As exposed previously, one verified profile can be used to issue multiple local profiles, this creates a validation chain. To verify an attribute the validation chain is followed until the original issuer of the attribute is found. The original issuer checks the validity and veracity of the required attributes and either validates the data or rejects the validation request.

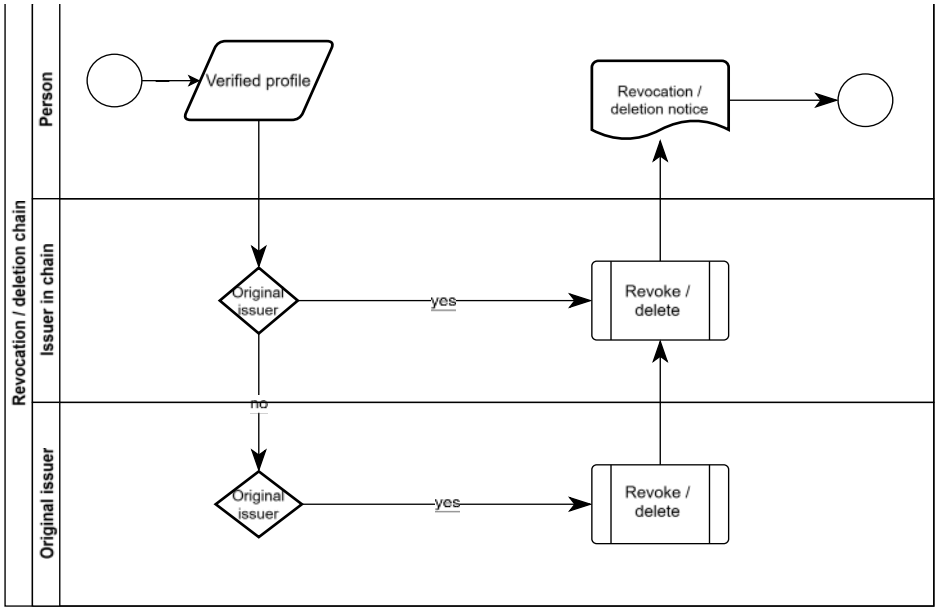


Figure 44 - Steps required to remove information from a verified profile.
© 2025 European Union

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 facilitates transferring user data required to identify, authenticate, and authorise users between institutions. It is important to differentiate the following concepts:

Business objects:

- **Identity:** Data object with the attributes needed to distinguish one person from others.
- **Verified profile:** Identity attributes of a person alongside institution specific attributes such as roles or access rights.
- **Validation chain:** Information of other verified profiles that have been issued based on attributes incorporated to the verified profile by that institution.

Services:

- **Verified profile issuing service:** Oversees creating a verified profile based either on identity attributes or attributes from an existing verified profile issued by another institution. This service implements the issuing processes depicted in Figure 41- Steps required to issue a verified profile based on identity attributes and Figure 42 - Steps required to transfer a verified profile between institutions.
- **Verified profile transfer service:** This service securely shares an existing profile with another institution.
- **Verified profile validation service:** This service implements the validation process described in Figure 43 - Validation of an existing profile process.
- **Verified profile revocation service:** This service implements the process described in Figure 44 - Steps required to remove information from a verified profile.[20]

Systems:

- **Student information system (SIS):** Student information systems manage student data, including registering students in courses, managing grades, transcripts, and student test data.[23]

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 for use case 7. After the second squad meeting, it became clear that as the diagram became more complex, it could no longer accommodate all the existing solutions and would lose even more clarity as those solutions were incorporated. In addition, since this was a foundational use case, most 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.

[20] https://library.educause.edu/topics/administrative-and-business-services/student-information-systems

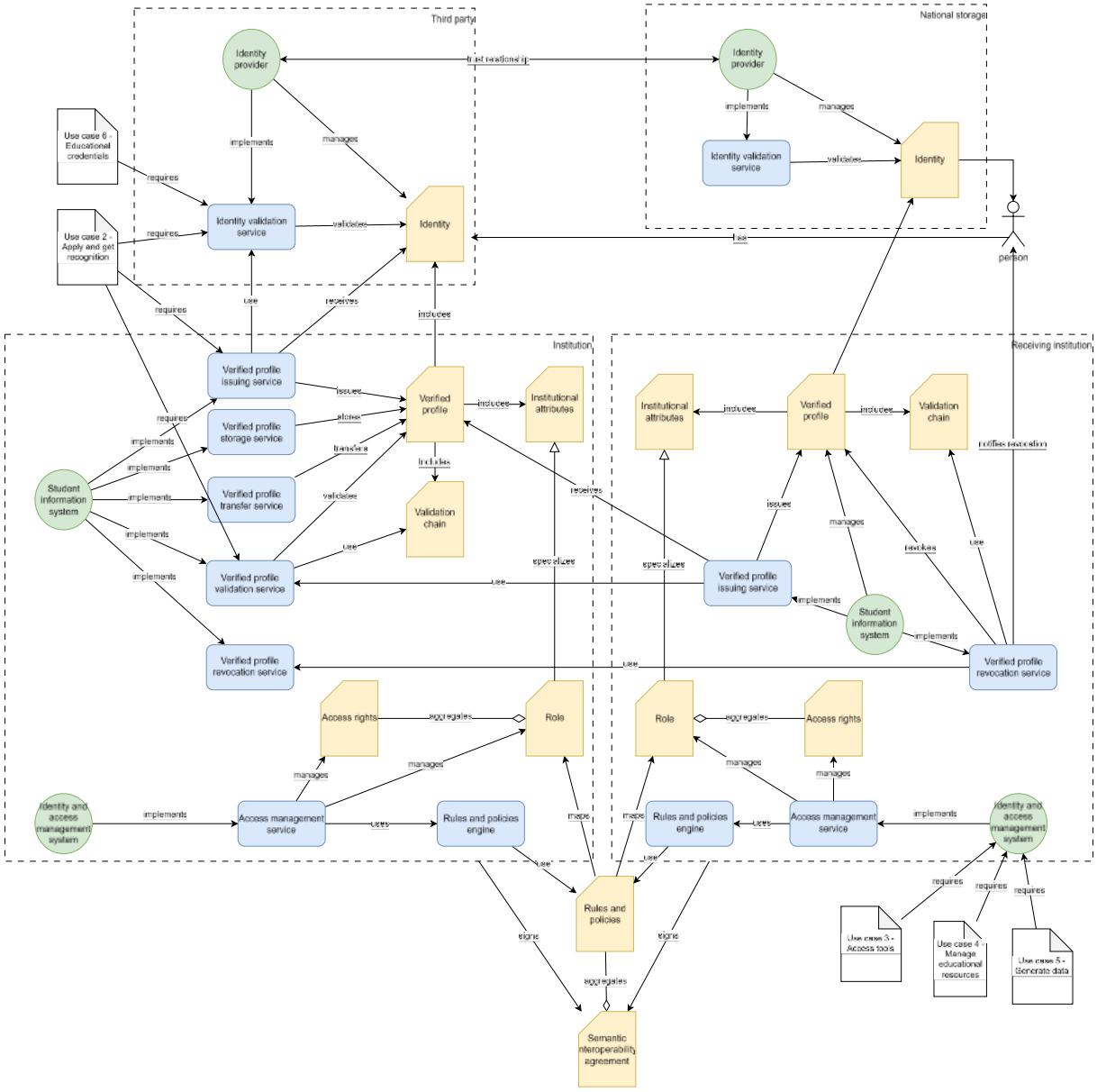


Figure 45 - Main components required to share and manage verified profiles linked to an identity.
© 2025 European Union.

7.4 Interoperability required capabilities

Approaches:

Two main approaches have been identified for this use case: centralised identities and decentralised identities. The following sections outline these approaches, differentiating the technical aspects and capabilities required for each.

The figure of the central identity provider (IdP) needs to cover a series of needs to guarantee the interoperability of identity validations among the HEIs of an alliance. The IdP must be compatible with identity standards such as SAML, OAuth or OpenID Connect, ideally adapting to those that may already be in use in the institutions of the alliance. This would facilitate the secure exchange of authentication and authorisation information, allowing HEIs to collaborate and share resources without developing specific integrations for each system.

It must have centralised identity management or identity federation and should implement a Single Sign-On (SSO) system to allow the user to access multiple services with a single authentication. Identity federation will facilitate institutional collaboration by allowing user identities to be recognised and accepted among the HEIs of the alliance, avoiding duplicate accounts. This is achieved through the establishment of trust agreements between HEIs. The central IdP must know how to redirect identification requests to the corresponding IdPs of the institutions.

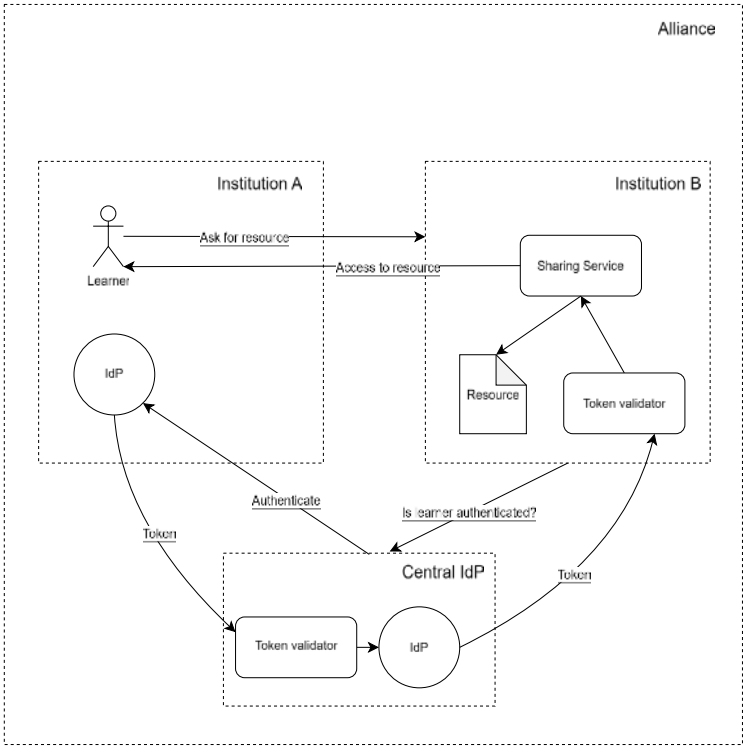


Figure 46 - Resource sharing with federated identities diagram.
© 2025 European Union

The following example flow is shown in the previous figure:

1. A learner from institution A wants to access a resource from institution B.
2. Institution B consults the alliance's IdP to see if the learner is already authenticated.
3. If not authenticated, the central IdP redirects the authentication request to the learner's institution's IdP, in this case, A.
4. The learner authenticates at institution A and then, passes a token to the central IdP.
5. The central IdP, after validating the token, issues a new one for institution B.
6. Institution B validates the received token and provides access to the requested resource.

The central IdP could integrate with existing identity directories in institutions, such as LDAP and Active Directory, be based on identity federation using SAML or other protocols, or support identity synchronisation. Maintaining the **consistency of identity data** among the HEIs ensures that users have the same appropriate permissions on all platforms.

It could be useful to have only one IdP at the alliance level. However, maintaining an IdP at the HEI level provides autonomy and local control over authentication and authorisation policies. In addition, a local IdP could serve as a backup in case the central IdP could suffer problems or service interruptions. The approach of maintaining local IdPs also helps to meet the specific requirements of each HEI in terms of the privacy of sensitive data in the face of local regulations.

Support for customised identity attributes should also be considered. Each institution may have specific needs, for example, they may have attributes related to specific academic programmes for certain users.

At the alliance level, there may be common attributes such as a global user identifier within the alliance or roles in international committees. Certain key attributes (e.g., role of student or staff, which programme a student in enrolled to, ...) need to be understood beyond the own institution to realise access policies for tools, for example (see use case 3 – Access tools).

This requires attribute interoperability, which is achieved through **attribute mapping**. The central IdP of the alliance can establish mapping schemes to translate and standardise the identity attributes it receives from the different IdPs of the HEIs. It also allows each HEI to customise and manage their own identity attributes according to their needs, while the alliance's IdP ensures interoperability at the inter-institutional level.

In terms of security and privacy, the following capabilities should be covered:

- **Data Encryption:** Protects the confidentiality and integrity of identity data during transmission and storage, complying with best security practices.
- **Regulatory Compliance:** Ensures that the IdP complies with relevant regulations and standards, such as GDPR, protecting user rights and avoiding legal penalties.
- **Incident Management:** Provides capabilities to detect, manage, and respond to security incidents, minimising the impact of potential breaches and improving the resilience of the HEI.

To increase security in user authentication processes, a desired capability of these systems is to provide Multiple Factor Authentication (MFA), thus reducing the risk of unauthorised access.

A central IdP must support a high load of communications, so it must be a **scalable** system that can manage a large number of users without degrading performance, supporting the growth of the alliance and the adoption of new services. In addition to being scalable, it must have high availability and disaster recovery. Service continuity must be ensured by minimising downtime.

On the other hand, there is the possibility of not centralising users' identities and instead using a decentralised identity. Decentralised identity is an approach that allows individuals to manage and control their digital identity autonomously, without relying on a centralised entity to store and verify their data. This can offer an advantage by reducing the risks of data security breaches, as the information is not centralised, and by facilitating mobility. For example, a student uses a decentralised identity wallet to store their academic credentials (degrees, transcripts) as verifiable credentials. When applying to different universities globally, the student shares only the necessary credentials from their wallet. Each receiving institution verifies the credentials independently, without relying on a central authority, enhancing privacy, and simplifying cross-border credential recognition.

To support the use of decentralised identities, institutions must be able to issue, validate, and revoke verifiable credentials in line with current standards (ESSIF, Verifiable credentials...). Additionally, with the advent of eIDAS 2.0, decentralised identities must meet European requirements for trust levels and regulated validation during implementation. Adopting decentralised identities may also require a reassessment of the current Level of Assurance (LoA) in processes accessed by users, with the objective of enhancing security levels.

Capabilities:

To promote interoperability from the institutions' own IdPs, they must comply with the same characteristics that have been previously discussed for the alliance-level IdP: compatibility with identity standards, implementation of SSO and use of federated identities, data encryption, and scalability and availability.

The information in a SIS about a learner is not used directly as a user identity in an IdP, but it can be integrated/linked and used to create and manage user identities in an IdP. In the proposed architecture scheme, it is seen how this piece has several services that integrate this information to form a verified profile. The functionalities that the services needed to be implemented by the SIS must cover are detailed below.
Verified Profile Issuing Service: The creation of a verified profile in a Student Information System (SIS) must be a rigorous process that ensures the accuracy and authenticity of the learner's data. First, the learner must provide all the necessary information for the creation of their profile, such as name or date of birth.

Subsequently, the learner must provide official documents (e.g., identification document) that validate the information they have provided. These official documents must be cross-checked in turn to validate them and consider them as a guarantee for the provided information. Realistically, practical solutions will still need to support this happening either offline/manually (physical ID card) or fully digitally (e.g., using eIDAS).

Once the data is validated, it will be consolidated as a user profile within the SIS, assigning it a unique identifier. Finally, the new profile created must be digitally certified.

Verified Profile Storage Service: The storage of verified profiles is a very delicate point. The information that is going to be stored in these systems is sensitive, so it is necessary to consider the compliance with various data protection regulations (e.g., GDPR). This implies that it must be ensured that only authorised users have access to this information and that data encryption techniques are used where necessary.

Verified Profile Transfer Service: The transfer of verified profiles should always be done using secure protocols such as HTTPS or RESTful APIs with OAuth 2.0. In addition, the identity and authorisation of the entities requesting access to this data must be verified. In addition to security, to ensure interoperability, it must be ensured that verified profiles can be interpreted by other systems, using the various common standards that exist. As an audit and traceability measure, access records to the profiles must be kept.

Verified Profile Validation Service: The service must be able to contact other validation services belonging to the different issuers in the validation chain. In addition, if it is in the role of issuer, it must verify the integrity and validity of the data of the provided verified profile.

Verified Profile Revocation Service: This service must define and automate the process to revoke verified profiles, including the validation of the revocation request and the removal of associated certificates or tokens. It must also implement a notification system to notify the affected user and all systems that have received the verified profile. Just like in the issuing process, for revocation it is advisable to have records detailing all revocation actions.

The different scenarios regarding the mobility of Learners between institutions can impact this use case since student data is often shared. The particularities for the cases of Joint programmes, credit mobility, and Open programmes are shown below.

In **joint programmes**, learners enrol in all participating institutions from the beginning, so their data is distributed among them. This can allow the learner to access resources from multiple institutions, which happens most frequently in this scenario.

Currently, multiple user identities and profiles might be created in parallel by participating institutions and not be interconnected. Hence an identity federation and an SSO implementation favour interoperability and are particularly important in this scenario.

In **credit mobility** scenario, learners only register at the home institution initially, after which they apply for mobility.

Currently, the learner's data is mainly managed by the sending institution, and temporary credentials are often given to the learner to access the resources of the receiving institution. As these are specific accesses, identity management is usually less integrated in these cases, depending much on the level of cooperation between institutions. This implies managing multiple credentials for the same learner during their mobility period.

By adopting the interoperability measures described in this chapter, this case could become simpler in terms of access management. Currently, in line with the proposed solutions, there is the Erasmus Without Papers

(EWP) programme that simplifies the administrative management of learners. This programme allows institutions to verify the identities of learners securely through a federated network, although it does not provide an identity federation itself.

Open programmes have a more flexible nature than the previous scenarios as they are not restricted to specific agreements between institutions. Learners must enrol and register at the destination institution. There is no centralised system, so each destination institution will provide learners with their own credentials and authentication mechanisms. This implies having to manage a large set of different credentials if participating in exchanges with institutions. Open programmes do not have a standard identity federation or SSO system. Following the interoperability guidelines described in this chapter regarding identity management, these programmes could be carried out in a much simpler way.

7.5 Overview of resources in use

After the sessions held with the alliances, it has been observed that approximately sixty percent of them use commercial tools for this use case. The most widely used commercial service is EduGAIN. Open-source tools used for this case account for only about ten percent.

7.5.1 Standards

This section includes a table that contains most used data standards, protocols, standardised APIs, or similar standards identified in the project, which can be implemented by tools and services.

Excludes: purely internal, unpublished standards used only by a specific tool.

Name	Information	Capabilities covered	Open standard	Owned / maintained by
SAML	Standardised way to tell external applications and services that a user is who they say they are. Technical standard used by SSO providers to communicate that a user is authenticated.	Single Sign-On (SSO), Federated Identity, Single Logout (SLO), Authentication, Authorisation, Attribute Sharing	✓	OASIS Consortium
OAUTH (OAuth2)	Standard designed to allow a website or application to access resources hosted by other web apps on behalf of a user.	Authorisation Grants, Access / Refresh Tokens	✓	Internet Engineering Task Force (IETF)

EDUPERSON	Lightweight Directory Access Protocol (LDAP) schema designed to include widely used person and organisational attributes in higher education.	Single Sign-On (SSO), Federated Identity, Attribute Sharing	✓	REFEDS
SCHAC	The SCHema for ACademia (SCHAC) is the result of the work carried out in attributes coordination to address inter-institutional data exchange.	Single Sign-On (SSO), Federated Identity, Attribute Sharing	✓	REFEDS / SCHAC community
European Student Card (ESC)	Digital or physical card that provides students with a unified identity to access services and benefits across participating universities and countries in Europe.	Digital Identification, Access to Services, Mobility Management, Recognition of Credits, Personalised Information, Erasmus+ Integration	✓	European Commission
eIDAS	EU regulation that aims to create a unified framework for secure and seamless electronic transactions and digital interactions across member states.	Electronic identification, electronic signatures, electronic seals, electronic timestamps, electronic delivery services, website authentication	Regulation	European Union: its implementation and enforcement fall under the authority of EU member states, with oversight by various EU bodies and agencies
ESSIF	This is a specific component of EBSI that develops the technical framework and standards for implementing self-sovereign identity across Europe. ESSIF focuses on the interoperability of decentralised identities and credentials, providing European citizens and students with control over their personal data.	Federated Identity, Authentication, Authorisation, Attribute Sharing	✓	European Commission
Verifiable Credentials	An open standard developed by the World Wide Web Consortium (W3C), it is designed for free use and is widely accessible for developing verifiable credentials across a variety of contexts.	Federated Identity, Authentication, Authorisation, Attribute Sharing	✓	W3C

7.5.2 Services

This section provides a table listing the main inter-institutional networks (e.g. Europe-wide, national, regional, alliance-wide), services, software, federations, platforms, etc. that institutions (or alliances) can connect to for data exchange or aggregation. It includes both open and commercial options that are of minimum relevance for this use case.

A complete list of identified services and tools could be found in Annex I – Inventory of tools and services.

Name	Information	Offered / managed by	Openness	Standards used
ADFS	Active Directory Federation Service enables Federated Identity and Access Management by securely sharing digital identity and entitlements rights across security and enterprise boundaries.	European Commission	Open access	EDCI, Verified Credentials (W3C) compatible
EduID	Digital identity for organisations in education and research.	SURF	Not open source; offered as a free service to educational institutions and their members in the Netherlands.	SAML, OAuth2
BankID	Identity management system	BankID Group (collaboration among banks and financial institutions in Sweden, Norway, and Denmark)	Not open source, not free.	OAuth 2.0, SAML
EduGAIN	The EduGAIN interfederation service connects identity federations around the world.	EBP	Not open source, free for participating institutions	EDCI, Verified Credentials (W3C) compatible
Eduroam	Eduroam is an international Wi-Fi internet access roaming service for users in research, higher education, and further education. It provides researchers, teachers, and students network access when visiting an institution other than their own. Offering international authentication infrastructure.	Eduroam Consortium (federation of institutions and national eduroam operators)	Not an open-source project, free for users	RADIUS for authentication and authorisation

eduTAP	Digital campus card for every member of higher education institutions. Their mission is to fulfil the interoperability vision of the European Student Card. eduTAP Is an educational ID and a collection of service passes in the digital wallets.	European Commission's Directorate-General for Education, Youth, Sport, and Culture	Open source and free	SCORM, xAPI
ESC Router	The European Student Card establishes a common European identity for higher education students. Students can get their student status verified easily across Europe with their European Student Card.	EBP	Open access	EDCI, Verified Credentials (W3C) compatible
MyAcademicID	Aims to establish a European-wide solution for digital student identity and credential verification, facilitating secure and trusted access to academic services and resources. The Attribute is released as part of the EduGAIN attributes.	European Commission, specifically the European Student Card initiative.	Free of charge and intended to be open source	GDPR, SAML, EDUFID, OAuth2
ORCID	ORCID enables transparent and trustworthy connections between researchers, their contributions, and their affiliations by providing a unique, persistent identifier for individuals to use in research, scholarship, and innovation activities.	ORCID Inc.	ORCID is not open source but offers free basic registration for individual researchers along with APIs and tools for integration.	OAuth

7.6 Analysis

Two different kinds of solutions are in use at most higher education institutions: the first ones are the student information systems that manage the creation, storage, deletion, and validation of student information. The other are identity providers: services that manage the identity as such and extract the user's permissions and roles from there; provide solutions used for log into 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.

Different from other use cases, user identity is already supported by widely mainstreamed European solutions that many higher education institutions have already adopted. EduID is an institution-independent digital identity specifically designed for the education and research sector currently implemented in the Netherlands and Sweden.

EduGAIN is an international service that connects identity federations specifically for research and education purposes. In simpler terms, 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.

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

RegApp is a federated open-source identity management system, which is developed at the Scientific Computing Center (SCC) at KIT.

While EduGAIN provides mature and widespread SSO capabilities, some core use cases (e.g. use case 3 on access to tools) will require better interoperability at the level of key attributes (e.g. programme or field of study, status, ...) that need to be understood consistently alliance-wide to implement access policies. One major note on the table above is that the absence of a mark in storage service, revocation service... does not mean that 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

© 2024 Freepik

8.1 Use case definition

This second supporting use case covers the necessary framework for trusted institutional identities, facilitating smoother collaboration and exchanges between HEIs. To realise seamless exchange and data flow, HEIs need systematic and trusted ways of identifying other HEIs as such, whether they are "known" to each other or there has been prior contact between the institutions. There are multiple attributes that form an institution's identity, ranging from formal attributes such as the accreditation or license obtained from an accreditation body to various indicators (e.g., ranking, enrolment data or research capacity).

It should be noted that the need to address institutional identity systematically primarily arises when considering data exchanges between or beyond EU-As: within one alliance – normally including less than 10 institutions – all institutions know each other and can easily manage identity, including establishing that all partners are accredited.

8.2 High-level flow

Being able to share this data systematically facilitates building trust relationships between institutions. For the core use cases that rely on this supporting use case, basic institutional identity and accreditation status are essential, which is thus the focus of the use case and the reference architecture at this stage.

Additionally, processes are defined for verifying an institution through a digitally signed asset and the workflow in which an institution consults a public directory for information on an external institution to access details about its interoperable APIs.

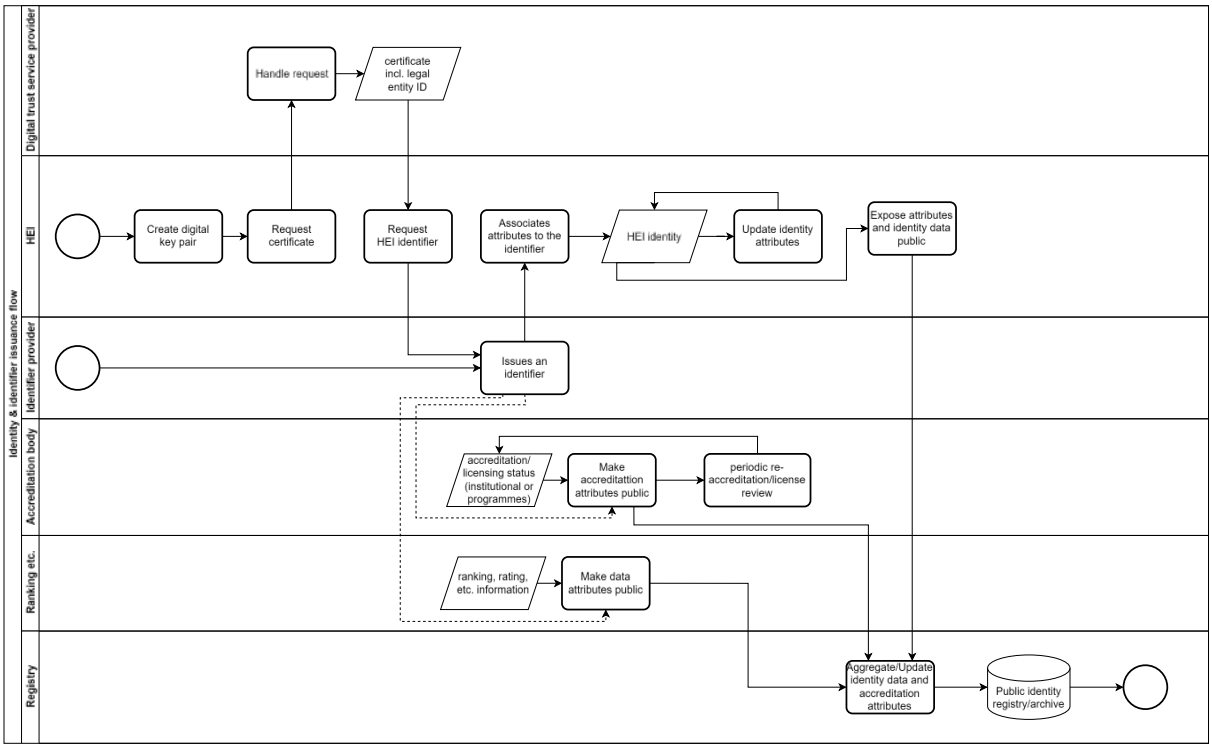


Figure 47 - Steps required to make public institutional attributes.
© 2025 European Union

In the diagram above, the process by which an institution obtains an identity is represented, considering all the parties involved in the process:

- An **identifier provider** (e.g., a national ministry or agency responsible for higher education) assigns an identifier to the institution, either at the institution's request or pro-actively. The identifier provider also makes that information publicly available.
- The **higher education institution** itself may attach additional attributes and data to the identifier and publish those. Moreover, the institution requests accreditation or renewal thereof.
- The **accreditation body** will decide on the institution's (re-)accreditation and make public information on the accreditation decision.

- The **ranking** entity provides additional information to the identity, such as a comparative rating or ranking.
- The **registry** aggregates all information related to the institution and maintains it, making this information publicly accessible.
- The **digital trust service provider** issues a certificate that the entity can later use 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. This identifier will then be referenced by the accreditation body and other actors, such as ranking providers, who will link additional information such as ratings or licensing status. This additional information will eventually be aggregated with the core details of the institution and the identifier in a public registry that displays 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. Additionally, a certificate object has been defined that includes a legal entity ID. However, it is possible that an alliance may not possess this ID, though this is neither expected nor required for this flow.

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

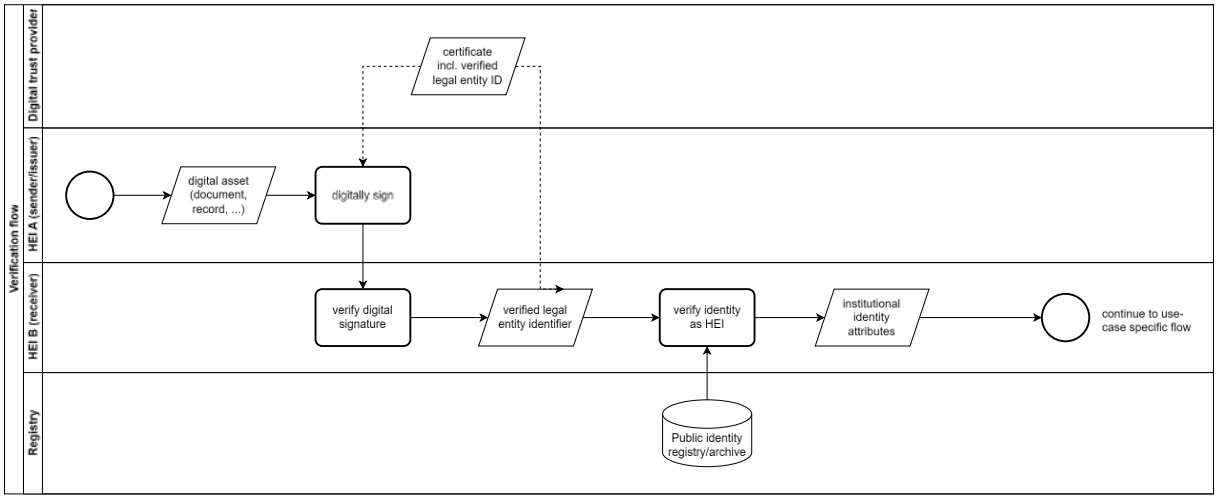


Figure 48 - Steps required to verify an institutional identity.
© 2025 European Union

The foregoing diagram describes the flow through which, given a digital asset, the trustworthiness of the issuing institution is verified. The asset is signed with a certificate issued by a digital trust provider, and this signature is subsequently verified by the institution receiving the asset, using a public registry that securely stores the institution's data. Once verification is complete, the flow can continue to other use cases. For instance, it may proceed to use case 2 (apply and get recognition) when an institution receives a credential and confirms that the issuing institution is trustworthy..

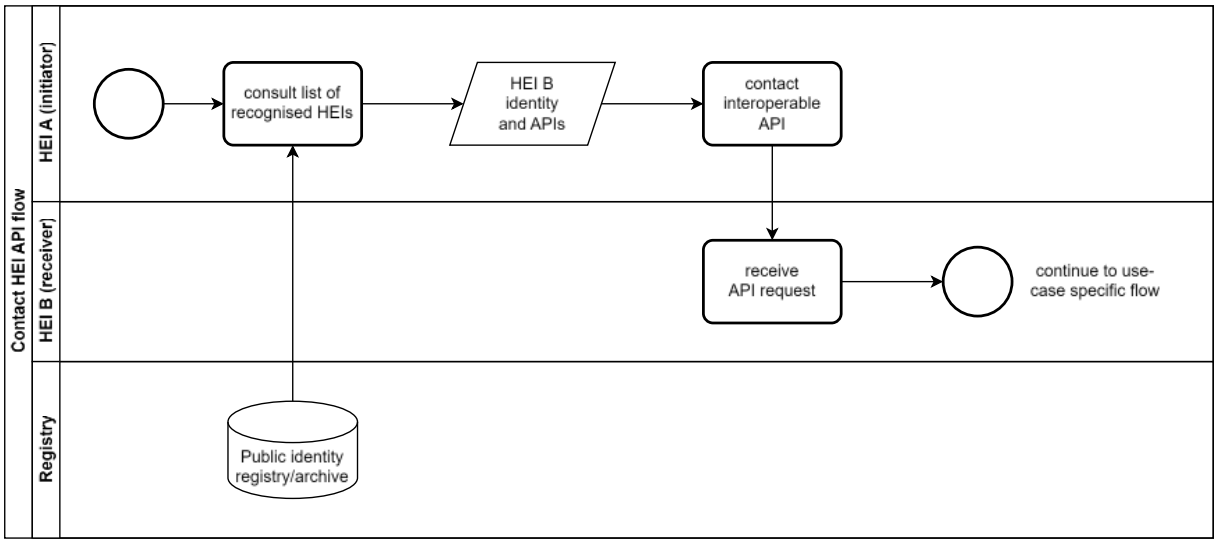


Figure 49 - Steps required to get interoperable API information from an institution.
© 2025 European Union

This flow, which is the simplest of the three, outlines the steps to make calls to an API exposed by an external institution. First, a query is made to the identity registry to obtain a list of trusted institutions. Finally, contact is made with the exposed API of the desired institution, which provides information on how to integrate with it in an interoperable manner. This flow may lead to another, more complex flow, such as querying the available courses at the contacted institution, having already obtained the necessary information to integrate this data.

8.3 Draft architecture

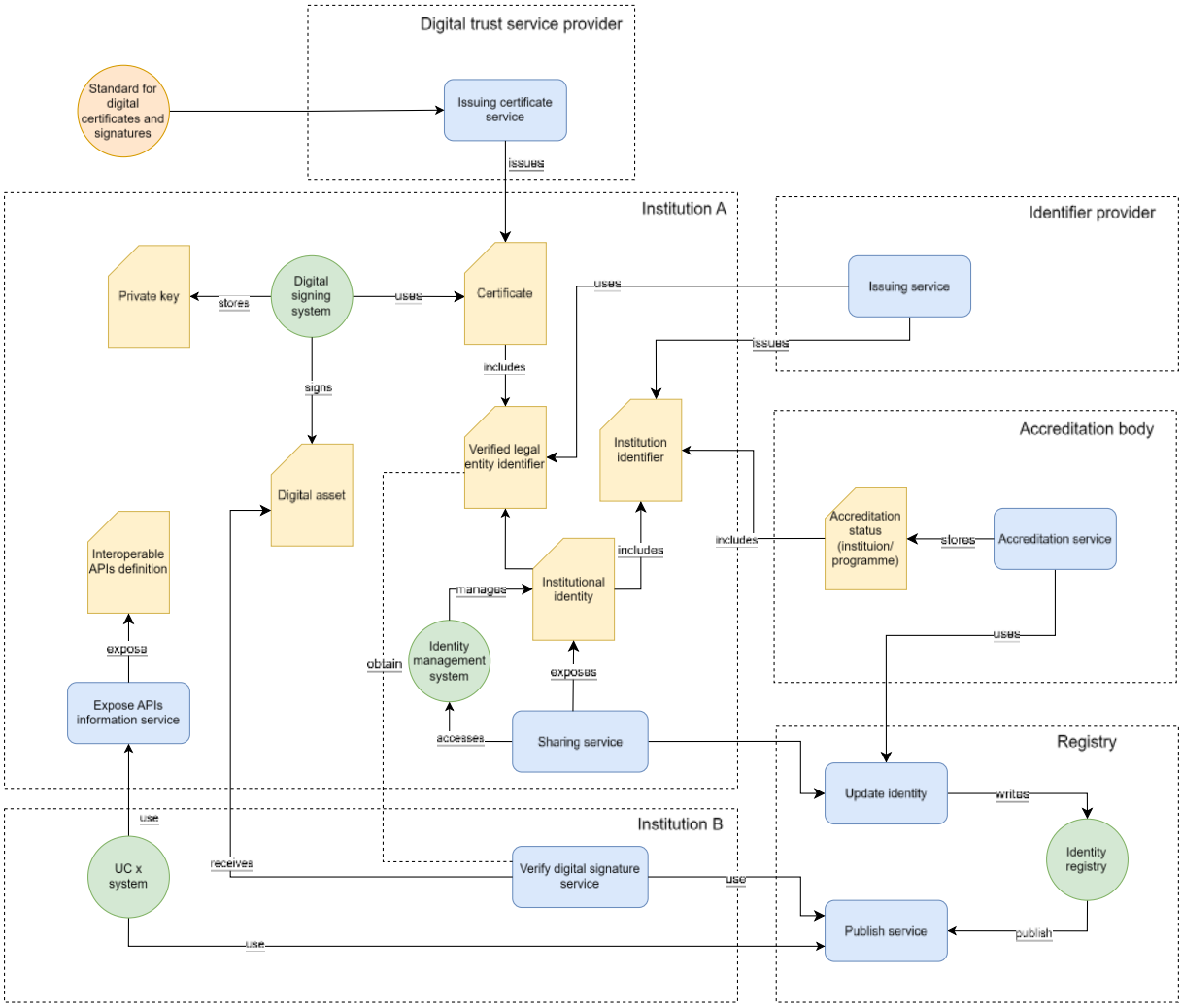


Figure 50 - Main components required to share institutional identity attributes.
© 2025 European Union

This draft architecture represents the essential components needed to support the previously described high-level flows. The following sections detail the key components of this architecture:

Business objects:

- **Institution identifier:** Unique identifier that distinguishes one institution from others.
- **Institutional identity:** Data object with additional information on the institution.
- **Interoperable APIs definition:** Definition of the interoperable APIs exposed by the institution to facilitate seamless integration with external institutions.

Services:

- **Sharing service:** Exposes identity information, together with technical information required for interoperability (e.g., API endpoints of other interoperable services the institution exposes). The identity information would also be available on the institutional webpage and might be aggregated into listings of institutions such as global rankings or those provided by the ENIC-NARIC networks.
- **Verify digital signature service:** A service that validates the signature used to verify an asset from an external entity. This service uses the publication service of the identity registry to confirm the verified legal entity identifier of the institution.

Systems:

- **Identity management 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. The first step is to contact the service of the institution that publishes information on interoperable APIs.

8.4 Interoperability and required capabilities

At present, this use case is among the lowest priorities for alliances and institutions. This is due to the small number of institutions within each alliance, where identity is managed based on existing trust relationships that do not require an automated approach to checking accreditation of other institutions.

However, as the need for interoperability among institutions and alliances expands, the number of involved institutions could rise significantly. This will create new trust relationships that will need formal validation through the institutions' identities. These identities must be certified and include specific characteristics that clearly define and position the 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. Additionally, this would allow for classification and grouping based on these characteristics, making it easier to position institutions within specific areas (e.g., research, technological resources, academic offerings) that align with 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.

8.4.1 Communication

To securely transfer this data, appropriate **communication protocols** such as HTTPS should be used to protect the integrity of the data during transmission. This protocol helps prevent man-in-the-middle attacks. Implementing **frequency and volume limits** on requests to the service will also help to prevent server overload and potential denial-of-service (DoS) attacks.

8.4.2 Data protection and licensing

Since the institution's identity is the trust anchor for the entire ecosystem, security measures to ensure the integrity of the data are crucial.

- **Authorised Access:** Access to the identity management system and systems managing accreditation data should be restricted to authorised users only. Additionally, it is advisable for these users to follow Multi Factor Authentication (MFA) systems for access. Using the least privilege principle, rights to change this information should be disabled by default.
- **Digital Signatures:** Providing key data with digital signatures that can be verified by recipients independently can increase trust in the identity data.
- **Auditing and Monitoring:** Establish logging and monitoring systems to capture all actions conducted within the identity management system. Regularly scrutinise these logs to swiftly identify and address any unusual or concerning behaviour.
- **Data Backup:** Consistently create backups of the identity management system data and securely store them off-site. This guarantees the ability to recover data in the event of loss, damage, or corruption.

Another useful security measure that can be adopted universally is training personnel with access to such sensitive data about security best practices and procedures. Human error renders previous measures ineffective and is often the most common factor in causing security breaches.

8.4.3 Boundaries

There are various processes for certifying and accrediting institutional identities, ranging from accreditation by national or international agencies to quality certification. Similarly, there are many authorities that can validate institutional identities, such as ministries of education or international organisations. This use case only addresses how the accreditation/quality assurance status can be provided in an interoperable way but does not seek to change the required accreditation and validation processes.

8.5 Overview of resources in use

Since this use case is still quite new and there are many small to medium-sized alliances, there is not a significant number of related tools or standards. However, there are relevant services and projects that may be of interest for the future.

8.5.1 Standards

This section includes a table that contains most used data standards, protocols, standardised APIs, or similar standards identified in the project, which can be implemented by tools and services.

Excludes: purely internal, unpublished standards used only by a specific tool.

Name	Information	Capabilities covered	Open standard	Owned / maintained by
ELM	European Learning Model	Digital identification	✓	DG EMPL

8.5.2 Services

This section provides a table listing the main inter-institutional networks (e.g. Europe-wide, national, regional, alliance-wide), services, software, federations, platforms, etc. that institutions (or alliances) can connect to for data exchange or aggregation. It includes both open and commercial options that are of minimum relevance for this use case.

A complete list of identified services and tools could be found in Annex I – Inventory of tools and services.

.

Name	Information	Offered / managed by	Openness	Standards used
European Tertiary Education registry (ETER)	European Tertiary Education Register, a database containing information on European higher education institutions (HEIs), including names, locations, and statistics.	European Commission	Open, data available for public access	European Tertiary Education Register, a database containing information on European higher education institutions (HEIs), including names, locations, and statistics.

Register of Public Sector Organisations (OrgReg)	OrgReg is a comprehensive database that provides basic identifying information on higher education institutions (HEIs) in Europe, a historical record of previous names, relationships/linkages between institutions as well as demographic events, such as mergers.	RISIS	Registration required	ORCID
World Higher Education Database (WHED)	World-wide database of officially recognised higher education institutions.	International Association of Universities	Access limited to authorised users, subscription-based	ORCID
EWP institutions API + Registry	Once implemented by the host, it allows external clients to retrieve general information on institutions either covered, or otherwise known, by this host. This information includes things like address, logo image and key contact persons. It also enables the discovery of API endpoints for EWP protocols.	Erasmus Without Paper Consortium	Public API	REST API, EWP specifications, OAuth 2.0

8.6 Analysis

Institutional identity is currently often based on non-digitalised trust relationships. There are already Europe-wide organisations/projects like the ENIC-NARIC[21] network or DEQAR[22] listing accredited institutions, with the latter providing standardised data on external quality assurance/accreditation in line with agreed European standards. With ETER, OrgReg and WHED there are large-scale database of verified institutional identity attributes and further rich datasets. The EWP API & Registry not only provide identity information, it also allows discovery of interoperable APIs that an institution exposes.

Despite the existing tools and networks, each in widespread use in its specific domain, these are not yet seamlessly connected between each other, nor with additional identity attributes or other institutional data self-published by institutions.

[21] ENIC-NARIC - gateway to recognition of qualifications
[22] Database of External Quality Assurance Results, https://www.deqar.eu/



PART 9

Key data standards

9 Key data standards

Data standards play a major role in semantic interoperability. The following sections propose a set of key data standards that are necessary to achieve interoperability in one or several use cases. For interoperability within one European University alliance, the respective data standard to be used could be agreed at alliance-level. For interoperability between and beyond EU-As, standards agreed at a higher level might be necessary.

9.1 Learning data standard

Learning specification

- **Identifier:** The learning specification should be clearly identified; thus, a unique identifier is needed. This identifier must be unique at alliance or institution level. The former is desirable due to the potential future overlap between identifiers of two or more institutions within an alliance.
- **Title:** The title of the learning unit.
- **Description:** A learning specification description is also required to make the learning specification readable. It should clearly explain and include all aspects of the learning specification.
- **Mode:** The mode identifies the learning specification modalities supported (e.g., online, live or hybrid). This information is important as the mode of the learning specification could be a barrier for learners.
- **Activities:** Learning specifications integrate related activities (e.g., problem solving, report writing). These activities should be defined and seamlessly identifiable.
- **Prerequisites:** The learners start the discovery use case by searching learning opportunities, which match their learning path. This means that every learning specification should reflect prerequisites regarding knowledge or skills related or not with other learning specifications.
- **Assessments:** Related assessments that demonstrate learner's acquisition of a particular knowledge or skill in relation to the learning specification.
- **Outcome:** To the outcome presents to the learners the specific knowledge or skills that they will acquire through the learning specification.
- **Credits:** Number of ECTS credits awarded for successful completion of the learning unit.
- **Entitlement:** A specification of an entitlement that this learning specification may give access to another learning opportunity.
- **Usage Rights:** Information about the usage rights and license of the course content.
- **Intellectual Property:** Information about the intellectual property of the content.

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

Learning offering

- **Mode:** Although the learning specification already contains this information, in specific cases the same learning specification could give access to learning offerings with different learning modalities.
- **Schedule:** Detailed information about the actual timetable of the learning opportunity. This information will help learners to assemble their own learning path without scheduling conflicts between learning opportunities.
- **Duration:** The total duration of the course (for example, in weeks, months).
- **Cost:** The cost of the course for learners.
- **Accessibility Options:** Information about the accessibility options available for learners with disabilities.

In use case 2 - Apply and get recognition, learning application standards are discussed so that institutions can reach agreements on the enrolment of learners in joint programmes. These learning applications, to achieve the goal of interoperability, should have the following base fields as standard.

Learning application

- **Personal Identification:** Learner's name, date of birth and national identification number.
- **Contact Information:** Email, telephone number.
- **Academic History:** This is the information related to previous institutions, degrees obtained, and their corresponding dates.
- **Learning Offering Information:** Name of the learning offering and identifier the potential learner seeks to enrol in.
- **Destination Institution:** Institution where the learner wants to take the learning offering.
- **Privacy Policy:** Acceptance of the privacy policy and personal data processing.
- **Truthfulness Statement:** Declaration that the information provided is truthful and accurate.

Interoperability: learning data standards should be compatible with existing standards that cover this area, such as ELM.

9.2 Agreements standards

To achieve interoperability, it is necessary to reach a series of agreements between institutions. These agreements can lead to exchanges of information, allow access to resources by learners from other institutions, and even be the basis for creating joint programmes such as the joint programme. The standardisation of these agreements could facilitate collaboration between institutions, thus promoting mobility programmes and interoperability.

Within the framework of the agreements, in terms of mobility, there is an agreement between institutions that defines a series of requirements to be able to recognise the learning offering of the institutions as valid and recognisable by other institutions. This agreement allows that once the learner finishes the learning offering, this achievement is recognised by their home institution and by all those that are part of the agreement. A standard for this type of agreements should include 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 focuses on the recognition of learning offerings between institutions. If we expand the framework to a higher level of collaboration between institutions, the agreements need to be similarly broader. Having a standard that covers the basic concepts of these agreements, as in the previous case,

would facilitate and promote collaboration between institutions. A standard agreement between multiple institutions for a common mobility plan as in use case 2 - Apply and get recognition should include at least this information:

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

- **Programme name:** Defined name for the inter-institutional collaboration programme.
- **Participating institutions:** Names and details of the institutions that will be part of the collaboration agreement.
- **Objectives:** Objectives and goals of the collaboration programme.
- **Curriculum:** Detailed description of the curriculum that makes up the collaboration programme. This includes the learning offerings of which it is composed.
- **Credits:** Distribution of ECTS credits.
- **Distribution:** Distribution of teaching among the different participating institutions.
- **Admission criteria:** Prerequisites that learners must meet to be able to apply to the programme.
- **Application process:** Procedures and deadlines for the application and admission of learners to the programme.
- **Credit recognition:** Measures of credit recognition and their transfer between participating institutions.
- **Evaluation process:** Methods and scales for evaluating the performance of learners with respect to the programme.
- **Roles and responsibilities:** Definition of roles and responsibilities of each institution in the management of the programme in which they collaborate.
- **Intellectual property:** Agreements on intellectual property on the materials used in the offerings that make up the programme.
- **Jurisdiction:** Determination of legal authority in case of disputes for conflict resolution.
- **Agreement terms:** Validity period, termination, and review procedure.
- **Agreement signature:** Signatures of the authorised 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.

On the other hand, within the framework of the Erasmus+ project, templates[23] have been developed for this type of agreements, which are useful for establishing new agreements between institutions.

[23] 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 such as tools, this document has discussed controlled vocabularies. These controlled vocabularies are a set of terms with their respective definition and translations that represent basic concepts. It is a good idea to use these vocabularies commonly to be able to group heterogeneous information into homogeneous groups that facilitate their interoperability and use.

The use of controlled vocabularies can be complemented with the standard definition of tools. Below are the minimum fields that a standard representation of a tool should have. Please continue with the fields you consider necessary for this standard representation.

Tool/asset data standard

- **Identifier:** Unique identifier of the resource. This field will allow each resource to be uniquely identified.
- **Name:** Name of the resource.
- **Description:** Summary of the functionality of the resource and its purpose.
- **Resource type:** Category of the resource (e.g., software, laboratory...).
- **Provider institution:** Name and identifier of the institution providing the resource.
- **Access details:** Requirements necessary to access the resource, application procedure and limitations of use of the resource.
- **Cost:** Information about the cost of the resource.
- **License and terms of use:** Terms and conditions of use associated with the resource.
- **Format:** Data format and protocols supported by the resource. This information will help interoperability in terms of integrating this data by multiple institutions.
- **Tags:** Keywords that allow grouping between resources and that later facilitate their search.
- **Usage indicator:** Data on the use of the resource. This data is important as it will allow usage statistics to be obtained and will allow planning its scaling if necessary.

The use of tools, whether they are integrated within the institutions' LMSs or as external tools, generate a multitude of data that can be difficult to organise. These data (learning records) must be standardised to organise and consult them effectively. In addition, considering interoperability, this standardisation is especially necessary to share learning records that learners have generated with tools that other institutions different from their original one may have been able to share.

There are different models for the standardisation of learning records in use. Those used by appliances are mentioned in this document. Therefore, this section focuses on the minimum capabilities that must be met to be considered on the path to interoperability.

- **Interoperability:** It must be compatible with a wide range of systems and learning platforms (LMS). Also, it should be compatible with other educational standards such as xAPI, SCORM or cmi5.
- **Flexibility:** Due to the heterogeneous nature of the results of activities using tools, the standard must allow dealing with all of them.
- **Scalability:** Given the amount of data that can be generated, it must be light enough not to penalise processing and storage performance.
- **Detail:** It must capture data accurately and in detail to provide a comprehensive picture of learning records.
- **Metadata:** It should support descriptive metadata that provides additional context about learning records.

To summarise, the chosen standard must be robust and flexible, capable of managing a variety of data and learning situations, while ensuring interoperability, security, and usability. Integrating advanced analytics, descriptive metadata, and privacy and security considerations will ensure that learning data is useful to 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 using 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 similarities with, for example, xAPI, as it follows the standard actor-verb-object-result format.

9.4 Educational resources standard

Educational resources exist in a variety of formats, making it complicated to find a shared model to describe them. Agreeing on a common standard to follow is mandatory to successfully share resources between institutions. This section contains an analysis of the interoperability requirements of the different systems and services outlined in the reference architecture.

Discoverability of educational resources requires a metadata standard providing:

- **Identifier:** Unique identifier of the educational resource.
- **Name:** Name of the resource.
- **Description:** Summary of the functionality of the resource and its purpose.
- **Author:** Information about the creator of the resource.
- **Owner:** Information about the owner of the rights to the resource.
- **Learning objectives:** Description of the objectives and competencies of the resource.
- **Format:** Description of the format of the resource, e.g., video, text.
- **Access point:** Location from which the exposed resource can be accessed.
- **Terms of use:** Licenses 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:** Date of publication of the resource.
- **Version:** Current version of the exposed resource.
- **Technical requirements:** Software or hardware that is necessary to use the resource.

- **Compatibilities:** Information about the compatibility of the resource with educational standards.
- **Tags:** Keywords that facilitate its search and categorisation.

Using an existing educational resource requires associated tool metadata as information about the tools that can be used to open de content such as tool identifier. This tool identifier could be used to search for it in the tool catalogue, thereby obtaining all the detailed standard information about it as described in the previous chapter 9.3 Tools and assets data standard.

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

9.5 User identity standard

In student mobility scenarios, as seen 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 followed. A standard defining a user identity must contain the necessary information to identify the user uniquely and unequivocally.

The minimum fields 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:** User contact information.
- **Role:** The user's role within the institution.
- **Department:** The department or faculty to which the user belongs.
- **Authentication Methods:** Information about supported authentication methods (e.g., MFA).
- **Digital Certificates:** Certificates if used for authentication.
- **Permissions:** List of specific permissions assigned to the user.
- **Last Update:** Date of the last update to the user's data.
- **Change History:** 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 resorting to a proprietary user identity model, differentiation between the identity provider system and student information system must be considered. 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

In line with the description in chapter 8.4 Interoperability and required capabilities – Institutional Identity, promoting interoperability between institutions requires the creation of a distinct identity that is recognisable and easy to position. The main basic 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. This may include the Erasmus code, which facilitates 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, including phone number, email address, and any other relevant communication channels.
- **Institutional accreditation:** Details of the formal recognitions and accreditations that the institution has received, which certify its educational quality and standards.
- **Optional:**
    - **Indicators/metrics:** Quantitative data that provides insight into various aspects of the institution's performance, such as 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 that provides 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 function as an interpreter, translating local terms to the shared controlled vocabulary, and reorganising fields from the local data model to the ones in the shared standard.

Central catalogue approach: Mapping only translates metadata. Sharing service can take a reactive role: Receives a request from the central catalogue to send data and responds with the list of updated learning opportunities. If the local catalogue is proactive (sends updates to the central catalogue) it does not have to expose a query interface.

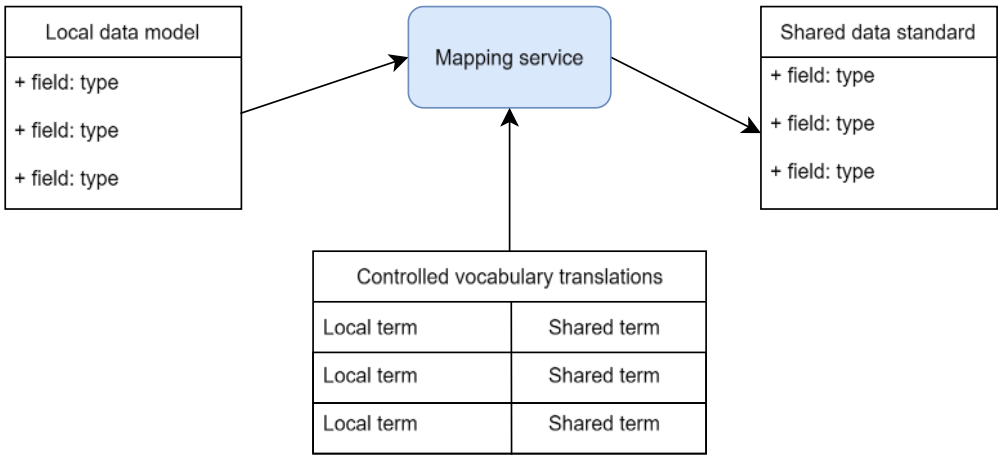


Figure 51 - Mapping service data conversion process schema.
© 2025 European Union

PART 10, 11, 12

Annexes

10 Annex I – Inventory of tools and services

Tools	Link	Description	Draft architecture systems covered
Bestr	External link	Digital credentialing platform to valorise competencies growing in the higher education system and connect them with employers.	Credentials management system Claim management system
A+ (in house developed platform, mostly for CS)	External link	An interoperable and extendable Learning Management System (A+ LMS, apluslms) that uses a combination of services to enable teachers to fully customise their e-learning materials and to combine different kinds of materials flexibly.	Learning Management system Educational resources management system Tool
Aalto.fi (for Open University)	External link	Course catalogue with the list of courses open to everyone. Open University offers individual courses in Business, Technology, Languages, and Art and Design.	Catalogue management system
Aaltodoc	External link	Institutional repository of Aalto University.	Educational resources management system
Biblioteca do conhecimento online	External link	Educational resources repository.	Educational resources management system
Academic Directory	External link	Registry of academics and researchers, can be publicly shown, interconnecting them and they can send emails.	
EC2U - Internal tool - Semantic Search engine		EC2U is developing a Developing a semantic search engine supporting automatic classification and structural search of the large document corpora	Educational resources management system - search service
ADFS	External link	Active Directory Federation Service enables Federated Identity and Access Management by securely sharing digital identity and entitlements rights across security and enterprise boundaries.	Identity provider
Shibboleth	External link	Identity management system	Identity provider
EduID	External link	Digital identity for organisations in education and research.	Identity provider
BankID	External link	Identity management system	Identity provider
EduGAIN	External link	The EduGAIN interfederation service connects identity federations around the world.	Identity provider

Sisu	External link	Sisu is a tool that students, teachers, and members of Learning Services staff in various roles can use for managing all aspects of study planning and scheduling as well as credit entry.	Student information system Claim storage Learning records store Catalogue management system
RegApp	External link	Federated open-source identity management system, which is developed at the Scientific Computing Center (SCC) at KIT.	Identity provider
Apogee	External link	APOGEE is a management system that gather a big part of our curricula and students processes such as student registration, grades, or certifications. This solution has been mandatory and nationally developed since 1995 for all French HEIs. HEIs must implement their own APOGEE instance. APOGEE instances can then communicate between one another in the APOGEE network.	Student information system Claim storage Credentials management system
Apply@PoliTO	External link	Application portal developed at Politecnico di Torino.	Student information system Curriculum management system
Aprèn	External link	Portal that provides access to the teaching support materials developed by the teaching staff of the Universitat Politècnica de Catalunya (UPC).	Catalogue management system
Asana	External link	Project management tool. Mainly used for organisational tasks.	
ATENEA BI	External link	Based on Moodle.	Learning records store Learning management system Educational resources management system
ATENEA TFE	External link	Multilingual portal for Support Platform for bachelor's and master's theses. Platform to formally submit the final bachelor's and master's theses Exchange information with the thesis supervisor. Once the student has uploaded all the final thesis documents via the Atenea-TFE platform, the thesis supervisor can approve the documents. This system is self-developed based on Moodle.	Educational resources management system
AZON – The Atlas of Open Science Resources	External link	Collect, process, and share science resources in an open digital form to all interested parties.	Educational resources management system
Azure AD	External link	Unified identity and network access.	Identity provider
BCDiploma	External link	Digital credentials solution.	Credentials management system Claim management system
Big Blue Button	External link	Virtual classroom software	

Biper	External link	Identity management system.	Identity provider
Blackboard	External link	Learning management system	Learning Management system Educational resources management system
BLOOM Hub	External link	BLOOM Hub is a “European hub for blended and online learning”	Catalogue management system Learning management system
Brokers		Applications to connect local student management system to the UNIC virtual campus.	Publishing services Mapping services Sharing services
Campus Management system link		Applications to connect local Student information systems to the central one.	Publishing services Mapping services Sharing services
Campus+	External link	Campus+ is a space where higher education professionals can learn, share, and connect with their colleagues at universities.	Educational resources management system
CampusNet 2022 SP4 Classic	External link	Integrated campus management system. CampusNet® digitises the entire student life cycle.	Catalogue management system Curriculum management system Student information system
CAMPUSonline		It encompasses the entire student life cycle, from applying for a study programme to student and examination management, all the way to graduation.	Student information system Credentials management system Catalogue management system Educational resources management system
Canvas LMS	External link	Learning management system.	Educational resources management system Catalogue management system Learning management system Credentials management system
Virtual Card	External link	The EC2U Virtual Card is a lightweight mobile-based academic identification card built on top of two mature and widespread identity management systems: • European Student Card (ESC) framework • EduGAIN federated identity network Planning to add support for verifiable credentials.	Identity provider Claim storage system
Chamilo	External link	Open source LMS and LCMS.	Learning Management system Educational resources management system

CINECA	External link	Software for the management of teaching aimed at universities allow to digitise both the student's lifecycle and all activities to prepare, provide and manage an institution teaching offer. Cineca also provide tools to digitise teaching and learning themselves, with digital education services. Such services include tools for e-learning, e-assessment (computer based testing) and digital credentialing through Open Badges and Blockcerts (see Bestr).	Student information system Credentials management system Claim management system
civica.eu	External link	The my.civica.eu platform is part of the CIVICA initiative, which is a collaborative project involving leading European universities focused on social sciences. The platform displays a course catalogue, a Researcher Directory, and facilitates the management and coordination of various academic and administrative processes for students, researchers, and faculty members across these institutions.	Catalogue management system
CIVIS Passport	External link	This digital certification tool will give students a visual record of their CIVIS achievements to accredit their success. For each CIVIS activity successfully completed, students will receive a digital OpenBadge which sets out the: • Learning outcomes • Competences and skills acquired • The method of assessment (for curricular activities)	Credentials management system Claim management system
Colibri	External link	Automate notetaking with AI.	Tool
Courses.aalto.fi	External link	Catalogue contains active degree-level teaching of Aalto University	Catalogue management system
CrownLabs	External link	CrownLabs is a set of services designed to deliver remote computing labs through per-user environments, based either on virtual machines or lightweight containers.	Tool
Dialnet	External link	Educational resources repository. Includes Scientific papers and research material.	Educational resources management system

DIDATTICA (Campus Management System)	External link	• Student Management (enrolment, registrations, transfers, fees, degrees, state exams, educational offerings, study plans, contracts, and selections of external teachers, assignments, educational reports and budgets, and more). • Didactic Management (educational offerings, study plans, programme guides, course coverage, admission tests, lists of enrolled students, interface with institutional email service, and other services). • Support for Teaching and e-Learning (sharing educational materials between teachers and students, submission of assignments, forums, delivery of video lessons, tests, and self-assessment exercises).	Student information system Catalogue management system Educational resources management system
DOVECOT	External link	Dovecot is an open-source IMAP and POP3 email server for Linux/UNIX-like systems.	Communication tools
Dropbox	External link	Data storage service.	Educational resources management system
Erua-ID	External link	Authoritative User Identity (Digital Wallet).	Identity provider Claim storage system
DSpace	External link	The Software of Choice for Academic, Non-profit & Commercial Organisations Building Open Digital Repositories.	Educational resources management system
EC2U internal tool -Interchange Platform		Mobility students' management system.	Mobility management system
eCandidat	External link	Aix Marseille University eCandidat application.	Student information system Application portal
edubadges (pilot)	External link	edubadges is the platform for digital certificates, including micro credentials, for the Dutch education sector. With an edubadge, you give learners proof of the knowledge and skills they have acquired.	Credentials management system Claim management system
EDUC course catalogue (Own solution as Course Catalogue)	External link	Custom solution for course catalogue.	Catalogue management system

EDUC8U	External link	Recommend tailored learning pathways aligned with student's career goals and aspirations.	Catalogue management system
Educast	External link	Record, edit, and publish with Educast. Repository of national educational videos.	Educational resources management system Tool
eduCloud	External link	EduCloud is a cloud-based School Management System and Learning Management System (LMS). It offers features such as online assignment management, attendance tracking, exam and result management, report card generation, communication tools, and AI-based analytics. The platform also includes tools for fee management, admissions, and transport tracking.	Learning management system Educational resources management system Student information system
Eduroam	External link	Eduroam is an international Wi-Fi internet access roaming service for users in research, higher education, and further education. It provides researchers, teachers, and students network access when visiting an institution other than their own. Offering international authentication infrastructure.	Identity provider
eduTAP	External link	Digital campus card for every member of higher education institutions. Their mission is to fulfil the interoperability vision of the European Student Card. edutap Is an educational ID and a collection of service passes in the digital wallets.	Credentials storage solution
EduXchange with OOAPI standard	External link	Open-source catalogue solution adapted for international use, which implements a custom identity provider. This centralised catalogue is filled with information from the local course databases via SURFeduhub using the OOAPI standard.	Catalogue management system
Erasmus+ App	External link	The Erasmus+ App has been developed under the 30 Years of Erasmus Campaign and is being further enhanced as part of the European Student Card Initiative. The aim of the application is to become the single point of entry for participants to access information on Erasmus+ opportunities, as well as to guide them through the processes surrounding their mobility and give them access to information and services.	

European Student Card (ESC)	External link	The European Student Card establishes a common European identity for higher education students. Students can get their student status verified easily across Europe with their European Student Card.	Identity provider
Europass	External link	Europass users can create a free profile with Europass, to record all their skills, qualifications, and experiences in one online location.	Credentials storage solution
EWP	External link	A digital solution for higher education institutions to connect their Erasmus+ mobility management systems so they can manage their mobility students online.	Mobility management system
Fullfabric	External link	Software solution for HEIs that supports digital transformation in admissions. Has three main modules: • Communication • Application and enrolment • CMS and LMS	Application portal Student information system Learning management system Catalogue management system Educational resources management system
Gala	External link	Gala is an open platform for collaborative authoring, revising, and sharing interactive learning modules and case studies.	Educational resources management system Learning management system
GitHub	External link	GitHub is a code hosting platform for collaboration and version control. It allows individuals and teams to use Git, a software for tracking and managing changes in code, in a web-based interface. GitHub is used for hosting, storing, and editing code for various projects, such as websites, applications, and open-source software. GitHub enables developers to share code files and work together on software development.	Educational resources management system
Gitlab	External link	GitLab is a web-based Git and DevOps platform that provides free open and private repositories, issue-tracking, and wikis. It is a self-hosted system that helps developers monitor, test, and deploy their code.	Educational resources management system
Gmail	External link	An email service provided by Google.	Communication tools
Google classroom	External link	Google Classroom is a suite of online tools that allows teachers to set assignments, have work submitted by students, to mark, and to return graded papers.	Tool

Google Drive	External link	Cloud storage and synchronisation service.	Tool
Google Meet	External link	Google Meet is a video conferencing service from Google.	Tool
Google Workspace	External link	Google Workspace, formerly G-Suite, is a surprisingly powerful cloud-based productivity suite.	Tool
ILIAS	External link	Open-source Learning management system.	Educational resources management system Catalogue management system Learning management system
INCF-TS	External link	The INCF Training Suite is a collection of open access platforms that aims to facilitate self-guided study in the sub-specialisms of neuroscience with an emphasis on Neuroinformatics.	Educational resources management system
Invest Virtual Campus	External link	The INVEST Virtual Campus is a central platform supporting key use cases for the alliance: • Provides a public catalogue of programmes, courses, and micro-credentials, enhancing discoverability and accessibility. Features include detailed programme information and news modules for promoting opportunities. • Facilitates applications for programmes, including bachelor's degrees and microcredentials, and supports cross-institutional enrolment. It also enables recognition of prior learning by managing transcripts and grading histories. • Offers a microcredentials platform for creating, issuing, and verifying digital badges, supporting modern credentialing and lifelong learning. • Includes an identity provider with single sign-on capabilities for seamless access across platforms. While external integration with partner universities is pending, it is designed for future interoperability via OpenID Connect.	Student information system Course Catalogue
Jabber	External link	Cisco Jabber delivers instant messaging, voice and video calls, voice messaging, desktop sharing, conferencing, and presence	Tool

Kahoot (Game Based Learning)	External link	Kahoot! is a game-based learning platform that allows educators, students, and other users to create and participate in quizzes, surveys, and interactive games in real time.	Tool
Kaltura (Video Platform)	External link	Establish, design, and manage a content. Video portal.	Tool
Keycloak	External link	Open-Source Identity and Access Management.	Tool
Knowledge Hub	External link	The EC2U Knowledge Hub is the central knowledge sharing and semantic search facility of the EC2U Alliance: it gathers, cleanses and cross-links content from a wide range of internal and external data sources, providing data consumers like user-facing apps and intelligence tools a ready-to-use source of structured data about skills, courses, research, local events, and other areas of common interest.	Educational resources management system Catalogue management system
KOPPS	External link	Kopps provides system support when planning courses and programmes at KTH and publishes information about the courses and programmes at kth.se.	Catalogue management system
LADOK (National system of student records)	External link	Ladok is a student record system. In Ladok you can register for a course, view your grades, and study results, and sign up for an exam. In Ladok, you can also generate an Official Transcript of Records and apply for a degree certificate. Ladok is used by most higher education institutions in Sweden and the system contains your academic records from all Swedish higher education institutions that use Ladok.	Student information system Claim storage Learning records store Credentials management system
Lime-Survey	External link	LimeSurvey is a simple, quick, and anonymous online survey tool for students, professionals, and enterprises.	Student information system Tool
Mahara	External link	Personal online spaces for students to access services and store work. They will become ever more useful as learners grow up and start moving between different types of learning and institutions.	Personal learning environment
Mastodon	External link	Decentralised social network.	Tool
Matrix	External link	An open network for secure, decentralised communication.	Tool

Microsoft 365	External link	It encompasses online services such as Outlook.com, OneDrive, Microsoft Teams, programmes formerly marketed under the name Microsoft Office, enterprise products and services associated with these products such as Exchange Server, SharePoint, and Viva Engage.	Tool Educational resources management system
Miro	External link	Visual workspace.	Tool
Möbius	External link	Interactive Learning Platform.	Tool
Moodle	External link	Moodle is an open-source learning management system designed to provide educators, administrators, and learners with a single integrated system to create personalised learning environments.	Educational resources management system Catalogue management system Learning management system
Mon Master	External link	French national platform aggregating information of available master's degrees.	Catalogue management system
MonDossierWeb	External link	Application to track your schooling.	Credentials management system Credentials store solution
MoveON	External link	A data and insights-based SaaS platform for international offices of higher education institutions.	Application portal Application validation service
MyAcademicID	External link	Aims to establish a European-wide solution for digital student identity and credential verification, facilitating secure and trusted access to academic services and resources. The Attribute is released as part of the eduGAIN attributes	Identity provider
my-memory.io	External link	Universal content platform for any sector.	Educational resources management system
National Federated Authentication (RCTSaai)	External link	Single Point of Authentication With RCTSaai you will only log in with your institutional account to access the various services. This service provides an authentication and authorisation infrastructure with the aim of simplifying the access of teaching and research communities to web services.	Identity provider
National Scientific Repository (RCAAP)	External link	Portuguese open repository.	Educational resources management system

Nextcloud	External link	Nextcloud Hub integrates the four key Nextcloud products Files, Talk, Groupware and Office into a single platform, optimising the flow of collaboration.	Educational resources management system Tool Communication tool
NOLEJ	External link	Empower instructional designers and teachers to rapidly generate interactive eLearning material.	Tool
Odoo	External link	Learning management system.	Learning management system Educational resources management system Communication tool Catalogue management system Tool
Open Educational Resources Platform	External link	Repository with open educational resources and courses	Educational resources management system Catalogue management system
OER repository	External link	Repository with open educational resources.	Educational resources management system
InvenioRDM	External link	The turn-key research data management repository.	Educational resources management system
One Identity Manager	External link	Identity Manager governs and secures organisation's data and users.	Identity provider
OneDrive	External link	Repository.	Educational resources management system
OnlyOffice	External link	Online office suite and workspace for students and educators to create, share, and collaborate on knowledge	Educational resources management system Tool
Open Educational Resources Observatory	External link	National Community Portal for Open Educational Resources.	Educational resources repository
Open edX	External link	Learners, course teams, and instructors use the LMS throughout the duration of a course.	Learning management system
Opencast (Video Platform)	External link	Opencast is an open-source video management system for academic institutions.	Tool
OpenLDAP	External link	OpenLDAP Software is an open-source implementation of the Lightweight Directory Access Protocol.	Identity provider
OpenLearning (Open / Mooc)	External link	The AI-powered learning platform for educators.	Tool
Open LMS	External link	Fully Customisable Open-Source LMS.	Learning management system Educational resources management tool

ORCID	External link	ORCID provides a persistent digital identifier (an ORCID iD) that you own and control, and that distinguishes you from every other researcher. You can connect your iD with your professional information — affiliations, grants, publications, peer review, and more.	Identity provider
Ouriginal	External link	Ouriginal by Turnitin is a software that helps detect and prevent plagiarism regardless of language.	Tool
Padlet	External link	Tool to make boards to collect, organise, and present anything.	Tool
Panopto	External link	Panopto provides software primarily for universities and enterprise businesses. Panopto's software is commonly used for lecture recording, screen casting, video streaming, and as video content management software, and is often used in remote work, e-learning, and corporate Training, and development environments.	Tool
PIN (National identifier Croatia) & ESI implemented as identifier	External link	The Croatian Ministry of Finance Tax Administration initiated the introduction of the personal identification number (OIB) into the Croatian legal system. The Ministry of Finance - Tax Administration is responsible for the assignation of the OIB to every person as a unique and obligatory identifier in the whole Croatian public administration system.	Identity provider
Postfix	External link	An open-source mail transfer agent (MTA).	Communication tools
PRISMA	External link	PRISMA is a multilingual course management system that lends support to the management of academic processes at UPC. It covers the three main aspects of course management: planning, development, and assessment processes.	Catalogue management system
PumuKit	External link	Open-Source Video Platform.	Educational resources repository
Roundcube	External link	Webmail client.	Communication tools
Sakai	External link	Open-source Learning management system.	Educational resources management system Catalogue management system Learning management system
Salesforce	External link	CRM.	Tool

FenixEdu	External link	Open-source software for higher education, knowledge creation and knowledge transmission.	Student information system Leaning management system
Slack	External link	Cloud-based team communication platform.	Communication tools
Socrative	External link	Game Based Learning.	Tool
Survey Monkey Apply	External link	Streamline how you collect and review applications for grants, scholarships, awards, and other programmes.	Tool
Microsoft Teams	External link	Microsoft Teams is cloud-based team collaboration software that offers core capabilities, including business messaging, calling, video meetings and file sharing.	Communication tools
UniverSIS	External link	Open-Source Student Information System.	Student information system
USOS	External link	Student management information system.	Student information system
Vortex	External link	A platform for collaboration and document sharing.	Catalogue management system
VURS	External link	VURS is a complete CMS/SIS adopted by EPICUR alliance which consists of the following components for supporting the necessary functionality to monitor mobilities, issue and recognise certifications (including ECTS and micro-credentials): • Course Catalogue: Public catalogue • Candidates App: Application portal • Students App: Application for the selected students • Registrar App: Application for the administrative staff to monitor learning pathways and students mobilities. • Faculty App: Application for the teaching staff delivering a course. • Admin panel: Specific part of the application for the Registrar App to admin the rights and roles of the rest of the users. • VURS API Server: Core service interacting with all the apps above and the VCLP component.	Student information system Catalogue management system Registrar Admissions system

VCLP	External link	Learning Management System, which is based on ILIAS. ILIAS is an open-source and free Learning Management System.	Learning management system
Webex	External link	Video conferencing and collaboration product suite.	Tool
Whaler	External link	Social and collaboration platform.	Educational resources management system Learning records store
Wordpress	External link	Web content management system.	Catalogue management system
Wowza Streaming Engine	External link	Customisable streaming software.	Tool
YouTube	External link	Platform for publishing videos.	Tool
Zonavídeo UPC (Video Web Portal)	External link	Platform for publishing videos.	Tool
Zoom	External link	Communication tool.	Tool
Zulip	External link	Communication tool.	Tool
Edu-sharing	External link	Edu-sharing software enables you to network your learning platforms and other educational software. Share learning content, metadata, and tools - make them available in an educational cloud and let your users use them in all connected systems.	Learning management system Educational resources management system
Apereo OpenLRW	External link	OpenLRW is a Java-based learning record warehouse.	Learning records system
Open Dashboard-api	External link	A web application that provides a framework for displaying visualisations and data views called „cards“. Cards represent a single discrete visualisation or data view but share an API and data model.	Learning records system - query service

11 Annex II – Inventory of standards and protocols

Tools	Link	Description	Usage
Open badges	External link	Open Badges is the world's leading format for digital badges. Open Badges is not a specific product or platform, but a type of digital badge that is verifiable, portable, and packed with information about skills and achievements.	Issue, manage and verify digital credentials
Blockcerts	External link	Blockcerts is an open standard for creating, issuing, viewing, and verifying blockchain-based certificates. These digital records are registered on a blockchain, cryptographically signed, tamper-proof, and shareable. The goal is to enable a wave of innovation that gives individuals the capacity to possess and share their own official records. We invite feedback, contributions, and general discussion.	Create, issue, view and verify credentials
xAPI	External link	Standard for learning technology that makes it possible to collect data about the wide range of experiences a person has.	Share student data
2FA	External link	Two factor authentication.	Security enabler used for authentication and authorisation

LTI	External link	Learning Tools Interoperability. Set of specifications to allow remote tools and content to be integrated into a Learning Management System.	Share content between tools and LMS
EDCI Standards	External link	European Digital Credentials standards is a set of standards, services and software which allows institutions to issue, store, verify, share, and identify digital, tamper-proof credentials within the European Education Area. It allows for the identification, verification, issuing, storage, and sharing of digitally signed credentials in cross-border context.	Identification, verification, issuing, storage, and sharing of digitally signed credentials
eIDAS	External link	Regulation (EU) No 910/2014 (hereafter the eIDAS Regulation or eIDAS), on electronic identification and trust services for electronic transactions in the internal market, provides a regulatory environment for electronic identification of natural and legal persons and for trust services.	Legal framework for electronic identification
Kerberos	External link	Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well.	Authenticate users
SSO		Authentication scheme that allows a user to log in with a single ID to any of related, yet independent, software systems.	Authenticate users
EMREX	External link	EMREX is an international (European) data protocol that can be implemented with simple means to exchange education data (with focus on educational data from Higher Educational Institutions (HEI)), between two digital systems in a digitally machine-processable and GDPR-compliant way. The benefit of EMREX, with its electronic data exchange solution, is to empower individuals to control their own student data and exchange throughout lifespan, across borders for various purposes in a GDPR-compliant way.	Exchange education data

Identity federation	External link	A federated identity in information technology is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.	Authenticate users
Verifiable credentials	External link	Digital credentials which follow the relevant World Wide Web Consortium open standards. They can represent information found in physical credentials, such as a passport or license, as well as new things that have no physical equivalent, such as ownership of a bank account.	Issue, manage and verify credentials
OAuth	External link	The OAuth 2.0 authorisation framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.	Authenticate users.
Open Education API	External link	This open API is the result of a collaboration between education institutes and suppliers in the Netherlands and is facilitated by SURF (known collectively as the Community). Within the Working Group of the Community, the OOAPI is being constantly defined and developed so that new and existing education data can be efficiently processed.	Exchange education data
Learning Object Metadata	External link	A conceptual data schema that defines the structure of a metadata instance for a learning object is specified in this standard. For this standard, a learning object is defined as any entity, digital or non-digital, that is used for learning, education, or training; a metadata instance for a learning object describes relevant characteristics of the learning object to which it applies. Such characteristics can be regrouped in general, life cycle, meta-metadata, educational, technical, educational, rights, relation, annotation, and classification categories.	Exchange educational resources

LRMI	External link	The LRMI specification is a collection of classes, properties and concept schemes for markup and description of educational resources. The specification builds on the extensive vocabulary provided by Schema.org and other standards. Read more about LRMI.	Exchange educational resources
SCORM	External link	SCORM stands for "Sharable Content Object Reference Model." "Sharable Content Object" indicates that SCORM is all about creating units of online training material that can be shared across systems. SCORM defines how to create "sharable content objects" or "SCOs" that can be reused in different systems and contexts.	Exchange educational resources
cmi5	External link	This specification describes interoperable runtime communication between Learning Management Systems (LMS) and Assignable Units (AU).	Exchange learning opportunities
OneRoster	External link	Solves a school's need to exchange roster information securely and reliably, course materials and grades between systems.	Exchange student data
CLR	External link	Comprehensive Learner Record Standard (CLR Standard) is the new generation of secure, verifiable learning and employment records supporting all academic and workplace recognition and achievements, including courses, competencies, skills, and employer-based achievements and milestones.	Issue, manage and verify digital credentials
openID	External link	The OpenID Foundation (OIDF) is a global open standards body committed to helping people assert their identity wherever they choose.	Authenticate users
ELM	External link	European Learning Model.	Model for defining learning objects (resources, assessments, credentials...)
ELMO	External link	The ELMO XML format is the basis for the exchange of result information. Elmo is based on the CEN standard EN 15981-2011 EuroLMAI. EuroLMAI is a data model describing assessments.	Exchange educational assessments

ESSIF	External link	This is a specific component of EBSI that develops the technical framework and standards for implementing self-sovereign identity across Europe. ESSIF focuses on the interoperability of decentralised identities and credentials, providing European citizens and students with control over their personal data.	Authenticate users

12 Annex III – EU-A reports

Collected reports have not been incorporated into this document. The reports can be found in the following folder: European Digital Education Hub teams folder

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